The Sedona Conference Journal®

Volume 21 ❖ 2020

Articles

Antitrust Law, Complex Litigation, Intellectual Property Rights, and Data Security and Privacy Law

The Sedona Conference Journal®

Volume 21

■

2020

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing the nonpartisan consensus commentaries created by The Sedona Conference Working Group Series, selections from the preceding year's conferences, and selected articles from individual authors. The Journal is available on a complimentary basis to courthouses and public law libraries. Additionally, each printed issue is available for purchase ($45 for the general public; $30 for Working Group Series members). PDF copies of The Journal are complimentary. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference,
301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or
info@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® cover designed by MargoBDesignLLC at www.margobdesign.com.

Cite items in this volume to "21 Sedona Conf. J. _____ (2020)."

Publisher's Note

Welcome to Volume 21 of The Sedona Conference Journal (ISSN 1530-4981), published by The Sedona Conference, a nonprofit 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way through the creation and publication of nonpartisan consensus commentaries and advanced legal education for the bench and bar.

The various Working Groups in The Sedona Conference Working Group Series pursue in-depth study of tipping-point issues, with the goal of producing high-quality, nonpartisan consensus commentaries that provide guidance of immediate and practical benefit to the bench and bar. The Sedona Conference conducts a "regular season" of limited-attendance conferences that are mini-sabbaticals for the nation's leading jurists, lawyers, academics, and experts to examine cutting-edge issues of law and policy. The Sedona Conference also conducts continuing legal education programs under The Sedona Conference Institute (TSCI) banner, an annual International Programme on Cross-Border Data Transfers and Data Protection Laws, and webinars on a variety of topics.

Volume 21 of the Journal contains three nonpartisan consensus commentaries from The Sedona Conference Working Group on Data Security and Privacy Liability (WG11), one nonpartisan consensus commentary from the Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6), one nonpartisan consensus commentary from Sedona Canada (WG7), and the fifth edition of The Sedona Conference Glossary, produced by The Sedona Conference Technology Resource Panel. I hope you find the commentaries to be thought-provoking pieces that stimulate further dialogue and ultimately serve to move the law forward, and the Glossary to be a valuable resource that will benefit all practitioners.

For more information about The Sedona Conference and its activities, please visit our website at www.thesedonaconference.org.

Craig Weinlein
Executive Director
The Sedona Conference
August 2020

The Sedona Conference gratefully acknowledges the contributions of its Working Group Series annual sponsors, event sponsors, members, and participants whose volunteer efforts and financial support make participation in The Sedona Conference and its activities a thought-provoking and inspiring experience.

Journal Editorial Board

The Sedona Conference Advisory Board

Kevin F. Brady, Esq., Volkswagen Group of America, Herndon, VA

Prof. Stephen Calkins, Esq., Wayne State University Law School, Detroit, MI

Michael V. Ciresi, Esq., Ciresi Conlin LLP, Minneapolis, MN

The Hon. John Facciola (ret.), Washington, DC

Prof. Steven S. Gensler, University of Oklahoma College of Law, Norman, OK

Prof. George A. Hay, Cornell Law School, Ithaca, NY

Ronald J. Hedges, Esq., Dentons US LLP, New York, NY

Allan Kanner, Esq., Kanner & Whiteley, L.L.C., New Orleans, LA

The Hon. Paul R. Michel (ret.), Alexandria, VA

Dianne M. Nast, Esq., NastLaw LLC, Philadelphia, PA

The Hon. Nan R. Nolan (ret.), Redgrave LLP, Chicago, IL

The Hon. Andrew J. Peck (ret.), DLA Piper, New York, NY

Jonathan M. Redgrave, Esq., Redgrave LLP, Washington, DC

The Hon. James M. Rosenbaum (ret.), JAMS, Minneapolis, MN

Prof. Stephen A. Saltzburg, George Washington University Law School, Washington, DC

The Hon. Shira A. Scheindlin (ret.), Stroock & Stroock & Lavan LLP, New York, NY

Daniel R. Shulman, Esq., Shulman & Buske PLLC, Minneapolis, MN

Dennis R. Suplee, Esq., Schnader Harrison Segal & Lewis LLP, Philadelphia, PA

Prof. Jay Tidmarsh, University of Notre Dame Law School, Notre Dame, IN

Barbara E. Tretheway, Esq., HealthPartners, Bloomington, MN

The Hon. Tom I. Vanaskie (ret.), Stevens & Lee, Philadelphia, PA

The Hon. Ira B. Warshawsky (ret.), Meyer, Suozzi, English & Klein, P.C., Garden City, NY

Judicial Advisory Board

The Hon. Jerome B. Abrams, Minnesota District Court Judge, First Judicial District

The Hon. Michael M. Baylson, Senior U.S. District Judge, Eastern District of Pennsylvania

The Hon. Laurel Beeler, U.S. Magistrate Judge, Northern District of California

The Hon. Cathy A. Bencivengo, U.S. District Judge, Southern District of California

The Hon. Cathy Bissoon, U.S. District Judge, Western District of Pennsylvania

The Hon. Hildy Bowbeer, U.S. Magistrate Judge, District of Minnesota

The Hon. Ron Clark, Senior U.S. District Judge, Eastern District of Texas

The Hon. Joy Flowers Conti, Chief U.S. District Judge, Western District of Pennsylvania

The Hon. Mitchell D. Dembin, U.S. Magistrate Judge, Southern District of California

The Hon. James L. Gale, Senior Judge, North Carolina Business Court

The Hon. George C. Hanks, U.S. District Judge, Southern District of Texas

The Hon. Susan Illston, U.S. District Court, Northern District of California, San Francisco, CA

The Hon. Kent A. Jordan, U.S. Appellate Judge, Third Circuit

The Hon. Barbara M.G. Lynn, Chief U.S. District Judge, Northern District of Texas

The Hon. Kristen L. Mix, U.S. Magistrate Judge, District of Colorado

The Hon. Kathleen McDonald O'Malley, U.S. Appellate Judge, Federal Circuit

The Hon. Katharine H. Parker, U.S. Magistrate Judge, Southern District of New York

The Hon. Anthony E. Porcelli, U.S. Magistrate Judge, Middle District of Florida

The Hon. Xavier Rodriguez, U.S. District Judge, Western District of Texas

The Hon. Lee H. Rosenthal, Chief U.S. District Judge, Southern District of Texas

The Hon. Elizabeth A. Stafford, U.S. Magistrate Judge, Eastern District of Michigan

The Hon. Gail J. Standish, U.S. Magistrate Judge, Central District of California

The Hon. Patrick J. Walsh, Chief U.S. Magistrate Judge, Central District of California

The Hon. Leda Dunn Wettre, U.S. Magistrate Judge, District of New Jersey

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

THE SEDONA CONFERENCE COMMENTARY ON APPLICATION OF ATTORNEY-CLIENT PRIVILEGE AND WORK-PRODUCT PROTECTION TO DOCUMENTS AND COMMUNICATIONS GENERATED IN THE CYBERSECURITY CONTEXT

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editor-in-Chief:

Douglas H. Meal

Contributing Editors:

David Thomas Cohen
Emily Duke
Timothy D. Edwards
Brian Ray
Jami Mills Vibbert

Steering Committee Liaison:

Alfred J. Saikali

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily represent the views of any of the individual participants or their

employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on Application of Attorney-Client Privilege and Work Product Protection to Documents and Communications Generated in the Cybersecurity Context*, 21 SEDONA CONF. J. 1 (2020).

PREFACE

Welcome to The Sedona Conference *Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context* ("*Commentary*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages. We hope the *Commentary* will be of immediate and practical benefit to clients, attorneys, and jurists.

The Sedona Conference acknowledges Editor-in-Chief Doug Meal for his leadership and commitment to the project. We also thank contributing editors David Cohen, Emily Duke, Tim Edwards, Brian Ray, and Jami Vibbert for their efforts, and Al Saikali for his valuable counsel as Steering Committee liaison. We also thank Ernâni Magalhães for his contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings, where drafts of the *Commentary* were the subject of the dialogue. The publication was also subject to a period of public comment.

On behalf of The Sedona Conference, we thank all of them for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
November 2019

TABLE OF CONTENTS

This *Commentary* evaluates the application of the attorney-client privilege and work-product protection to documents and communications that an organization generates in the cybersecurity context. The goal of the *Commentary* is to address the absence of "settled law" on this topic by assessing (1) how the courts have and can be expected to decide, and what organizational practices will be important to a court's decision regarding, whether the attorney-client privilege or work-product protection applies to documents and communications generated in the cybersecurity context; and (2) how the development of the law in this area should be informed not just by established attorney-client privilege and work-product protection legal principles, but also by the policy rationales underlying the attorney-client privilege and work-product protection generally and those unique to the cybersecurity context.

Part A of the *Commentary* elaborates on the *Commentary's* purpose (as summarized above) and sets forth its target audience. Part B sets forth the legal principles generally applicable to claims of attorney-client privilege and work-product protection. Part C uses the general principles set forth in Part B and other relevant legal sources to evaluate how the courts have and can be expected to decide, and what organizational practices will be important to a court's decision regarding, whether the attorney-client privilege or work-product protection applies to various types of documents and communications that an organization generates in the cybersecurity context. Section 1 of Part D examines whether and to what extent the results suggested in Part C are consistent with the policy rationales underlying the attorney-client privilege and work-product protection generally and those unique to the cybersecurity context. Section 2 of Part D considers various proposals for adapting existing attorney-client privilege and work-product protection law, or developing entirely new protections, for documents and communications

that an organization generates in the cybersecurity context, and the tradeoffs those proposals present.

A. PURPOSE AND TARGET AUDIENCE

With cybercrime on the rise, cybersecurity breaches have become more frequent, and organizations have increasingly found themselves subject to litigation and/or regulatory investigations by reason of having experienced such breaches. In such litigation and/or regulatory investigations, it is often (if not always) the case that the organization has created documents and/or engaged in communications that contain information about the organization's cybersecurity practices that are therefore relevant to the litigation or investigation. Examples include pre-breach documents and communications such as assessments of the organization's information security posture (e.g., technical and gap assessments), table-top exercise results, internal audit reports, reports to third parties (e.g., clients or insurers), or post-hoc analyses of prior incidents. Relevant cybersecurity-related documents and communications also are regularly generated by an organization after it suffers a cybersecurity breach, as it conducts a forensic investigation of the breach, assesses its information security posture, remediates the circumstances that may have enabled the breach to occur, and/or communicates with third parties (e.g., law enforcement, insurers, vendors, clients, or public relations firms) regarding the breach.

Such documents and communications are often highly relevant to litigation or regulatory investigations over a breach because they pertain to issues such as (1) whether the organization's cybersecurity practices, or its oversight of third parties' (e.g., vendors') cybersecurity practices, complied with any applicable legal requirements; (2) whether the organization made deceptive statements regarding its cybersecurity practices that might provide a basis for misrepresentation-based claims; and/or (3) whether the organization provided legally sufficient notice to external parties regarding the breach. Accordingly,

such documents and communications are likely to be helpful to plaintiffs and regulators in trying to prove their claims in any breach-related litigation or regulatory investigations, and potentially damaging to the breached organization's legal defenses to such claims. As a result, the breached organization may desire to shield such documents and communications from discovery under the attorney-client privilege or as protected trial preparation "work product" (such protection being referred to both colloquially and in this *Commentary* as "work-product protection"), whereas plaintiffs and regulators may desire to overcome any such assertion of attorney-client privilege or work-product protection.

Because cybersecurity law is in its infancy, there are only a few judicial decisions in the cybersecurity area that even address, and certainly there is no "settled law" in the cybersecurity area that establishes, when, if ever, a breached organization's pre- and post-breach cybersecurity-related documents and communications (collectively, CI) can be protected from discovery under the attorney-client privilege or the work-product protection. Moreover, because CI tends to be unique to the cybersecurity context, or at least not regularly encountered in litigation generally, the applicability of the attorney-client privilege and the work-product protection to CI has received little if any judicial attention *outside* the cybersecurity area.[1] Cybersecurity lawyers and judges handling cybersecurity cases are therefore currently operating with only minimal guidance in considering

1. For instance, while there is substantial case law on the applicability of the attorney-client privilege and work-product protection to documents like financial reports and product safety investigations, courts have had little occasion to rule on whether CI such as penetration test reports or data-breach forensic investigations qualifies for either protection.

whether and to what extent CI qualifies for the attorney-client privilege or the work-product protection.

The *Commentary* seeks to address the absence of settled law in this area by providing cybersecurity lawyers (whether they are private practitioners, in-house organizational attorneys, or government regulators) and judges with: (i) an evaluation of how the courts have extrapolated and can be expected to extrapolate general principles of attorney-client privilege and work-product protection law into the context of CI; and (ii) guidelines as to what practices by the organization in question the courts can be expected to consider as important in deciding whether an organization's CI[2] can be protected from discovery under the attorney-client privilege or the work-product protection.[3] The

2. The *Commentary* focuses on attorney-client privilege and work-product protection claims that an organization might assert as to *its own* CI, rather than attorney-client privilege and work-product protection claims that such an organization's adversaries might assert as to *their* documents and communications.

3. The *Commentary* focuses on attorney-client privilege and work-product protection law, as opposed to other privileges and protections that might potentially apply to CI, but recognizes that other privileges and protections may potentially be applicable to CI and/or may have underlying policy rationales that bear upon the propriety of according attorney-client privilege and/or work-product protection to CI. In addition, while private lawsuits and regulatory investigations regarding cybersecurity breaches occur inside and outside of the United States, and accordingly, data security lawyers have an interest in both the U.S. and the non-U.S. legal standards governing attorney-client privilege and work-product protection claims that might be made as to CI, the *Commentary* focuses solely on the U.S. legal standards. In this regard, it bears noting that many of the cybersecurity decisions discussed in Part C below, while brought in federal court, were decided under state attorney-client privilege law pursuant to Federal Rule of Evidence 501, because the court's jurisdiction rested on diversity of citizenship. However, none of those decisions are at odds with any of the general governing principles of attorney-client privilege law discussed in Part B.1 below or turned on the

Commentary also seeks to help move the law forward by providing practitioners (faced with advocating for and against the discoverability of CI), judges (faced with rendering decisions on its discoverability), and legislators (seeking to create law on its discoverability) with an assessment of the arguments for and against having the discoverability of CI be determined under general principles of attorney-client privilege and work-product protection law, as opposed to modifying those principles in the context of CI to create more or less protection of CI from discovery than otherwise would be provided under the attorney-client privilege and the work-product protection. Finally, the *Commentary* considers various proposals for adapting existing attorney-client privilege and work-product protection law, or developing entirely new protections, in the CI context. To this end, the *Commentary* calls for enacting a qualified—but not an absolute—stand-alone cybersecurity privilege under which CI would enjoy some measure of protection against discoverability, whether or not lawyers were sufficiently involved in its creation to qualify the CI in question for the attorney-client privilege and/or the work-product protection. The *Commentary* also calls for all U.S. jurisdictions to recognize a "no waiver" doctrine that provides a data holder's disclosure of CI to law enforcement would not waive any privilege or protection that might otherwise be claimed in future civil litigation.

---

attorney-client privilege law of the state in question being at odds with one or more of those general governing principles. Accordingly, while differences do exist in various states' attorney-client privilege laws, none of those differences are relevant to the discussion in Parts C and D below regarding the application of attorney-client privilege law to CI. Similarly, while differences also exist in various states' laws regarding work-product protection and waiver of privilege, none of those differences are relevant to the discussion in Parts C and D below regarding the application of those laws to CI.

B. GENERAL GOVERNING PRINCIPLES

This Part of the *Commentary* summarizes the general principles of attorney-client privilege and work-product protection law most relevant to the application of the attorney-client privilege and the work-product protection to CI. This Part is therefore not intended as a generalized primer on attorney-client privilege and work-product protection law. Part B.1 sets forth the relevant general principles of attorney-client privilege law; Part B.2 sets forth the relevant general principles of work-product protection law; and Part B.3 sets forth the relevant general principles regarding waiver of attorney-client privilege and work-product protection.

1. The Attorney-Client Privilege

The attorney-client privilege generally protects a communication made in confidence for the "predominant purpose" of obtaining legal advice from a lawyer.[4] The privilege protects communications, including observations of the client's communicative acts (such as the client revealing a hidden scar or submitting to a medical examination by a doctor enlisted by the attorney), but does not permit a party to resist disclosure of the facts underlying the communications to the extent they are discoverable separate from the communications.[5] The

4. *In re* County of Erie, 473 F.3d 413, 419–20 (2d Cir. 2007); United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961). Courts sometimes alternatively use the phrase "primary purpose" or "dominant purpose" in this context, acknowledging that it has the same meaning as "predominant purpose." *See, e.g.*, *In re County of Erie*, 473 F.3d at 420 (citing *In re* Buspirone Antitrust Litig., 211 F.R.D. 249, 252–53 (S.D.N.Y. 2002); U.S. Postal Serv. V. Phelps Dodge Refining Corp., 852 F. Supp. 156, 163 (E.D.N.Y. 1994).

5. 1 KENNETH S. BROUN & ROBERT P. MOSTELLER, MCCORMICK ON EVIDENCE § 89 (7th ed. 2016).

privilege's "purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."[6] "[L]ike any other testimonial privilege," however, "this rule contravenes the fundamental principle that the public has a right to every man's evidence," and therefore courts "construe it narrowly to serve its purposes."[7]

In the corporate context, confidential communications between corporate employees and counsel for the predominant purpose of assisting counsel in rendering legal advice to the company are protected by the attorney-client privilege.[8] The majority of courts today employ a "functionality" or "subject-matter" test that extends the attorney-client privilege to include a company lawyer's communications with any corporate employee as long as the communication relates to the subject matter for which the company is seeking legal representation.[9] Courts generally have held under both federal common law and

---

6. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

7. *In re* Pac. Pictures Corp., 679 F.3d 1121, 1126 (9th Cir. 2012) (internal citation and quotation marks omitted).

8. *Id.* at 396.

9. 1 THE AMERICAN LAW INSTITUTE, RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 73 (2000). Note: Some states continue to employ the more restrictive "control group" test, which designates only upper-level management as clients of the corporate counsel. *See, e.g.,* Alaska (*see* Manumitted Cos. v. Tesoro Alaska Co., 2006 WL 8431821, at *2 (D. Alaska Aug. 16, 2006)); Illinois (*see* Consolidation Coal Co. v. Bucyrus-Erie Co., 432 N.E.2d 250 (Ill. 1982); Sterling Fin. Mgmt., L.P. v. UBS PaineWebber, Inc., 782 N.E.2d 895, 900 (Ill. 2002)); Hawaii (HAW. REV. STAT. § 626-503); Maine (ME. R. EVID. 502(a)(2)). Many other states have yet to specifically decide which test to apply. *See* Brian E. Hamilton, *Conflict, Disparity, and Indecision: The Unsettled Corporate Attorney-Client Privilege,* 1997 ANN. SURV. AM. L. 629, 630 (1997). The control group test has been explicitly rejected for use by federal courts. *See Upjohn Co.*, 449 U.S. at 390–92.

state law[10] that this includes not just communications with actual employees, but also with independent contractors who are the "functional equivalent" of an employee.[11] Because in-house counsel may play multiple roles in a corporation, *some* courts applying either federal common law or state law have applied additional scrutiny to assertions of privilege involving communications with in-house counsel, requiring organizations to make a "clear showing" that such communications were made for a legal, rather than a business, purpose.[12]

Communications between "privileged persons" *may* include those between employees, in-house counsel or outside counsel, and any of the company's subsidiaries or affiliates and any combination of them. These could be communications: (1) from employees to counsel; (2) from counsel to employees; (3) between counsel; (4) between employees or their functional equivalents;[13] or (5) with qualified agents of counsel or the client (e.g., employees or counsel of an agent, confidential litigation

10. In U.S. federal courts, privilege law is governed by FED. R. EVID. 501. If jurisdiction is based on a federal question, FED. R. EVID. 501 provides for the application of the federal common law of privilege. State privilege law applies in most cases brought under the federal court's diversity jurisdiction, and in other federal proceedings "with respect to an element of a claim or defense as to which state law supplies the rule of decision." FED. R. EVID. 501. State law regarding privilege issues applies in state court proceedings. Each state has its own articulation of the privilege, and there are considerable differences among jurisdictions regarding its scope and application.

11. *See, e.g.*, *In re* Bieter Co., 16 F.3d 929 (8th Cir. 1994).

12. *See, e.g.*, *In re* Vioxx Prod. Liab. Litig., 501 F. Supp.2d 789, 799 (E.D. La. 2007) ("While this expanded role of legal counsel within corporations has increased the difficulty for judges in ruling on privilege claims, it has concurrently increased the burden that must be borne by the proponent of corporate privilege claims relative to in-house counsel.").

13. 2 DAVID M. GREENWALD, ROBERT R. STAUFFER & ERIN R. SCHRANTZ, TESTIMONIAL PRIVILEGES § 1:31 (2012).

consultants, or informal consulting experts).[14] The nature and scope of the privilege varies state-by-state and is not uniform as a matter of federal common law, with certain states and federal courts limiting the extent and/or existence of any claim of privilege, for example, between nonlawyer employees, or with functional equivalents and/or affiliated entities.

Courts have generally held under both federal common law and state law that, for the attorney-client privilege to apply, the dominant or predominant purpose of the communication itself must have been to solicit or render legal advice.[15] At least one state (California) is more protective, providing that communications will be deemed to present a prima facie claim of attorney-client privilege so long as obtaining advice was the predominant purpose of the *relationship* between the client and counsel.[16]

Courts have generally held under both federal common law and state law that the attorney-client privilege can extend to communications involving counsel-retained experts where the

---

14. *Id*. at §§ 1:28–1:32 (agents of counsel), and at § 1:36 (representatives and agents of the client).

15. *See In re* County of Erie, 473 F.3d 413, 420 (2d Cir. 2007) ("We consider whether the predominant purpose of the communication is to render or solicit legal advice.") (applying federal law); THE AMERICAN LAW INSTITUTE, *supra* note 7, at § 72 cmt. c (2000) ("A client must consult the lawyer for the purpose of obtaining legal assistance and not predominantly for another purpose.").

16. *See, e.g.*, Costco Wholesale Corp. v. Super. Ct., 219 P.3d 736, 746 (Cal. 2009) (a court must first determine "the dominant purpose *of the relationship* between the [client] and its in-house attorneys," and if the dominant purpose is the provision of legal advice, those communications would be subject to the privilege) (emphasis in original); *see also* Cason v. Fed. Life Ins. Co., No. C-10-0792, 2011 WL 1807427, at *2 (N.D. Cal. May 11, 2011) ("It is not the dominant purpose of a communication that dictates whether the attorney-client privilege is applicable; rather, the issue is what was *the dominant purpose of the relationship*." (emphasis in original)).

expert is necessarily included for the purpose of assisting the attorney in providing legal advice. Specifically, under what is often referred to as the *Kovel* doctrine, the attorney-client privilege will extend to the work and communications of third-party experts if the expert was hired "for the purpose of obtaining [confidential] legal advice from the lawyer."[17] In *Kovel*, the attorney hired an accountant to assist him in understanding his client's tax position, and the communications at issue were between the client and the accountant. The court analogized the accountant to a translator, whose assistance in overcoming a language barrier would not destroy the privilege. Where the requirements for this exception are met, i.e., where the expert's presence in the communication is necessary for counsel's provision of legal advice, courts have held that the privilege may extend not only to communications between counsel and the expert, but also to communications between the expert and the client directly.[18]

---

17. United States v. Kovel, 296 F.2d 918, 922–23 (2d Cir. 1961); *see also* CAL. EVID. CODE § 952 (privilege extends to "those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted"); Rodriguez v. Super. Ct., 18 Cal. Rptr. 2d 120, 123–24 (Cal. Ct. App. 1993) (communications between client and a doctor hired by counsel to evaluate client for defense of criminal proceedings were privileged); Nat'l Steel Prods. Co. v. Super. Ct., 210 Cal. Rptr. 535, 538 (Cal. Ct. App. 1985) (privilege could extend to communications involving engineering expert retained by counsel to perform technical analysis of building structure to assist counsel in providing legal advice).

18. *See* Umpqua Bank v. First Am. Title Ins. Co., 2011 WL 997212, at *7 (E.D. Cal. Mar. 17, 2011) (communications between client and counsel-retained expert protected where for the purpose of furthering legal advice); *see also In re* OM Group Sec. Litig., 226 F.R.D. 579, 588–89 (N.D. Ohio 2005) (same); *In re* Grand Jury Subpoenas Dated March 24, 2003, 265 F. Supp. 2d 321, 331–32 (S.D.N.Y. 2003) (same).

For communications among company employees (or the functional equivalents of employees) that do not include counsel or counsel-retained experts, the inquiry is highly fact-dependent, and generally turns on the intent of the creator of the communications.[19]

In order to be privileged, a communication must be made in confidence. Communications contained in public documents, such as final press releases and corporate annual reports, are not privileged. The party asserting a privilege or protection has the burden of establishing that withheld information qualifies for protection.

2. Work-Product Protection Law

In U.S. federal court, the work-product doctrine is governed by Fed. R. Civ. P. 26(b)(3)(A), which provides that "a party may not discover documents and tangible things that are prepared *in anticipation of litigation* or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)."[20] To satisfy the "anticipation of litigation" test, a document must be prepared after a point at which the company "anticipated" that litigation would be filed against it. Courts applying the rule have differed somewhat in their formulation of the test for determining when an as-yet-uncommenced litigation is sufficiently "anticipated" to make work-product protection potentially applicable. They

19. *E.g.*, Williams v. Sprint/United Mgmt. Co., 238 F.R.D. 633, 639–40 (D. Kan. 2006) (sustaining privilege as to drafts that ultimately were not shared with counsel, because they nonetheless "constituted communications made for the purpose of obtaining legal advice"); *In re* Bieter Co., 16 F.3d 929, 938 (8th Cir. 1994) (applying a fact-intensive privilege analysis to the functional equivalent of an employee).

20. FED R. CIV. P. 26(b)(3)(A).

agree, however, that the prospect of that future litigation must be more than speculative.[21]

Evidence that courts have looked to in determining whether litigation was "anticipated" includes evidence that a prospective plaintiff intended to make a claim;[22] hiring of outside counsel;[23] dissemination of a "litigation hold" or preservation notice;[24] and putting a potential adversary on notice, either directly

---

21. *See, e.g.*, Willis v. Westin Hotel Co., No. 85 Civ. 2056 (CBM), 1987 WL 6155, at *1 (S.D.N.Y. Jan. 30, 1987) ("The mere contingency that litigation may result does not give rise to the privilege."); Hertzberg v. Veneman, 273 F. Supp.2d 67, 75 (D.D.C. 2003) ("While litigation need not be imminent or certain in order to satisfy the anticipation-of-litigation prong of the test, this circuit has held that at the very least some articulable claim, likely to lead to litigation, must have arisen, such that litigation was fairly foreseeable at the time the materials were prepared.") (quotations and citation omitted); *In re* Grand Jury Investigation, 412 F. Supp. 943, 948 (E.D. Pa. 1976) ("Advising a client about matters which may or even likely will ultimately come to litigation does not satisfy the 'in anticipation of' standard. The threat of litigation must be more real and imminent than that."); Helt v. Metro. Dist. Comm'n, 113 F.R.D. 7, 12 (D. Conn. 1986) ("To qualify, the documents must have been prepared any time after initiation of the proceeding or such earlier time as the party who normally would initiate the proceeding had tentatively formulated a claim, demand or charge.") (internal quotation omitted).

22. *See, e.g.*, Resolution Trust Corp. v. Mass. Mut. Life Ins. Co., 200 F.R.D. 183, 189–90 (W.D.N.Y. 2001); McNulty v. Bally's Park Place, Inc., 120 F.R.D. 27, 29 (E.D. Pa. 1988).

23. *See* Maertin v. Armstrong World Indus., Inc., 172 F.R.D. 143 (D.N.J. 1997); *but see* Lindley v. Life Investors Inc. Co., Nos. 08-CV-0379-CVE-PJC, 09-CV-0429-CVE-PJC, 2010 WL 1741407, at *4 (N.D. Okla. Apr. 28, 2010) ("[T]he mere fact that the Taskforce consulted in-house or outside counsel about potential litigation scenarios does not mean that defendant was acting in anticipation of litigation.").

24. *See* Major Tours, Inc. v. Colorel, Civil No. 05-3091 (JBS/JS), 2009 WL 2413631, at *2 (D.N.J. Aug. 4, 2009) (collecting authorities that deem litigation hold notices subject to work-product protection).

or through public disclosure, of facts that reasonably could be expected to result in the adversary initiating litigation.[25]

In addition to showing that litigation was anticipated, the proponent of the work-product protection must also show that the document was prepared "in anticipation of" the anticipated litigation, and not for some other purpose. Most circuits decide this aspect of work-product protection by applying the "because of" test, asking if the document was prepared "because of" the prospect of the litigation in question.[26] In regard to "dual purpose" documents that serve both business and litigation purposes, the "because of" test is often characterized as a "but for" test: "[w]here a document was created because of anticipated litigation, and would not have been prepared in substantially similar form *but for* the prospect of that litigation, it falls within Rule 26(b)(3)."[27] The Fifth Circuit applies the more restrictive "primary purpose" test, requiring that "the primary motivating purpose . . . was to aid in possible future litigation."[28]

Materials otherwise qualifying for work-product protection may be discovered under certain circumstances where a party

---

25. *See, e.g.*, Schwarz & Schwarz of Virginia L.L.C. v. Certain Underwriters at Lloyd's London, No. 6:07cv00042, 2009 WL 1043929, at *3–4 (W.D. Va. Apr. 17, 2009) (finding that the date on which insurer began to anticipate litigation was the date it denied coverage, and noting the other cases with same holding); Country Life Ins. Co., v. St. Paul Surplus Lines Ins. Co., No. 03-1224, 2005 WL 3690565, at *7 (C.D. Ill. Jan. 31, 2005) (same); *see also* United States v. Roxworthy, 457 F.3d 590, 597 (6th Cir. 2006) (finding that a potential defendant anticipated litigation against the I.R.S. based on the fact that the I.R.S. frequently litigated tax losses of the sort the potential defendant had decided to claim, even though the IRS was not, at the time, aware that the defendant was going to claim such a tax loss).

26. *E.g.*, *In re* Grand Jury Proceedings, 604 F.2d 798, 803 (3d Cir. 1979).

27. United States v. Adlman, 134 F.3d 1194, 1195 (2nd Cir. 1998).

28. *In re* Kaiser Aluminum & Chem. Co., 214 F.3d 586, 593 (5th Cir. 2000).

"shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means."[29] But, "[i]f the court orders discovery of those materials, it must protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation."[30]

3. Waiver

The attorney-client privilege or the work-product protection may in certain circumstances be waived as to a document or communication that would otherwise be protected from discovery under one or both doctrines. The attorney-client privilege is more easily waived than the work-product protection. For instance, disclosure of an otherwise attorney-client privileged document or communication to any third party generally results in waiver of the privilege (subject to limited exceptions, such as for disclosures to a third-party having a common interest or who is the functional equivalent of an employee), whereas disclosure of a work-product protected document to a third party generally does not waive the protection unless the disclosure is to an adversary or a conduit to an adversary.[31] Courts have also indicated that disclosure of an attorney-client privileged communication within a company may waive that privilege if the disclosure is made to an employee who did not "need to know"

29. FED. R. CIV. P. 26(b)(3)(A)(ii).

30. FED. R. CIV. P. 26(b)(3)(B).

31. *See, e.g.*, United States v. Deloitte LLP, 610 F.3d 129, 140 (D.C. Cir. 2010); United States v. Graf, 610 F.3d 1148, 1158 (9th Cir. 2010); *In re* Bieter Co., 16 F.3d 929 (8th Cir. 1994); La. Mun. Police Employees Ret. Sys. v. Sealed Air Corp., 253 F.R.D. 300, 309 (D.N.J. 2008).

of the document or communication.[32] Moreover, language in some decisions could be read to suggest that in jurisdictions that employ a "control group" test for attorney-client privilege, disclosures of attorney-client privileged communications to internal employees outside the "control group" may waive the privilege as well.[33]

Disclosure of attorney-client privileged or work-product protected documents or communications to a third party may result in waiver of the privilege or protection for the documents or communications not only as against that third party, but also as against other third parties. While at least one court has held that a "selective waiver" theory may protect a party who discloses information to a governmental entity from losing either the attorney-client privilege or the work-product protection as to that information as against other entities,[34] many courts have rejected this theory.[35] Some courts have allowed disclosure to

---

32. *See, e.g.*, Verschoth v. Time Warner, Inc., No. 00CIV1339AGSJCF, 2001 WL 286763 at *3 (S.D.N.Y. Mar. 22, 2001) (company "lost any privilege with respect to" legal advice when that advice was conveyed to worker who did not need to know that advice).

33. *See, e.g.*, Barr Marine Prods., Co., Inc. v. Borg-Warner Corp., 84 F.R.D. 631, 634 (E.D. Pa. 1979) ("if one member of the control group relays legal advice *to another member* the privilege is not lost") (emphasis added).

34. *See, e.g.*, Diversified Indus., Inc. v. Meredith, 572 F.2d 596, 611 (8th Cir. 1977) (referring to a selective waiver as a "limited waiver"); *In re* McKesson HBOC, Inc. Secs. Litig., No. C-99-20743 RMW, No. C-00-20030 RMW, 2005 U.S. Dist. LEXIS 7098, at *47 (N.D. Cal. Mar. 31, 2005).

35. *In re* Columbia/HCA Healthcare Corp. Billing Practices Litig., 293 F.3d 289, 306 (6th Cir. 2002) (finding that a party's voluntary disclosure of protected documents to the SEC, even under a confidentiality agreement, constituted a complete waiver of attorney-client and work-product privilege); *see also* Westinghouse Elec. Corp. v. Republic of Phil., 951 F.2d 1414, 1429 (3d Cir. 1991) (determining party's "disclosure of work product to the SEC and to the DOJ waived the work-product doctrine as against all other

law enforcement or regulators under some circumstances without waiving the attorney-client and work-product protections as against other parties, provided that the company entered into a confidentiality or protective order containing appropriate non-waiver and other provisions.[36]

In addition, disclosure of attorney-client privileged and/or work-product protected information may operate not only as a waiver of the disclosed information as to others, but also as a waiver of attorney-client privilege and/or work-product protection as to any related *undisclosed* information, both as to the recipient of the disclosed information and as to others. Such subject-matter waivers historically were not recognized in the work-product protection context (with some exceptions),[37] but were typically recognized in the attorney-client privilege context.[38] Today, Federal Rule of Evidence 502, which became effective in 2008, consolidates treatment of the scope of waiver of the attorney-client privilege and work-product protection into a

---

adversaries," notwithstanding if there was or was not a finding that there was a confidentiality agreement entered into with government agencies).

36. *Compare In re Columbia/HCA.*, 293 F.3d at 303 (declining to apply selective waiver even in instances where the parties enter into confidentiality orders), *with In re* Steinhardt Partners, L.P., 9 F.3d 230, 236 (2d Cir. 1993) (indicating that selective waiver would apply in disclosure to the government as long as a confidentiality agreement existed). *See also, e.g.*, *In re* Qwest Commc'ns Int'l Inc., 450 F.3d 1179, 1195-99 (10th Cir. 2006). A footnote accompanying documents voluntarily disclosed to a government entity concerning the exemption of such documents from production under the Freedom of Information Act (FOIA) is not a sufficient confidentiality agreement to attain selective waiver. *See, e.g.*, *In re* Aqua Dots Prod. Liab. Litig., 270 F.R.D. 322, 330 (N.D. Ill. 2010), *aff'd*, 654 F.3d 748 (7th Cir. 2011).

37. *See, e.g.*, Pittman v. Frazer, 129 F.3d 983, 988 (8th Cir. 1997); 2 DAVID M. GREENWALD ET AL., *supra* note 13 § 2:32 (3d ed. 2015).

38. *See, e.g.*, *In re* Sealed Case, 676 F.2d 793, 809 (D.C. Cir. 1982); 2 CHRISTOPHER B. MUELLER ET AL., FEDERAL EVIDENCE § 5:33 (4th ed. 2017).

single regime when the disclosure is made in a federal proceeding or to a federal office or agency.[39] Under Rule 502, when such a disclosure waives the attorney-client privilege or work-product protection, the waiver extends to undisclosed information only if "the waiver is intentional, the disclosed and undisclosed communications or information concern the same subject matter, and they ought in fairness to be considered together."[40]

39. Chick-fil-A v. ExxonMobil Corp., No. 08-61422-CIV, 2009 WL 3763032 (S.D. Fla. Nov. 10, 2009).

40. FED. R. EVID. 502(a). Even as to disclosures covered by Rule 502(a), however, some courts have been more reluctant to find a subject-matter waiver as to work-product protection than as to attorney-client privilege. *See, e.g., Chick-fil-A*, (subject matter waiver under Rule 502(a) extended only to fact work product, not opinion work product, given the special protection afforded to opinion work product).

C. APPLICATION OF ATTORNEY-CLIENT PRIVILEGE AND WORK-PRODUCT PROTECTION PRINCIPLES TO CYBERSECURITY INFORMATION

Taking the general principles of privilege and protection law and applying them to the CI context becomes more complex. The question of whether the attorney-client privilege or work-product protection applies to CI generally arises when a company is faced with litigation or a civil government investigation following a security incident. During this post-incident litigation or investigation, many types of CI may be sought by a regulator or private plaintiff concerning actions taken (or not taken) by the company prior to and after the security incident. These types of CI may be relevant to show the organization's security posture pre-incident, the causes of the incident, and the efficacy of the response.

This Part of the *Commentary* will discuss a variety of CI that organizations may create prior to a security incident when building and implementing a cybersecurity program, and in response to security incidents and breaches. To date, few courts have been faced with questions regarding whether to apply attorney-client privilege and work-product protection principles to the cybersecurity context. While parties often dispute attorney-client privilege and work-product protection issues in cybersecurity litigation or investigations, given the dearth of case law, such disputes appear to be primarily resolved without any judicial intervention. Thus, in addressing how courts may determine whether the attorney-client privilege or work-product protection attaches to certain CI, this Part analyzes not only on-point case law, but also decisions addressing similar types of documents in other contexts. This Part also extrapolates practices that may affect the likelihood that the attorney-client privilege and/or work-product protection will apply.

Because the legal concepts vary in some respects, we have divided this Part into sections separately dealing with the privilege and protection concepts that may apply to CI created (1) before a security incident is discovered ("pre-incident CI"), and (2) after a security incident is discovered (post-incident CI"). The third section of this Part discusses the various types of waiver that may apply if the CI holder discloses privileged or protected information.

This Part analyzes the application to CI of the general governing principles set forth in Part B. It does not consider whether CI should, as a policy matter, receive more or less protection than it does under the general governing principles set forth in Part B. That issue is, however, discussed at length in Part D. Moreover, Part C's analysis of the application of the attorney-client privilege to CI gives no consideration to the importance of the CI in question to plaintiffs and regulators, because there is no basis in attorney-client privilege law for communications otherwise protected by the attorney-client privilege to lose that protection based on the need of the opposing party to obtain such discovery. On the other hand, such a basis does exist in work-product protection law, so Part C's analysis of the application of the work-product protection to CI gives substantial consideration to the importance of the CI in question to the party seeking the CI.[41]

1. *Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work-Product Protection to Pre-Incident CI*

Pre-incident CI concerning an organization's security program, policies, and procedures prior to any security incident

41. *See* Part C.2.c.ii, *infra*.

being discovered can fall into several distinct categories. Depending on the level of security protocols and programs in place and the size of the organization and its security team, an organization may have little-to-no pre-incident CI, or it may have large amounts. Because cybersecurity issues are multidisciplinary, involving technical tools and processes that interact with legal standards and obligations, this CI may or may not involve lawyers, consultants, technologists, security teams, and others at various stages and for various reasons.

a. Types of Pre-Incident CI

The potential pre-incident CI that may be sought in a post-incident situation includes the following, non-exhaustive list.

i. Technical Inventories, Configuration Reviews, Vulnerability Scans, and Penetration Tests

One aspect of pre-incident cybersecurity processes can include the identification and inventory of an organization's assets, data, and systems. This identification process allows organizations to prioritize risk and assign security controls in a methodical manner. A technical security expert or vendor may use a variety of tools to take an inventory of the network infrastructure, measure what devices are connected to the network, inventory the software applications installed and where the applications are installed, catalogue external information systems, map communication and data flows, and measure which software applications are up to date.

Configuration reviews may include review of the configuration of servers, firewalls, routers, and user accounts, and a review of certain related policies, such as how user groups are configured for permissions and access to the network.

Technical experts may also be hired, or the internal security team may be used, to conduct vulnerability scans to identify weaknesses in a network or system; for example, open ports, unregistered devices, or firewalls that are not turned on. These scans typically use software tools to investigate the current state of a computer system or network to identify points of weakness. Penetration tests add the aspect of exploiting discovered weaknesses to see if other checks and balances will nonetheless prevent the tester from doing harm to the system. Thus, the testing entity will attempt to access confidential, personal, or sensitive information, alter information, or shut down the system using one of the now-known vulnerabilities.

Data generated and retained with respect to these inventories, reviews, scans, and tests discloses the current state of the system, including possible gaps in security controls or related processes, potential vulnerabilities, and aspects that may be ripe for remediation. In most of these instances, the tools used and expertise required to perform the investigation of a system's "current state" are beyond the understanding of a lawyer or operational personnel within the organization. Thus, whether a lawyer is involved depends on the circumstances. For example, sometimes a basic vulnerability assessment may be conducted through interviews of employees and users to determine the location of weaknesses. This interview could uncover people- or process-oriented vulnerabilities. The interview may (or may not) have been done by a lawyer or someone from audit or compliance working under the direction of a lawyer. The CI in this instance may take the form of attorney notes and, potentially, a written compliance or gap report for management, with potential remediation.

Similarly, while these technical inventories, configuration reviews, vulnerability scans, and penetration tests may be part

of an organization's larger risk assessment process done at the behest of counsel, those activities often do not involve counsel.

ii. Security Risk Assessments, Outside Audits, and Remediation Efforts

Another aspect of pre-incident CI could be in the form of a security risk assessment, which may be completed internally or by hiring third-party security vendors and/or outside counsel. The risk assessment may include the entire organization or some specific systems (systems containing personal information, for example), or some aspect of the organization's security controls (vendor management, for example). The output of these security assessments is often a prioritized list of items the organization may wish to address with more extensive security measures. Sometimes these are technology-based, such as the need to encrypt certain types of data on portable media; sometimes these are process-based, such as the need to create a procedure for dealing with exiting and transferring employees; and sometimes these are people-based, such as the need to increase training or compliance.

If outside counsel is involved, these assessments may be done to help the lawyer explain to the organization what legal obligations it has, whether they are being met, and any opportunities to improve. Such legal assessments may also explain how the organization might remediate its security posture to meet those obligations, including addressing what specific activities are considered reasonable under various laws.

Legal counsel often will work with technical experts within the organization or hire technical experts to assist in creating a legally prioritized remediation report. Assessments prioritized by reference to the legal standards and environment in which the company operates, and conducted under the supervision of

counsel, contain legal decisions about what is reasonable under the law for the particular organization.

Other times, only security vendors are involved, and while risks are categorized and prioritized, they typically are not done with reference to the legal environment in which the company sits, but rather prioritized according to technical standards. These security vendors are often, but not always, hired by the IT or security departments, and no counsel is involved.

In addition to security assessments, organizations will sometimes hire outside vendors to perform compliance audits, such as audits to assess for compliance with the Payment Card Industry Data Security Standard (PCI DSS). Again, these are often done without legal counsel's advice, in order to obtain independent certification of PCI compliance.

Following up on these assessments and audits, companies will often engage outside security vendors and/or legal counsel to assist in remediation of any gaps and/or opportunities for improvement identified in the security assessment or audit process.

iii. Policies and Procedures

Many aspects of a well-run and reasonable cybersecurity system are documented in IT, management, or employee policies or procedures. This could include policies and procedures directed at one specific security control. For example, an access-control policy could dictate how to determine who has access to what, document these permissions, and describe the process for terminating such access, granting additional access, or changing access. Accompanying forms may provide documentation of these decisions, and accompanying procedures would describe how to implement the specific access controls associated with each decision. Another example could be a mobile-device policy

regarding how to handle company-owned or "bring your own" mobile devices. The policy could also be one that concerns incident response, privacy and cybersecurity generally, or acceptable use. Some state and federal laws require that organizations maintain a written information security policy, and many other standards indicate that such written policies are a requirement of reasonable cybersecurity.

While the legal team (in-house or outside) will typically be involved in drafting and revising the policies required by state and federal law, that may not be the case with respect to more technology-focused procedures, or technical configuration procedures, such as the type of encryption to use at rest or in transit. During post-incident proceedings, both IT-focused and legal policies and procedures may be relevant and sought. In addition, drafts of those same policies and procedures may be requested. Decisions made during the drafting process may indicate risk-based approaches that can be questioned in hindsight.

iv. Tabletop Exercises

Organizations may test their incident detection and response times or the functioning of their incident response programs by conducting tabletop exercises. Tabletop exercises typically involve the presentation of one or more hypothetical scenarios involving a security incident meant to test the incident response capabilities of the organization. These exercises usually include gathering a group of high-level stakeholders within the company, including c-suite executives, the chief information security officer or other individuals responsible for the organization's security, and individuals from the organization's risk, communications, marketing, audit, business units, customer service, and legal teams. These exercises are typically conducted by outside counsel, a technology or security vendor, or a team of both.

In addition to any information documented before and during the tabletop, a lessons-learned report typically documents how the gathered team and the organization responded to the given hypothetical. Potential gaps in process, knowledge, culture, policy, and the like will often be documented with recommendations for improvement.

v. Internal Audit Reports

In the course of ensuring a robust security system, organizations often internally test the system controls in place to determine whether they are functioning as planned. The findings from internal audits or ongoing "maintenance" monitoring typically identify gaps in security processes or gaps between policies and practice.

vi. Reports of the Security Team

This category of documents includes reports of prior security events or incidents (that may or may not have led to a breach) drafted by the security team. Some of those documents will be forwarded to the legal team or the broader incident response team (if significant enough) to inform their advice and next steps, but many are not.

vii. Board-level Documents and Communications

This category includes reports given to the board or board committees responsible for overseeing cybersecurity, as well as meeting minutes or other documentation of the board or board committee itself. As with reports of the security team, some such board-level documents and communications will have been created by or with the involvement of lawyers, but that will not always be the case.

* * *

Each of the above categories of pre-incident CI usually involves some assessment of the organization's information security posture. All will produce evidence of what the organization knew and when, and likely will result in the organization making decisions about what, if any, actions it will or will not take to reduce compliance gaps and identified risks. Below, this Part of the *Commentary* explores how the attorney-client privilege and work-product protection may apply to these general categories of CI, and what factors might be determinative in whether the protection attaches, recognizing that most determinations will be highly fact-specific.

b. Application of Attorney-Client Privilege to Pre-Incident CI

Under the basic principles of attorney-client privilege law (Part B, *supra*), the likelihood that pre-incident CI will be protected by the attorney-client privilege will vary, depending on the involvement of counsel in creating the CI in question, the purpose for counsel's involvement, and how the engagement or project is structured and executed. We examine the elements of the attorney-client privilege below and discuss the factors affecting whether the categories of pre-incident CI delineated above would likely be considered privileged under those general principles.

i. Involvement of a Lawyer

As discussed above, for documents and communications to be privileged, a lawyer must be involved in the circumstances surrounding the generation of the communication. If an attorney is not involved, under the general legal principles governing attorney-client privilege, the CI will not be considered privileged. Thus, referring back to the categories of CI listed above, any technical inventories, configuration reviews, vulnerability

scans, or penetration tests that are done by an internal or outside security vendor or expert and not done to assist an attorney will not be privileged. The same is true for security risk assessments, outside or internal audits, tabletop exercises, reports of the security team, and board-level documents and communications.

ii. For the Predominant Purpose of Obtaining Legal Advice from the Lawyer

As discussed above, for documents and communications to be privileged, such documents and communications must have been made predominantly for the purpose of assisting counsel in rendering legal advice to a client.

Courts examining whether the communication is predominantly for the purpose of providing or soliciting legal (as opposed to business) advice will focus on several indicators. Courts will examine the content of the communications to determine whether they contain or ask for legal analysis or whether they primarily concern the growth and development of profit.[42] In the context of pre-incident CI, the question of whether certain communications were made or documents created for the predominant purpose of obtaining or giving legal advice is difficult. With respect to technical inventories, configuration reviews, vulnerability scans, and penetration tests, these documents often are part of an organization's ongoing IT operations. For example, an inventory of devices, software, or locations of personal information is often part of the IT department's

42. *See, e.g.*, Fed. Trade Comm'n v. Abbvie, Inc., No. CV 14-5151, 2015 WL 8623076, at *10 (E.D. Pa. Dec. 14, 2015); Lindley v. Life Inv'rs Ins. Co. of Am., 267 F.R.D. 382, 392 (N.D. Okla. 2010), *aff'd in part as modified*, No. 08-CV-0379-CVE-PJC, 2010 WL 1741407 (N.D. Okla. Apr. 28, 2010).

inventory control, which is a business function.[43] An organization may also measure response times for identifying, containing, and remediating security incidents to measure the quality and efficacy of its security team or to maintain its normal operations. This would also not be considered privileged, even if an attorney relied upon such information in conducting a security risk assessment, prioritizing legal risk, or in drafting a report for the board of directors.

However, if this CI was created for the purpose of a legally driven or mandated security assessment, audit, or report, such underlying documents may be privileged. One can readily envision the need for such a legal analysis for any type of organization handling sensitive information; this is especially true given the broad-ranging cybersecurity activities over which the Federal Trade Commission (FTC)[44] has taken enforcement actions, including, for example, protection of passwords or adequacy of operating system security on smartphones. Other laws and regulations governing specific industries or enacted in certain states have express security requirements or require organizations to have "reasonable" or "adequate" security. These requirements include overarching statements regarding the comprehensiveness of the program, the existence of policies and procedures, training requirements, and the effectiveness of the security program. Lawyers may need to give advice regarding whether the company's security requirements comply with these laws and regulations, which often are opaquely drafted.

---

43. "[D]ocuments prepared by non-attorneys and addressed to non-attorneys with copies routed to counsel are generally not privileged since they are not communications made primarily for legal advice." Neuder v. Battelle Pac. Nw. Nat'l Lab., 194 F.R.D. 289, 295 (D.D.C. 2000).

44. The FTC is not the only regulator seeking broad enforcement powers in the data security context, but likely is the most active to date.

Similarly, many laws and regulations require organizations to oversee the security of their vendors, so legal analysis of such vendor oversight will be necessary. Counsel may also need to be involved regarding compliance with commercial contracts requiring one party to "provide reasonable security measures" for the other party's confidential information or to engage in "adequate security measures."

In other contexts, courts will generally find that documents not primarily concerned with business or marketing decisions, but rather primarily related to legal concerns (including legal risk and potential litigation or regulatory enforcement) are privileged.[45] Given the complex legal landscape and varying cybersecurity standards applicable to organizations, to the extent a lawyer engaged in a security risk assessment or audit focused on prioritizing security controls based on legal risks or compliance with legal requirements, as opposed to business decisions, courts may well find this pre-incident CI primarily related to legal concerns and risk and therefore privileged.

Similarly, internal audit reports drafted to provide insight to counsel, when counsel provides revisions and comments and uses the reports to provide advice to the organization, often are considered privileged in other contexts[46] and thus would

45. *See In re* Denture Cream Prods. Liab. Litig., No. 09-2051-MD, 2012 WL 5057844, at *15 (S.D. Fla. 2012) (finding documents regarding legal concerns, including potential litigation, related to product labeling, as opposed to marketing and business decisions related to labeling, privileged); *see also* Shire Dev. Inc. v. Cadila Healthcare Ltd., C.A. No. 10–581–KAJ, 2012 WL 5247315, at *7 (D. Del. June 15, 2012) (finding presentation by lawyer reflected legal advice concerning patent design decisions and was therefore privileged).

46. *See* United States v. Lockheed Martin Corp., 995 F. Supp. 1460, 1464 (M.D. Fla. 1998) (finding that an internal audit report drafted by a nonlawyer but provided to a lawyer for revisions and used by the lawyer to provide legal advice was privileged).

normally be expected to be privileged in the CI context. However, courts will carefully scrutinize whether the primary purpose of creating the report was truly to assist counsel's provision of legal advice. The court held in *In re Premera Blue Cross Customer Data Security Breach Litigation* (*Premera II)* that internal data-security reports prepared before any breach had been discovered (as part of normal business functions), for the purpose of enabling the company to assess the state of its technology and security, were not privileged—even if counsel supervised the audits and later used them for legal advice.[47] But *Premera II* also held that if the draft report or emails about the draft were sent to counsel seeking legal advice, those documents would be protected.[48] In other legal contexts, such as securities litigation, reports from counsel to boards of directors, committees, subcommittees, and senior executives are largely considered the provision of legal advice and subject to privilege protection.[49] Courts would likely treat the cybersecurity context no differently. If a security report to the board of directors is by an attorney and incorporates a security team report, the report may be considered privileged, whereas a security team report without the attorney analysis likely will not be considered privileged. In this pre-incident CI context, this could include not only reports on legal risk, but also reports to the board concerning disclosures to the Securities and Exchange Commission (SEC) in connection with security-related incidents and cybersecurity risk in general. The reports of the board itself are likely not privileged,

47. 329 F.R.D. 656, 666 (D. Or. 2019) [hereinafter *Premera II*].

48. *Id.* at 667.

49. *See, e.g.*, *In re* LTV Sec. Litig., 89 F.R.D. 595, 603 (N.D. Tex. 1981).

unless the board hires counsel to represent it in the preparation of the report.[50]

With respect to policies and procedures, generally, attorney-client privilege will apply to protect preliminary drafts of policies and procedures that contain legal advice and attorney opinions;[51] for example, if the policy or procedure contains comments to omit or add certain language for legal reasons. However, privilege will typically not apply to the final versions of policies and procedures merely because they were drafted by in-house or outside counsel; the final versions constitute business communications, not legal advice communications.[52] These general principles appear as applicable to CI policies and procedures as to those that are created in other contexts.

In addition to the involvement of an attorney and whether the pre-incident CI was reviewed and revised or created to assess legal risk or otherwise assist in the provision of legal advice, the creator of the communication may have some impact on whether a court will determine that the communication was made predominantly for the purpose of seeking legal advice. But "the mere fact that a document is created by a non-attorney is not dispositive of the privilege question, so long as the communication of the document to counsel was confidential and for the primary purpose of seeking legal advice."[53] Thus, whether

50. *See, e.g.*, Picard Chem. Inc. Profit Sharing Plan v. Perrigo Co., 951 F. Supp. 679, 689 (W.D. Mich. 1996).

51. *See, e.g.*, Dewitt v. Walgreen Co., No. 4:11-CV-00263-BLW, 2012 WL 3837764, at *6 (D. Idaho Sept. 4, 2012).

52. *See, e.g.*, Stevens v. Corelogic, Inc., No. 14CV1158 BAS (JLB), 2016 WL 397936, at *4 (S.D. Cal. Feb. 2, 2016).

53. United States v. ISS Marine Servs., Inc., 905 F. Supp.2d 121, 128–29 (D.D.C. 2012) (citing *In re* Grand Jury (Attorney–Client Privilege), 527 F.3d 200, 201 (D.C. Cir. 2008) ("Attorney-client privilege applies to a document a

the communicator is an attorney, or a member of the security team, or otherwise from the business, should not affect the ultimate decision of whether privilege applies, as long as the communication was made predominantly for the purpose of seeking or providing legal advice. However, some courts apply additional scrutiny to communications between in-house (as opposed to outside) counsel and corporate employees to determine whether such communications were made predominantly for a legal as opposed to a business purpose.[54] By contrast, under the general tenets of attorney-client privilege law, communications from "outside counsel are presumed to be made for the purpose of providing legal advice."[55] Thus, communications from in-house counsel may be less likely to be considered privileged, particularly with respect to security assessments, audits, and reports that have a dual purpose.

iii. Among or Within Privileged Persons

To be privileged, the communication must also be among or within privileged persons. To the extent an employee of the client sent or received the communication, the employee must qualify as part of the client under either the subject-matter or control-group tests described in Part B above. If not—for

client transfers to his attorney 'for the purpose of obtaining legal advice.'" (quoting Fisher v. United States, 425 U.S. 391, 404–5 (1976))).

54. *See* United States v. ChevronTexaco Corp., 241 F. Supp.2d 1065, 1076 (N.D. Cal. 2002) ("[U]nlike outside counsel, in-house attorneys can serve multiple functions within the corporation. In-house counsel may be involved intimately in the corporation's day to day business activities and frequently serve as integral players in business decisions or activities. Accordingly, communications involving in-house counsel might well pertain to business rather than legal matters. The privilege does not protect an attorney's business advice.").

55. *Id.* (emphasis omitted).

instance, because the communication was by a front-line IT analyst outside of the "control group" in a control-group jurisdiction—the privilege generally will not apply.[56]

Also, courts will scrutinize communications with outside experts or consultants by an organization or outside counsel to determine whether the use of the third-party expert was necessary for the provision of the legal advice, or whether the consultant was a functional equivalent of a corporate employee. If either is true, courts may extend the attorney-client privilege to cover these experts and consultants.

In 1961, the U.S. Court of Appeals for the Second Circuit decided *United States v. Kovel*,[57] in which it considered whether communications with an accountant prevented attorney-client privilege protection. *Kovel* held that if the accountant (or other third party) was necessary to "interpret" a client's "complicated tax story to the lawyer" to enable the lawyer to represent the client, the accountant did not destroy the privilege between the lawyer and his client. Courts following *Kovel* have extended the doctrine to allow the attorney-client privilege to cover communications to and from other, non-accountant third-party experts and consultants in some circumstances as long as the communications were necessary to assist the lawyer in communicating with the client. Typically, communications with experts in the course of an engagement will not be considered privileged if (1) the communications were not necessary to assist the attorney in understanding communications from the client, or (2) the

56. *See, e.g.*, Valenti v. Rigolin, 1:01-cv-05914, 2002 WL 31415770, at *3 (N.D. Ill. Oct. 25, 2002) (statement by nurse to employer's counsel not privileged because nurse was outside the control group).

57. 296 F.2d 918, 922–23 (2d Cir. 1961).

consultant's expertise was used to make a business decision, rather than to assist the lawyers in communicating legal advice.[58]

The attorney-client privilege may also extend to third parties acting as agents of the client, rather than as an agent of the lawyer as under *Kovel*, although it is more limited. The functional-equivalent doctrine will apply when a third party is retained by a company and is intended to, and does, function as an employee.[59] To determine whether such a third party functions as an employee, courts will look to whether the third party was an integrated member of the company, whether he or she played a significant role in the company, and whether he or she was intimately involved in the creation, development, and implementation of information at issue in the privilege determination and/or the relevant project.[60]

If a third party creates pre-incident CI, then it is possible that technical inventories, configuration reviews, penetration tests,

---

58. *See, e.g.*, Scott v. Chipotle Mexican Grill, 94 F. Supp.3d 585, 590-91 (S.D.N.Y. 2015) (finding that a human relations consultant's report provided to counsel concerning classification of its employees by title was not protected under the *Kovel* doctrine because the consultant engaged in factual research to assist in making a business decision); Church & Dwight Co. Inc. v. SPD Swiss Precision Diagnostics, GmbH, No. 14-cv-585, 2014 WL 7238354, at *2 (S.D.N.Y. Dec. 19, 2014) (holding that a lawyer's communications with an outside marketing firm were not protected from disclosure under *Kovel* in the context of launching a new product inside a complex regulatory scheme, because the expert was not necessary for lawyers to understand communications from the client, and the lawyers could get the necessary expertise without revealing privileged information).

59. *See, e.g.*, *In re* Flonase Antitrust Litig., 879 F. Supp.2d 454, 458 (E.D. Pa. 2012); *In re* Copper Mkt. Antitrust Litig., 200 F.R.D. 213, 220 n.4 (S.D.N.Y. 2001); *In re* Myers, No. 11-61426, 2013 WL 6092447, at *2 (Bankr. N.D. Ohio Nov. 18, 2013) (information provided to attorney by attorney-hired accountant, as agent for the client, held subject to the attorney-client privilege).

60. *See, e.g.*, *In re Flonase*, 879 F. Supp. 2d at 454.

and other pre-incident CI may be considered privileged if they were created for the purpose of aiding counsel in providing an assessment or report to the client. In *In re Arby's Restaurant Group, Inc. Data Security Litigation*, the court held that communications between a technical consultant and counsel, which had occurred prior to the discovery of the company's security incident, were protected by the attorney-client privilege where the consultant's role had been to assist counsel in connection with a "gap analysis" concerning the company's compliance with the PCI DSS.[61] In a decision concerning post-incident CI, *Genesco Inc. v. Visa, Inc.*, the court found that an assessment performed on the client's behalf, which suggested remediation measures, was attorney-client privileged because the expert was "retained . . . to provide consulting and technical services so as to assist counsel in rendering legal advice."[62] While this concerned post-incident CI, the logic appears to apply equally to pre-incident CI.

Therefore, the structure and purpose of outside vendor engagement are factors used by courts to determine whether the attorney-client privilege applies. Pre-incident CI created by third parties may more likely be considered privileged if outside counsel retains the expert and provides clear instructions in the engagement letter that the expert has been retained to assist counsel in providing legal advice. It may also be more likely to be considered privileged if counsel oversees the expert and participates in communications between the client and the expert. Finally, in determining whether a third party's communications were made to assist counsel in providing legal advice, courts have evaluated whether counsel in fact reviewed, and provided

61. Order, No. 1:17-cv-00514 (N.D. Ga. Mar. 25, 2019).

62. Case No. 3:13-cv-00202, 2015 WL 13376284, at *1 (M.D. Tenn. Mar. 25, 2015).

legal advice based on, the observations and findings by the expert.[63]

iv. Reasonable Expectation the Communication Will Be Kept Confidential

As noted in Part B above, to be privileged, the communication must have been made in confidence, i.e., with the intent that it be kept confidential. If CI is created for the purpose of being shared with a third party outside the circle of privileged persons—for instance, a description of IT inventory prepared for distribution to an assessor not working for the company's counsel—the communication will not have the requisite confidentiality, and the privilege will not attach.[64] Once a communication is privileged, the question of whether further disclosure of the communication would destroy the privilege is an issue of waiver, addressed in subsection 3 below.

c. Application of Work-Product Protection to Pre-Incident CI

As discussed in Part B, the work-product protection doctrine applies only to documents created "in anticipation of litigation." Although the application of this doctrine varies somewhat across states and jurisdictions, the requirement for the organization to perceive a real threat of litigation, rather than merely speculate that sometime in the distant future there might be litigation, will typically result in no work-product protection being afforded to any of the above types of pre-incident CI.

---

63. *See, e.g.*, United States v. Lockheed Martin Corp., 995 F. Supp. 1460, 1464 (M.D. Fla. 1998).

64. *See, e.g.*, *In re* Grand Jury Proceedings, 33 F.3d 342, 353-54 (4th Cir. 1994) (communication intended for public disclosure not privileged).

2. *Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work-Product Protection to Post-Incident CI*

In addition to CI created prior to the discovery of a security incident, several types of documents may be created following discovery of a security incident that an organization may consider or want to have considered protected by the attorney-client privilege or the work-product protection.

a. Examples of Post-Incident CI

i. Forensic Investigations—Documents and Reports

These documents include forensic investigations into the security incident, the vulnerability exploited, how it was exploited, what evidence of the incident is available, and what information may have been compromised. These forensic investigations are done by a forensic expert and may be conducted through in-house or outside counsel, but may also be commissioned by the organization's internal security team.

ii. Post-Incident Security Assessments

Organizations may also conduct, through a security expert, outside counsel, or both, a post-incident assessment into the organization's cybersecurity posture. This assessment could span far more of the organization's data infrastructure and security readiness than what would be necessary to determine the reasons for the security incident at issue. Some assessments, however, are narrowly tailored to a particular aspect of the organization's security posture associated with an incident.

iii. Remediation Efforts and Crisis Management[65]

In all post-incident scenarios, organizations will have some documents related to their efforts to remediate the incident that were generated by the security or technology team. There may also be communications about the incident, including internal communications with legal counsel, senior executives, human resources personnel, communications staff, boards of directors, and other portions of the organization, including with respect to: remediation, fact-finding, escalation, whether to notify various entities and individuals, how to notify and what to include in the notifications, and any legal analyses of such incident (including but not limited to litigation and regulatory risk and, for public companies, whether disclosure is required to the SEC). These same types of communications may occur not only internally, but also with outside counsel and public relations consultants, among others. Entities suffering a security incident may also consider whether they should or need to notify an insurance carrier or contractual third party whose systems or data may have been involved in the incident.

* * *

As discussed below, in trying to determine whether documents falling in the above categories should be considered attorney-client privileged and/or work-product protected, and what practices may affect that determination, a few cases involving post-incident CI provide some guidance. In the world of post-incident CI, courts faced with privilege and protection issues have been attempting to apply general legal principles to

65. Whether legally required notifications or communications with law enforcement, state attorneys' general, and other governmental entities will waive the privilege is discussed below, even though interaction with law enforcement is often done during and as part of the remediation efforts and crisis management.

these unique sets of documents. These fact-intensive decisions (as with most attorney-client privilege and work-product protection cases) will turn on a court's decision as to whether the communication was made to solicit or render legal advice or in anticipation of litigation.

b. Application of Attorney-Client Privilege to Post-Incident CI

In the context of post-incident CI, courts have begun to grapple with applying general principles of attorney-client privilege, but the case law is in its relative infancy. Few cases directly address these issues, but the ones that do provide invaluable guidance, even though they do not always clearly distinguish between the type of protection being applied or the exact purpose for which it is or is not being applied in any given circumstance. For example, when attempting to determine whether the report of a forensic expert is protected (by either the attorney-client privilege or the work-product protection), courts may not distinguish between whether the report was commissioned by an attorney "for the purpose of providing legal advice" (attorney-client privilege) or whether the report was drafted in a certain way "because of anticipated litigation" (work-product protection). For purposes of this Part of the *Commentary*, we have attempted to distinguish between the attorney-client privilege and the work-product protection where possible, noting along the way the ambiguities in the existing case law.

i. For the Predominant Purpose of Obtaining Legal Advice from a Lawyer

As with pre-incident CI, whether the predominant purpose of the CI in question was to provide legal advice, as opposed to serving a business purpose, is likely to become a prevalent inquiry in deciding whether certain post-incident CI is privileged.

This especially may be the case when in-house counsel is communicating internally with the organization directly following the incident. For example, questions may arise regarding whether the in-house counsel is merely trying to remedy the breach or is providing legal advice concerning how to manage breach notifications or legal risk. The communications may have a dual purpose to both assist in breach remediation *and* breach notification management or legal risk analysis, in which case the courts will determine the predominant purpose of the communications.

In *In re Target Corp. Customer Data Security Breach Litigation*, the court examined whether various types of post-incident CI were protected by the attorney-client privilege.[66] The court analyzed whether the privilege applied to CI relating to a data-breach task force established by Target in response to the data breach.[67] Plaintiffs' counsel argued that the communications and documents were not protected by the attorney-client privilege because "'Target would have had to investigate and fix the data breach regardless of any litigation, to appease its customers and ensure continued sales, discover its vulnerabilities, and protect itself against future breaches.'"[68] Target argued that those communications and documents were protected because the task force was established at the request of its lawyers (both in-house and retained) to educate counsel about the breach and allow counsel to provide Target legal advice.[69] While the court did not specifically weigh the business and legal purpose of various CI, it did determine that some internal communications were

66. 2015 WL 6777384 (D. Minn. Oct. 23, 2015).

67. *Id.* at *1.

68. *Id.* (quoting Pls.' Letter Br. 3–4).

69. *Id.*

privileged, while others were not, by discussing the purpose of the communications. Specifically, the court found that internal communications from Target's CEO to the Board of Directors were not privileged because they did not "involve any confidential communications between attorney and client, contain requests for or discussion necessary to obtain legal advice, nor include the provision of legal advice."[70] Conversely, the court did find that other communications with and documents created by the task force were privileged, as Target had demonstrated that the task force "was focused not on remediation of the breach, . . . but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice."[71] The court also found other email communications between in-house counsel and other Target employees privileged because they were made for the purpose of obtaining legal advice.[72] Evident in the court's determination is a consideration specifically regarding whether the communications and documents were created for the predominant purpose of providing or obtaining legal advice.

The District of Oregon, in *In re Premera Blue Cross Customer Data Security Breach Litigation (Premera I)*,[73] had opportunity to do the same. Similar to the court in *Target*, the *Premera* court engaged in a detailed analysis of whether CI was created for the primary purpose of informing counsel so that counsel could provide legal advice. The court evaluated the purpose behind CI created by non-attorneys that "incorporated" advice of counsel but were not sent to counsel, and CI created by employees

70. *Id.* at *2.

71. *Id.* at *3.

72. *Id.*

73. 296 F. Supp.3d 1230 (D. Or. 2017) [hereinafter *Premera I*].

"supervised" by counsel.[74] The court examined whether the CI was prepared primarily to assist counsel in providing legal advice, or whether the CI was prepared by the business to fulfill a business function, or required to be prepared by the business in response to the data breach, such as press releases, media interactions, and notices to consumers.[75] Generally, the court found that this CI was created for business purposes, not legal ones.[76] However, attorney redlines or edits communicating legal advice would be covered by the attorney-client privilege.[77]

Subsequently, in *Premera II*, the District of Oregon assessed the application of the attorney-client privilege to CI that was sent to and from counsel, as well as CI prepared at the request of counsel. The court stated that in order to qualify for the attorney-client privilege, emails sent to and from counsel about matters such as press coverage, notices to consumers, and remediation must request or provide legal advice (as opposed to containing merely a factual discussion), or they must contain facts transmitted to counsel so that counsel can provide adequate legal representation.[78] The court further stated that draft documents (e.g., draft notices) prepared by attorneys, at the request of attorneys, or by company employees or vendors and sent to or from attorneys for legal advice relating to the drafts are likely subject to the attorney-client privilege.[79] However, in the court's view, a draft document that is prepared for a business purpose and merely sent to an attorney for the attorney's

74. *Id.* at 1240–47.

75. *Id.*

76. *Id.*

77. *Id.* at 1242, 1250.

78. 329 F.R.D. 656, 662–66 (D. Or. 2019).

79. *Id.*

file or information, or is distributed among company employees or to third-party vendors for general discussion with an attorney merely copied, is not privileged merely because an attorney received it.[80] The court further held that Premera's "investigation into the breach was conducted primarily for a business purpose."[81] But if an attorney took the information from these documents and drafted a different document in preparation for litigation, and/or received emails or draft reports seeking the attorney's advice, those documents would be protected.[82] And the court allowed that CI relating to Premera's later actions in response to the breach may also be privileged: "Other than the initial business steps of remediation, notifying customers, and making public statements, which Premera would have had to do regardless, the later actions by Premera were likely guided by advice of counsel and concerns about potential liability."[83]

ii. Among or Within Privileged Persons

Courts conduct a similar analysis with respect to CI created by third parties. In *Genesco*,[84] Genesco brought suit against Visa in response to Visa's attempt to assess more than $13 million in fines and assessments for Genesco's alleged failure to comply with Visa's cybersecurity standards. Visa had assessed the fines and assessments in response to a breach of Genesco's network that exposed credit card data.[85] Genesco retained a forensic investigator, Stroz Friedberg, to provide consulting and technical

80. *Id.*

81. *Id.* at 666.

82. *Id.* at 666–67.

83. *Id.*

84. Genesco, Inc. v. Visa U.S.A., Inc., 302 F.R.D. 168, 170 (M.D. Tenn. 2014).

85. *Id.*

services to Genesco's in-house and outside counsel regarding the breach and its own cybersecurity posture, as well as with respect to a report issued by a forensic investigator authorized by the Payment Card Industry Security Standards Council, Trustwave International Security and Compliance (Trustwave).[86] Genesco provided evidence that it retained Stroz Friedberg, through outside counsel, specifically to conduct an investigation, under privilege, following the earlier investigation by Trustwave, to assist Genesco's attorneys in providing it legal advice.[87]

In these circumstances, the court, relying on *Kovel*, found that the documents and communications generated by the forensic expert were protected by the attorney-client privilege because the expert was "retained by counsel for the purpose of providing legal advice."[88] The court noted that the privilege extended to Stroz Friedberg because the firm "assisted counsel in his investigation."[89] The court also found, separately, but relying on its earlier ruling, that the privilege applied to documents and communications with IBM, which was retained to provide advice concerning remediation, because it was also hired to assist counsel in rendering legal advice to Genesco.[90]

---

86. *Id.* at 169.

87. *Id.* at 180–81.

88. *Id.* at 190 (citing United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961)). As noted above, it is unclear from the decision how important the retention of the third party was to the determination that the privilege applied.

89. *Id.*

90. Genesco, Inc. v. Visa USA, Inc., Case No. 3:13-cv-00202, 2015 WL 13376284, at *1 (M.D. Tenn. Mar. 25, 2015).

The court also addressed the privilege issues associated with third-party consultants in the *Target* case.[91] In that case, Target had hired a consultant firm to conduct two investigations following its breach. One investigation was conducted by Target's outside counsel, which hired the expert to provide the attorneys information about the breach and how to defend Target; the other investigation was conducted by the consultant firm "on behalf of several credit card brands" to assist in determining how the breach happened and how to remediate.[92] While the two investigations were being conducted by the same outside technical firm, the consultant set up two separate teams that did not communicate with one another.[93] At issue in the action was whether the documents created by and communications with the consultant team hired by outside counsel were privileged and protected from disclosure.[94]

The court found that the documents associated with the team of experts retained by outside counsel were protected by the attorney-client privilege because the investigation "was focused not on remediation of the breach, . . . but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice."[95]

91. *In re* Target Corp. Customer Data Security Breach Litigation, MDL No. 14–2522 (PAM/JJK), 2015 WL 6777384, at *1 (D. Minn. Oct. 23, 2015).

92. *Id.*

93. *Id.*

94. *Id.*

95. *Id.* at *3.

Similarly, the *Premera* decisions evaluated whether CI created by a third-party public relations firm[96] to inform counsel and by a third-party forensic investigator prior to and after the discovery of the breach was protected by the attorney-client privilege.[97] Relying on the primary purpose of the third party, the *Premera I* court generally found that CI created by an attorney-hired public relations firm following the breach (and communications between the firm and Premera) was not privileged. The court relied on the business nature and function of the public relations firm and denied the ability of companies to cloak CI in privilege merely by claiming such CI was created on behalf of an attorney or under the supervision of an attorney. Likewise, the court in *Premera II* held that merely sending such CI to counsel did not make it privileged.[98] The court held in *Premera I and II*, however, that if communications were sent to or from counsel seeking or providing actual legal advice, such as about possible legal consequences of proposed text or an action being contemplated by Premera, then such communications would be privileged.[99]

In connection with the third-party forensic investigator, two sets of CI were at issue: (1) CI created by the investigator prior to discovery of the breach, when the investigator had been hired by the company; and (2) CI, including at least one forensic report, created by the investigator after the discovery of the breach, after being hired by counsel, and after entering into a

96. The court conducted a similar analysis with respect to eDiscovery and other vendors hired by Premera. *Premera I*, 296 F. Supp.3d 1230, 1240–47 (D. Or. 2017).

97. *Id.*

98. *Premera II*, 329 F.R.D. 656, 663 (D. Or. 2019).

99. *Premera I*, 296 F. Supp.3d at 1240–47; *Premera II*, 329 F.R.D. at 662.

new and separate statement of work.[100] The court summarily rejected the notion that simply because the forensic investigator was hired by counsel after discovery of the breach, documents and communications relating to that investigator would necessarily be covered by the attorney-client privilege.[101] Largely relying on the fact that the company had initially hired the forensic investigator for business purposes prior to discovery of the breach, the court found that Premera would have "the burden of showing that [the forensic investigator] changed the nature of its investigation at the instruction of outside counsel and that [the forensic investigator's] scope of work and purpose became different in anticipation of litigation versus the business purpose [the forensic investigator] was performing when it was engaged by Premera before the involvement of outside counsel."[102] The court held, however, that if there were specific documents or portions of documents relating to the investigator that were prepared for the purpose of communicating with an attorney for the provision of legal advice, those particular documents could be withheld as attorney-client privileged.[103]

In *Arby's*, the court held that the attorney-client privilege protected the final and interim analyses of a cybersecurity consultant retained in the wake of the company's cybersecurity incident.[104] The court reasoned that the company had hired the consultant "to produce a report in anticipation of litigation and for other legal purposes," and therefore the consultant's

100. *Premera I,* 296 F. Supp.3d at 1240–47.

101. *Id.*

102. *Id.*

103. *Id.*

104. *In re* Arby's Restaurant Group, Inc. Data Sec. Litig., No. 1:17-cv-00514, at 1–3 (N.D. Ga. Mar. 25, 2019).

analyses were "privileged attorney-client communications between [the consultant] and counsel."[105]

And in *New Albertson's, Inc. v. MasterCard International*, the court likewise held that certain work that two companies commissioned from a forensic investigator following a cybersecurity breach the companies had suffered was protected by the attorney-client privilege, because the work was done principally for a legal purpose.[106] The court observed that while one of the companies had initially engaged the investigator directly (not through counsel), that changed when the company learned a new and material fact about the cybersecurity breach.[107] At that point, the company engaged outside counsel experienced in data breach cases for the purpose of assisting it in conducting an investigation, and the outside counsel then entered into a new engagement with, and began directing the work of, the investigator with knowledge of the likelihood that litigation would result from the security breach.[108] Both companies then entered into a common interest agreement documenting their common legal interest in connection with the security breach, permitting them to share information with each other without waiving the privilege.[109] This joint work with the forensic investigator under the direction of outside counsel, the court held, was protected by the attorney client privilege.[110]

---

105. *Id.*

106. No. 01-17-04410, slip op. at 6 (Idaho 4th Dist. Ct., Ada Cty., May 31, 2019).

107. *Id.* at 6-7.

108. *Id.*

109. *Id.*

110. *Id.*

Based upon the *Target*, *Genesco*, *Premera*, *Arby's*, and *New Albertson's* decisions, it appears courts that face attorney-client privilege claims as to post-incident CI will employ the generally applicable principle of focusing on the predominant purpose of the CI in question to make such privilege determinations—that is, whether the documents and communications were created or solicited predominantly for the purpose of aiding the lawyer in providing legal advice, including not only those created by forensic experts, but also by non-forensic investigator experts like public relations consultants.[111]

In this regard, courts will likely look to who retained the service provider as evidence of the purpose of, and hence whether to apply the privilege to, the CI at issue. Courts may be more likely to find a service provider was primarily retained to assist a lawyer in providing legal advice if such provider was retained by counsel, as the *Target*, *New Albertson's*, and *Genesco* courts noted that the expert was retained by counsel in making the determination that the CI at issue was privileged. While not noted by the court in *Arby's*, *Target*, and *Genesco*, courts may also look to the extent to which the agreement with the expert provided that documents/communications generated as part of the engagement will be kept confidential, the extent to which the lawyer actually relied upon the report and documents of the provider, and, as specifically highlighted by the court in *New*

111. *See, e.g.*, H.W. Carter & Sons, Inc. v. William Carter Co., No. 95 CIV. 1274, 1995 WL 301351, at *3 (S.D.N.Y. May 16, 1995) (finding the public relations consultants assisted the lawyers in rendering legal advice, which included how to respond to a lawsuit, and thus information was protected under the *Kovel* doctrine).

Albertson's, the extent to which the lawyer supervised the outside consultant.[112]

c. Application of Work-Product Protection to Post-Incident CI

Similarly, courts have already given some indication of whether and when post-incident CI will be protected under the work-product doctrine. As noted above, the discussion of whether the predominant purpose of a document or communication was to provide or obtain legal advice often melds into the discussion of whether a document or communication was created because of anticipated litigation, as these analyses are similar. The court often will rely on both the privilege and work-product protection, or find that neither applies, as discussed below.

i. Because of Anticipated Litigation

Courts dealing with work-product protection claims that are made as to post-incident CI have examined carefully whether the post-incident CI in question was created "because of" anticipated litigation, as is required for work-product protection. For example, the *Target* court found that communications from Target's CEO to the Board of Directors did not qualify for work-product protection because nothing showed that the update to

112. Contrarily, however, the court in *Premera I* used the fact that the attorney hired the public relations firm as evidence that the firm was not acting as the company's in-house public relations firm (entitling it to step into the shoes of the corporation vis-à-vis counsel), but rather was outside of that relationship and was advising both the company and counsel separately. *Premera I*, 296 F. Supp.3d 1230 (D. Or. 2017).

the Board was made *because of* any anticipated litigation.[113] However, as with respect to the application of the attorney-client privilege in that case, the court found that the documents created by and communications with the data-breach task force were protected by the work-product doctrine.[114] The court found those documents were created to "prepare to defend the company in litigation that was already pending and was reasonably expected to follow."[115]

A California federal court has similarly examined whether post-incident CI was prepared "because of" anticipated litigation in *In re Experian Data Breach Litigation*.[116] That court found that the question is whether the totality of the circumstances suggests that the document "'was created because of anticipated litigation, and would not have been created in substantially similar form but for the prospect of that litigation.'"[117] The court examined whether a report drafted by an outside forensic investigator was drafted "because of" anticipated litigation, focusing on whether the report was more relevant to the internal investigation and remediation of the incident, or to the defense of the litigation.[118] In making its determination, the court relied in part on the fact that the full report was shared only with the legal

113. *In re* Target Corp. Customer Data Security Breach Litig., MDL No. 14–2522 (PAM/JJK), 2015 WL 6777384, at *3 (D. Minn. Oct. 23, 2015).

114. *Id.*

115. *Id.*

116. *See* Order Denying Motion to Compel Production of Documents, *In re* Experian Data Breach Litigation, No. SACV 15-01592 AG (DFMx) (C.D. Cal. May 18, 2017).

117. *Id.* at 2 (quoting *In re* Grand Jury Subpoena (Mark Torf/Torf Envtl. Mgmt.), 357 F.3d 900, 907 (9th Cir. 2004)).

118. *Id.* at 3–4.

team (as opposed to the entire incident response team).[119] The court reasoned that the report would have been given in full to the incident response team if it "was more relevant to Experian's internal investigation or remediation efforts, as opposed to being relevant to defense of this litigation."[120]

In *Genesco*, the court also examined whether documents created by and communications with third-party experts were protected by the work-product doctrine.[121] Citing *United States v. Nobles*, the court found this post-incident CI squarely within the doctrine because the investigator was counsel's agent and was working under counsel's direction to prepare for litigation.[122]

Likewise, in *Arby's*, the court found that a third-party consultant's post-incident final and interim analyses of a data breach were subject to the work-product protection because the consultant was hired "in anticipation of litigation."[123]

And in *New Albertson's*, the court held that certain work that two companies commissioned from a forensic investigator following a cybersecurity breach the companies had suffered was subject to the work-product protection.[124] The court observed that while one of the companies had initially engaged the investigator directly (not through counsel), that changed when the company learned a new and material fact about the

119. *Id.*

120. *Id.*

121. Genesco, Inc. v. Visa U.S.A., Inc., 302 F.R.D. 168, 190–91 (M.D. Tenn. 2014).

122. *Id.* at 191.

123. Order, *In re* Arby's Restaurant Group, Inc. Data Sec. Litig., No. 1:17-cv-00514, at 2–3 (N.D. Ga. Mar. 25, 2019).

124. New Albertson's, Inc. v. MasterCard Int'l, No. 01-17-04410, slip op. at 6 (Idaho 4th Dist. Ct., Ada Cty., May 31, 2019).

cybersecurity breach.[125] At that point, the company engaged outside counsel experienced in data breach cases for the purpose of assisting it in conducting an investigation, and the outside counsel then entered into a new engagement with, and began directing the work of, the investigator with knowledge of the likelihood that litigation would result from the security breach.[126] Both companies then entered into a common interest agreement documenting their common legal interest in connection with the security breach, permitting them to share information with each other without waiving the privilege.[127] This joint work with the forensic investigator under the direction of outside counsel, the court held, was subject to the work-product protection.[128]

In *Premera I*, the court stated that if the CI at issue (drafts and CI created by employees and third parties following the breach, including press releases, notices, etc.) had a dual purpose, that CI would be protected by the work-product doctrine if the CI was created "because of" the prospect of litigation.[129] The court rejected the notion that the CI at issue was necessarily created because of litigation, rather than for business reasons, simply because the business functions at issue were directed by attorneys.[130] Rather, the court held that in order to establish that a particular document is subject to work-product protection, Premera must show that the document was prepared

125. *Id.* at 6-7.

126. *Id*.

127. *Id*.

128. *Id*.

129. *Premera I*, 296 F. Supp.3d 1230, 1240–47 (D. Or. 2017).

130. *Id.*

specifically because of anticipated litigation.[131] Likewise, with respect to the third-party investigator, the court relied on the fact that the investigator had not changed its scope or purpose at the direction of outside counsel in finding that Premera had not yet established that the CI relating to the investigator was created because of the anticipated litigation.[132] However, the court noted that if there were specific documents relating to the investigator that were created because of anticipated litigation, Premera could properly withhold them as subject to the work-product protection.

In *Premera II*, the court held that narratives drafted to help prepare responses to regulatory inquiries were entitled to work-product protection insofar as they were prepared for the regulatory inquiry and not a general business purpose.[133] It also held that draft notices and scripts prepared by counsel because of anticipated litigation were protected.[134] However, it stated that a timeline prepared by in-house counsel relating to remediation would not be protected if Premera did not demonstrate that the timeline would have been prepared in substantially different format absent anticipated litigation or regulatory investigations.[135]

Whether post-incident CI is protected by the work-product doctrine may also include an examination of when the documents or information were generated. Often, internal IT or security teams may create documents and engage in communications while trying to determine whether a breach occurred. If no

131. *Id.*

132. *Id.*

133. *Premera II*, 329 F.R.D. 656, 666 (D. Or. 2019).

134. *Id.* at 664.

135. *Id.* at 665.

lawyer is engaged in these communications or consulted and no regulatory investigation or litigation has been contemplated up to that point, courts may be less likely to find that these early documents were created in anticipation of litigation. If a company is contemplating that a security incident may result in an investigation or litigation, and has open lines of communication between first-line responders on the IT or security team and the relevant in-house or external counsel in connection with that contemplated investigation or litigation, the work-product protection is more likely to apply.

A court's determination regarding whether litigation was reasonably anticipated may rely either on language directly in a retainer agreement (as in *Genesco*)[136] or on the fact that litigation, though not yet commenced, has at least been threatened. Courts may also rely on the issuance of a litigation hold, the retention of outside counsel, or documentation that litigation or an investigation may be forthcoming.[137]

Analogous case law—such as the line of decisions concerning how the work-product protection's "anticipation of litigation" requirement applies to a situation in which a company suspects a defect in its product and investigates the defect, its scope, and remedial action—further underscores that courts likely will carefully distinguish between documents prepared

136. Genesco, Inc. v. Visa U.S.A., Inc., 302 F.R.D. 168, 181 (M.D. Tenn. 2014). The retention agreement with the forensic investigator specifically stated that the investigator was being retained "in anticipation of potential litigation and/or legal or regulatory proceedings" and to assist its attorneys in preparing for such litigation and providing legal advice. *Id.*

137. Companies should carefully consider when to issue a litigation hold and ensure that the litigation hold, once issued, is being complied with. The issuance of a litigation hold may have the unintended consequence of triggering notification requirements in some jurisdictions.

because of anticipated litigation and documents prepared for business purposes. For example, in *Adams v. Gateway, Inc.*, concerns about problems with its computers led Gateway to launch an internal investigation headed by an attorney and labeled a "legal investigation."[138] The attorney interfaced with engineers and other technical personnel as part of the investigation, and Gateway attempted to claim that several of the documents related to the investigation were work-product protected on that basis.[139] The court disagreed, finding that while Gateway may have become aware of product performance issues as a result of a litigation, "the investigation had at its core the diagnosis and resolution of potential problems" and was motivated by "Gateway's self-interest as a retailer of computer products."[140] In determining whether specific documents were work-product protected, the court found some of the documents showed "concrete litigation-related preparation" and attorney instructions, whereas others showed "technical efforts and results," not revealing or responsive to litigation concerns.[141] Thus, the court ordered the production of the latter documents.[142]

---

138. *See* Order Granting Motion to Compel, Adams et al. v. Gateway, 2:02-cv-00106, 2003 WL 23787856, at *3 (D. Utah Dec. 30, 2003), ECF No. 136 [hereinafter Adams Order].

139. *Id.* at *5–6.

140. *Id.* at *4.

141. *Id.* at *17.

142. *Id.* at *34, *38. Similarly, in Janicker by Janicker v. George Washington Univ., the District Court of Washington, D.C., found that "[i]f in connection with an accident or an event, a business entity in the ordinary course of business conducts an investigation for its own purposes, the resulting investigative report is producible in civil pretrial discovery." 94 F.R.D. 648, 650 (D.D.C. 1982). The court found that the report was "prepared in the ordinary course of business with the primary motivation being to determine what steps could be taken to prevent any repetition of such a tragedy to protect

Other case law evaluating whether an internal investigation or an internal audit qualifies for work-product protection indicates that courts are not likely to find post-incident CI work-product protected merely because counsel involved in a litigation generated or received the CI in question.[143] This may be

other resident college students and the University's standing in the college community and in recruiting students to attend the institution in the future." *Id*. For additional examples in the defective products' context, *see, e.g.*, Soeder v. Gen. Dynamic Corp., 90 F.R.D. 253, 255 (D. Nev. 1980) (granting plaintiffs' motion to compel in-house report regarding aircraft accident on grounds that "given the equally reasonable desire of Defendant to improve its aircraft products, to protect future pilots and passengers of its aircraft, to guard against adverse publicity in connection with such aircraft crashes, and to promote its own economic interests by improving its prospect for future contracts for the production of said aircraft, it can hardly be said that Defendant's 'in-house' report is not prepared in the ordinary course of business"); Bradley v. Melroe Co., 141 F.R.D. 1 (D.D.C. 1992) (ordering production of files related to incidents involving product); Scott Paper Co. v. Ceilcote Co., Inc., 103 F.R.D. 591, 595–96 (D. Me. 1984) (recognizing the "important but subtle distinction between reports prepared in response to an unfortunate event, that might well lead to litigation, and materials prepared as an aid to litigation" and finding that documents had business purpose of maintaining relationship with plaintiff and avoiding litigation).

143. *In re* Air Crash Disaster at Sioux City, 133 F.R.D. 515, 520 (N.D. Ill. 1990) (documents not work-product protected just "because the ultimate findings of the employees will be conveyed to the attorneys who are in charge of the litigation"); *In re* Kidder Peabody Sec. Litig., 168 F.R.D. 459, 465–66 (S.D.N.Y. 1996) (investigation conducted by outside counsel not protected work product because the investigation would have been undertaken even if litigation had not been filed against the company, noting the situation was "not only with a serious legal problem, but with a major business crisis" and "litigation was not the 'principal,' or dominant, motivator, but rather was, at most, an inducement equivalent in importance to the business necessities that we have already cited"); *see also In re* OM Sec. Litig., 226 F.R.D. 579, 586–87 (N.D. Ohio 2005) (holding that although company correctly anticipated litigation, documents prepared by audit committee and its consultant were not

more true to the extent it involves in-house counsel, as opposed to outside counsel.[144] Courts may be more likely to afford work-product protection to an internal investigation with a dual purpose if the litigation purpose is clear from the particular documents at issue, such as the legal ramifications of the investigation's findings.[145]

Given the case law in both the CI and non-CI scenarios, courts seem likely to scrutinize closely whether CI claimed to be work-product protected was in fact prepared in anticipation of litigation. Such scrutiny may include an examination as to whether counsel had a significant enough role in the preparation of a document as to suggest that it was created "because of" and/or for the "primary purpose of" aiding litigation, and/or whether it would not have been prepared in substantially the same form but for the litigation. If portions of such CI were

---

protected work product because investigation would have been conducted regardless of litigation).

144. *See* United States v. ChevronTexaco Corp., 241 F. Supp. 2d 1065, 1076 (N.D. Cal. 2002) ("[U]nlike outside counsel, in-house attorneys can serve multiple functions within the corporation. In-house counsel may be involved intimately in the corporation's day to day business activities and frequently serve as integral players in business decisions or activities.").

145. *See, e.g*, Adams Order, 2003 WL 23787856, at *21 (D. Utah Dec. 30, 2003) (concluding that email from in-house counsel "noting legal implications" of investigation of product deficiencies qualified as work-product protected); Hallmark Cards, Inc. v. Murley, No. 09-377-CV-W-GAF, 2010 WL 4608678, at *4 (W. Dist. Mo. Nov. 9, 2010) (work-product protection extended to documents created by outside counsel and forensic expert it retained to assess concern that third party had provided client with information misappropriated from former employer).

created in anticipation of litigation and others were not, segregation of these portions may also affect a court's decision.[146]

ii. Substantial Need

As discussed in Part B, work-product protection is not absolute, and courts may order documents and information covered by the work-product protection produced if the requesting party can show a substantial need for the information. The court in the *Target* case specifically addressed whether the work-product protection could be overcome by the "substantial need" exception, but found that plaintiffs did not have a substantial need to discover the work product being withheld because Target had "produced documents and other tangible things, including forensic images, from which Plaintiffs can learn how the data breach occurred and about Target's response to the breach."[147]

The court also addressed the substantial-need issue in *Experian*. In that case, plaintiffs argued that Experian's third-party expert had access to live servers that plaintiffs did not have access to, and therefore plaintiffs had a substantial need to access the work-product protected information.[148] Because Experian refuted that claim and plaintiffs could "get those exact server images and hire their own expert to perform the work,"

146. This may also have unintended consequences of making some portions of the document less likely to be protected by the work-product doctrine but should not impact the attachment of the attorney-client privilege.

147. *In re* Target Corporation Customer Data Security Breach Litigation, 2015 WL 6777384 at *3 (D. Minn. Oct. 23, 2015).

148. Order Denying Motion to Compel Production of Documents at 5, *In re* Experian Data Breach Litigation, No. SACV 15-01592 AG (DFMx), (C.D. Cal. May 18, 2017).

plaintiffs did not meet the substantial-need exception to the work-product protection.[149]

Similarly, the court in *Arby's* rejected plaintiffs' attempt to obtain post-incident CI of a forensic consultant that the court deemed subject to the work-product protection.[150] Although it did not explicitly address the "substantial need" exception by name, the court appears to have implicitly ruled that plaintiffs did not meet the exception, because the court reasoned that the "[p]laintiffs have not shown that [the consultant's] analyses cannot be duplicated should [the plaintiffs] be provided the underlying information used by" the consultant.[151] The court therefore ordered the defendant to provide plaintiffs "with the underlying information used by" the consultant in its investigation.[152]

In *New Albertson's*, the court held that the opposing party failed to demonstrate a substantial need for the work product of the breached companies' investigator because the opposing party's own investigator had already been provided with all of the same data and system access that the breached companies' investigator had.[153] Nor was there any indication that the breached companies were using the work-product protection to shield facts about the breach from being discovered.[154]

These cases indicate that courts likely will not find the substantial-need exception to work-product protection applicable

149. *Id.*

150. Order, *In re* Arby's Restaurant Group, Inc. Data Sec. Litig., No. 1:17-cv-00514, at 2–3 (N.D. Ga. Mar. 25, 2019).

151. *Id*.

152. *Id*.

153. New Albertson's, Inc. v. MasterCard Int'l, No. 17-04410, slip op. at 8–9 (Idaho 4th Dist. Ct., Ada Cty., May 31, 2019).

154. *Id.* at 10–11.

to post-incident CI unless the party seeking to apply the exception can prove that it lacks sufficient information regarding the breach, the investigation, and/or the response to the breach to recreate on its own the work product reflected in the CI in question.

3. Waiver of Attorney-Client Privilege and Work-Product Protection as to CI

Even if a court finds that the attorney-client privilege and/or work-product protection applies to certain CI, it may determine that the company has waived the privilege or protection as to that CI. This could be because the company disclosed the CI to a third party—which could include disclosure to: (1) a regulator (the FTC, the SEC, state attorneys' general, the Office for Civil Rights of the Department of Health and Human Services, etc.) pursuant to statute, an investigative demand, or voluntarily; (2) contract parties whose data or systems may have been impacted during an incident; (3) law enforcement to assist in the investigation seeking to apprehend the criminal attacker; (4) an information-sharing organization; (5) an insurance carrier; (6) an affiliated entity; or (7) other parties involved in the same or similar litigation. A court could even potentially find waiver because company personnel disclosed the CI to others within the company.[155]

155. The Federal Rules of Evidence provide that a federal court may order that disclosure of privileged or protected information in connection with federal court litigation does not constitute a waiver. FED. R. EVID. 502(d). In that event, the privilege or protection is also preserved in other federal or state proceedings. *Id.* However, this provision would not protect CI disclosed outside of or before a federal proceeding has been instituted. *Id.* Accordingly, it would not apply to disclosures outside of litigation to regulators, contract parties, law enforcement, information sharing organizations, insurance carriers, or other third parties.

a. Disclosures to Direct or Indirect Contract Parties

In *Genesco,* the court relied on *In re TJX Cos. Retail Sec. Breach Litig.*[156] in determining that the company's disclosure of brief portions of the counsel-retained forensic expert's report to Visa and the assistance of the forensic expert in creating an annotated response to Visa's forensic report did not constitute a waiver of the attorney-client privilege and work-product protection because the sections of the report containing the privileged information were not disclosed to Visa or any other third parties.[157] And in *Premera II*, the court suggested that whether disclosure of a document to a third-party vendor created a waiver would depend on whether the vendor is providing a "legal" as opposed to "business" service.[158] While neither *Genesco, TJX,* nor *Premera II* clearly distinguished between the test for waiver of the attorney-client privilege and the test for waiver of the work-product doctrine, these tests are in fact very different, with the attorney-client privilege generally being much more readily subject to waiver.[159] That being the case, there may be circumstances in which disclosure of CI to one person will waive the attorney-client privilege, but not the work-product protection, as to that CI in regard to other persons.

b. Disclosures to Internal Company Employees

One example of a situation where such differing results could arise is the disclosure of an attorney-client privileged and work-product protected forensic report, cybersecurity assessment, or other CI to internal company employees. While such a

156. 246 F.R.D. 389 (D. Mass. 2007).

157. Genesco, Inc. v. Visa U.S.A., Inc., 302 F.R.D. 168 (M.D. Tenn. 2014).

158. *Premera II*, 329 F.R.D. 656, 668 (D. Or. 2019).

159. *See* Part B.3 *supra*.

disclosure would *not* result in a waiver of the work-product protection unless a court were to somehow conclude that the employee recipient was likely to turn the report over to an adversary, the disclosure might result in waiver of the attorney-client privilege if the employee recipients did not "need to know" the information in the CI (e.g., where there was no need for the employee to provide feedback to the attorney on the report to facilitate the attorney's legal advice)[160] and/or the recipient employees were outside of the company's "control group."[161] Under either test, courts will likely scrutinize the employee recipients to determine whether their receipt of, for instance, an attorney-client privileged data-breach forensic report results in waiver of the privilege. For example, though an IT analyst may rank far lower on the company hierarchy than a vice president of sales, the IT analyst's role and knowledge may be critical for enabling the company's attorneys to provide legal advice. If so, sharing the forensic report with the IT analyst is unlikely to waive the attorney-client privilege under the widely used subject-matter test. However, insofar as the IT analyst is not considered part of the company's control group, sharing the report may waive the privilege in a control-group jurisdiction like Illinois.

160. As the court noted in Verschoth v. Time Warner, Inc., 2001 WL 286763 at *2 (S.D.N.Y. Mar. 22, 2001), the need to know "must be analyzed from two perspectives: (1) the role in the corporation of the employee or agent who receives the communication; and (2) the nature of the communication, that is, whether it necessarily incorporates legal advice. To the extent that the recipient of the information is a policymaker generally or is responsible for the specific subject matter at issue in a way that depends upon legal advice, then the communication is more likely privileged."

161. *See* Part B.3 *supra*.

c. Disclosures to Law Enforcement

Courts may also eventually need to determine whether, when, and to what extent, protected CI loses its protection by reason of being disclosed to law enforcement in connection with its investigation seeking to apprehend the perpetrator of the incident or to a regulator during its investigation of the breached entity's possible role in the incident. As noted in Part B above, at least one court has held that a "selective waiver" theory may protect a party who discloses information to a governmental entity from losing the attorney-client privilege or work-product protection as to that information as against other entities.[162] However, many courts have rejected this theory, despite the public policy benefits of such a position.[163] Some courts have found that disclosure of information to law enforcement or regulators does not waive otherwise applicable attorney-client and work-product protections, provided that the company entered into a confidentiality or protective order containing appropriate non-waiver and other provisions.[164] Thus, while doing so may

162. *See, e.g.*, Diversified Indus. v. Meredith, 572 F.2d 596, 611 (8th Cir. 1977); *In re* McKesson HBOC, Inc. Secs. Litig., 2005 U.S. Dist. LEXIS 7098, *47 (N.D. Cal. Mar. 31, 2005).

163. *In re* Columbia/HCA Healthcare Corp. Billing Practices Litig., 293 F.3d 289, 307 (6th Cir. 2002) (finding that a party's voluntary disclosure of protected documents to the SEC, even under a confidentiality agreement, constituted a complete waiver of attorney-client and work-product privilege); *see also* Westinghouse Elec. Corp. v. Republic of Phil., 951 F.2d 1414, 1429 (3d Cir. 1991) (determining party's "disclosure of work product to the SEC and to the DOJ waived the work-product doctrine as against all other adversaries" notwithstanding if there was or was not a finding that there was a confidentiality agreement party entered into with government agencies).

164. *Compare In re Columbia/HCA*, 293 F.3d at 303 (declining to apply selective waiver even in instances where the parties enter into confidentiality orders), *with In re* Steinhardt P'ners, L.P., 9 F.3d 230, 236 (2d Cir. 1993)

not necessarily prevent waiver, depending on the court at issue and the circumstances of the disclosure, requiring non-waiver and confidentiality provisions or agreements as a condition to any disclosure of CI to the government may at least increase the likelihood that a court will not find that such disclosure waived, as against other persons, any attorney-client privilege and/or work-product protection to which the disclosed CI might otherwise have been entitled.

d. Disclosures to Information Sharing Organizations

Information sharing of certain aspects of an incident or other vulnerabilities may also be protected via the Cybersecurity Information Sharing Act (CISA) of 2015. CISA provides protections to encourage sharing cyber threat indicators and defensive measures with the federal government, state and local governments, and other companies and private entities. Relevant here, CISA provides that the sharing of information pursuant to CISA does not waive as to other persons any attorney-client privilege or work-production protection to which the information may have been entitled and also protects information shared from Freedom of Information Act (FOIA) disclosure.[165]

(indicating that selective waiver would apply in disclosure to the government as long as a confidentiality agreement existed). *See also, e.g.*, *In re* Qwest Commc'ns Int'l Inc., 450 F.3d 1179, 1195 (10th Cir. 2006). A footnote accompanying documents voluntarily disclosed to a government entity concerning the exemption of such documents from production under the FOIA is not a sufficient confidentiality agreement to attain selective waiver. *See, e.g.*, *In re* Aqua Dots Prod. Liab. Litig., 270 F.R.D. 322, 330 (N.D. Ill. 2010), *aff'd*, 654 F.3d 748 (7th Cir. 2011).

165. CISA requires all personal information to be removed from the disclosure, however, and only protects the disclosure of some information that may not be considered privileged in any case.

e. Common Interest, Joint Defense, and Joint Representation Arguments Against Waiver

Whether the sharing of CI with insurance providers, third parties whose systems or data may be involved in the incident, and/or affiliated entities waives any attorney-client privilege or work-product protection that may otherwise have applied to such CI as against other persons may revolve around a court's determination as to whether the parties have a common interest. If the CI in question otherwise qualifies for protection under the attorney-client privilege or work-product doctrine, courts will typically find that a party sharing information with a person or entity in pursuit of a common legal goal or concerning a matter of mutual legal concern did not waive the privilege/protection by sharing the information.[166] Sharing of CI with third parties may qualify for the joint defense privilege if the contracting parties have a common legal goal, such as to prepare for defense of claims anticipated to be asserted against both entities by consumers or regulators. However, if one of the two parties believes the other is responsible for the incident and the disclosure occurs within the context of a discussion of who is at fault, a common legal goal will not be present. The common interest doctrine may also shield communications between affiliated companies, although a prominent appellate decision held that the so-called "joint representation doctrine"—which prevents waiver of communications between clients who share a common attorney—is a better fit for situations where a single attorney or group of attorneys represents multiple corporate affiliates.[167] A fact-intensive determination will dictate whether a

166. *See, e.g.*, United States v. Evans, 113 F.3d 1457, 1467 (7th Cir. 1997).

167. *In re* Teleglobe Commc'ns Corp., 493 F.3d 345, 370 (3d Cir. 2007) ("Courts typically offer versions of three arguments for not construing the sharing of communications with the corporate family as a waiver: (1) the

common interest exists between an insured and its insurer, as courts do not recognize a blanket privilege between insureds and insurers.[168] Similarly, where the two parties are in other sorts of privity, their contractual relationship may assist or work against a common-interest claim, depending on the nature of the contract and the relationship between the parties.

The court in *Premera I* had the occasion to review whether the disclosure of CI to third parties who were not defendants in the same litigation, but in similar litigations, was shielded by the common-interest doctrine.[169] Noting that generally joint-defense or common-interest parties are subject to the same litigation, the court found that entities in similar litigation to which Premera had disclosed documents would share a sufficient common interest if they were subject to the same data breach, but otherwise would not.[170]

f. Subject-Matter Waiver

Finally, in a situation where disclosure of attorney-client privileged and/or work-product protected CI operates as a waiver of the privilege and/or protection afforded to the *disclosed* CI, the question may then arise whether such disclosure also operates as a waiver of the privilege and/or protection as to

---

members of the corporate family comprise one client; (2) the members of the corporate family are joint clients; and (3) the members of the corporate family are in a community of interest with one another. Of these three rationales, we believe only the second withstands scrutiny.") (internal citations omitted).

168. *See, e.g.*, Linde Thoms Langworthy Kohn & Van Dyke, P.C. v. Resolution Trust Corp., 5 F.3d 1508, 1514–15 (D.C. Cir. 1993); Imperial Corp. of Am. v. Shields, 167 F.R.D. 447, 451 (S.D. Cal. 1995) (a limited common interest exists between an insured and an insurer paying for counsel).

169. *Premera I*, 296 F. Supp.3d 1230, 1247–50 (D. Or. 2017).

170. *Id.*

related *undisclosed* CI, both as to others and as to the recipient of the disclosed CI. Under the general principles discussed in Part B.3 above, whether there is such a "subject-matter waiver" may turn on both the identity of the recipient (e.g., federal government versus private party) and the circumstances surrounding the disclosure.

The court in *Premera I* had occasion to briefly consider whether a disclosure to third parties involved in similar litigation constituted a subject-matter waiver of all related documents. The court declined to find a subject-matter waiver as to all communications relating to the subject matter of the disclosed CI, on the ground that:

> because Premera believed in good faith that it and these entities were subject to the common interest exception to waiver, under the unique circumstances of this case, fairness requires that the waiver of privilege extend only to the communications actually shared among the entities and not to all documents relating to the same subject matter that was addressed in the communications that were shared.[171]

However, the court suggested that, but for this "good faith" exception, a broad subject-matter waiver would have applied.[172]

On the other hand, where attorney-client privileged information is used affirmatively or as a defense, courts have been inclined to hold that such use can operate as a waiver of the privilege in regard to related privileged CI. In *In re United Shore Financial Services, LLC*, the court found a waiver of the privilege

171. *Id.* at 1247–49.

172. *Id*.

in regard to CI created by an investigator because, according to the court, the defendant had used the conclusion of the investigator as a defense in the litigation.[173]

* * *

Having considered how courts have employed and presumably will continue to employ traditional principles of attorney-client privilege and work-product protection to analyze privilege/protection claims in the CI context, the *Commentary* next seeks to address whether such application of traditional principles adequately promotes the policy rationales favoring and disfavoring the discoverability of CI.

173. No. 17-2290, 2018 WL 2283893 (6th Cir. Jan. 3, 2018).

D. THE PATH FORWARD

Because discovery of CI is such a novel issue, it is not surprising that existing law fits imperfectly among many of the issues discussed in the previous Part regarding application of the attorney-client privilege and work-product protection to CI. Accordingly, Section 1 of this Part critically assesses the protections the current regime apparently provides and fails to provide to CI. Section 2 then considers various proposals for adapting existing attorney-client privilege and work-product protection law, or developing entirely new protections, in the CI context, and the tradeoffs those proposals present. We believe the existing regime has significant problems in the CI context that evolution of existing doctrines and/or development of new doctrines could address. First, as discussed in Sections 2.a and 2.b below, we believe the current regime's undesirable chilling effect on conducting frank and pointed analyses of (or even undertaking) various cybersecurity measures, coupled with its undesirable incentive for a data holder to put cybersecurity decision-making largely in the hands of the data holder's lawyers, calls for enacting a qualified—but not an absolute—standalone cybersecurity privilege under which CI would enjoy some measure of protection against discoverability, whether or not lawyers were sufficiently involved in its creation to qualify the CI in question for the attorney-client privilege and/or work-product protection. Second, as discussed in Section 2.c below, because of the significant hazards—including the risk of waiver—for data holders in sharing CI with law enforcement, and the public interest in prompt and complete knowledge about cybersecurity incidents, we propose that state and federal law recognize a "selective waiver" doctrine providing that, under certain specified circumstances, a data holder's disclosure of CI to law enforcement would not waive any privilege that might otherwise be claimed as to that CI in future civil litigation.

1. *A Critical Assessment of the Existing Regime*

An all-things-considered judgment about the merits of existing attorney-client privilege and work-product protection law in the CI context requires a consideration of many factors. These include (in no particular order): (1) the data holder's interests, as a crime victim and potential defendant in future civil litigation and/or regulatory enforcement actions; (2) law enforcement's (and the public's) interest in apprehending the criminal actors and preventing future crimes by the same actors and/or using the same techniques; (3) the privacy interests of individuals whose information has been or might be compromised by the incident; (4) the public's interest in and regulators' responsibility for enforcing the law and ensuring that entities that collect protected information have appropriate incentives to adopt legally required security and privacy protections; and (5) everyone's interest in seeing that justice is done.

These varying interests cut in different and sometimes conflicting ways.

- *Data holders*: Typically, data holders will want a legal regime that prevents forced disclosure of CI to its actual or potential adversaries in a litigation or regulatory enforcement context. Even where it makes sense from a data holder's perspective to share CI with one or more of those adversaries, the data holder will want to make that decision on its own terms, rather than have the law require disclosure.
- *Law enforcement*: The interests of criminal law enforcement tend to favor disclosure of CI, at least to law enforcement. Criminal law enforcement will need some access to CI to find clues about potential wrongdoers, even if

criminal law enforcement is much more interested in misconduct by hackers than misconduct by data holders.

- *The public*: The interests of the public are as varied as the public itself. To some extent, the public whose information is in the hands of data holders may want access to the data holders' CI, to make better decisions about sharing information with the data holder in the future. On the other hand, to the extent data holders will be better able to protect sensitive information if CI is not exposed, the public itself may be protected by having that CI under wraps.
- *Regulators*: A regulator's interest in enforcing the law will almost always argue in favor of more rather than less access to CI. CI contains critical clues about a data holder's legal compliance, and a regulator is practically working blind if it is unable to view that information.
- *Affected individuals*: Similarly, the interests of individuals whose personal information may have been, or may be vulnerable to being, compromised in a cyberattack will almost always argue in favor of more rather than less access to CI. As CI contains critical clues about a data holder's compliance with any potentially applicable legal regime that imposes a cybersecurity duty in regard to personal information, such individuals will want access to CI to evaluate and pursue claims that the data holder violated that duty.

- *Justice*: The legal system is meant to produce just results, which the system tries to accomplish by generally permitting broad discovery of legally relevant facts (suggesting greater access to CI), but then creating an exception that protects attorney-client privileged and work-product protected communications and documents from disclosure (suggesting less access to CI).

Part C shows that whether CI is protected from disclosure under the current regime hinges largely on two broad factors: (1) the type and extent of involvement by attorneys; and (2) the extent to which information was created or procured predominantly for purposes of obtaining legal advice or in anticipation of litigation. This tight focus on the role of attorneys and the connection to legal obligations, and especially litigation, is predictable given that we are discussing a set of protections designed to facilitate candid discussions between attorneys and their clients and to facilitate effective legal representation in an adversary system.

The rigid structure of the rules governing the attorney-client privilege, and even the somewhat more flexible approach that recognizes exceptions to work-product protection, however, largely preclude any balancing of the interest in effective legal representation against the other, similarly significant, interests that cybersecurity litigation implicates. That same rigid structure also ties any expansion or reduction of these protections in the cybersecurity context to a set of concerns that, at best, occasionally and largely incidentally overlap with the important objectives of incentivizing the adoption of robust and resilient cybersecurity measures and protecting all concerned against criminal cyberattacks.

a. Perverse Incentives Created by the Existing Regime

Ideally the rules for disclosure of CI would promote robust cybersecurity practices and policies. Companies should do what they reasonably can to protect information and computer networks, and the law should help them do that.

Given the limited protections against disclosure the existing regime affords to CI, companies may think twice before conducting the type of risk assessments that are essential to proper security, but that they otherwise are not required to do. And even where, after thinking twice, companies decide to do such a risk assessment, the existing regime could have a chilling effect on how frank and pointed the assessment, and the company's response to the assessment, turns out to be. A risk assessment may well reveal shortcomings in the company's security posture. With the law as it stands, an organization could not be reasonably confident that the results of a risk assessment will be protected from disclosure in litigation. These concerns may lead companies to entirely forgo non-legally-required risk assessments, or be less than thorough in creating or responding to risk assessments, both those that are legally required and those that are not. While such behaviors may be desirable and understandable from the perspective of protecting the company against legal exposure created by the risk assessment, they are assuredly undesirable from the perspective of making the company's cybersecurity efforts as efficacious as possible.

The counterargument that the existing CI disclosure regime operates to promote better cybersecurity practices assumes the precise opposite: organizations are more likely to expend sufficient resources and take proactive measures to prevent data breaches because their security planning and implementation processes will be closely scrutinized in litigation if they suffer a breach. Which assumption is correct ultimately is an empirical

question, the answer to which almost certainly will shift over time and likely depends on the relative maturity of an organization's cybersecurity posture.

Risk assessment activities have substantial operational components, because they are intended to create, test, and improve security policies and practices. Distinguishing between the core operational activities and activities arguably conducted for the purpose of seeking legal guidance is the central factor in determining whether and to what extent attorney-client privilege or work-product protection will apply to any given CI.[174] Moreover, pre-incident risk assessment activities typically are not initiated in response to a specific or reasonably foreseeable threat of litigation, which makes extending work-product protection to them next to impossible.

At the same time, these reports, or the information they contain, often are essential to determining whether an organization has taken reasonable measures to protect confidential and personal information. They are highly relevant to the core issues in data-breach litigation and investigations and frequently contain information that would be difficult or impossible for regulatory authorities or litigants to obtain in other ways.

While the example of risk assessments well illustrates the perverse incentives the existing regime creates regarding the creation of CI, those perverse incentives extend to *any* CI that discloses a company's mental impressions, conclusions, opinions, assessments, evaluations, or theories concerning its cybersecurity posture, a cyberattack on the company, or its actual or

174. *See In re* Target Corporation Customer Data Security Breach Litigation, 2015 WL 6777384 at *2 (D. Minn. Oct. 23, 2015) (rejecting claims of attorney client or work-product protection for emails from Target's CEO that "merely update[d] the Board of Directors on what Target's business-related interests were in response to the breach").

potential actions in anticipation of, or in response to, a cyberattack. The more frank and pointed companies are when they generate such CI, the more efficacious their cybersecurity efforts would be expected to be. But the current regime potentially chills companies from generating such frank and pointed CI because, except to the extent attorney-client privilege or work-product protection can validly be claimed as to the CI in question, the current regime allows such CI to be discovered and used against the company in question by regulators and private litigants intent on building a case that the company's cybersecurity efforts were legally insufficient.

Pre-breach activities most clearly illustrate the view that existing privilege and work-product law creates perverse incentives in the CI context. The law punishes companies that fail to engage in everyday risk assessments—a future adversary will surely argue that risk assessments are a bare minimum of adequate security. But then again, the law creates legal risk for companies that engage in routine risk assessments—the results may see the light of day, to the company's detriment. These conflicting incentives emerge directly from the fact that CI protection law and cybersecurity law are motivated by divergent goals.

To be sure, these perverse incentives are not as relevant after a breach. For one thing, responding to a known data breach is always a business imperative and often a legal one, so the perverse incentives are far less likely to result in a "do nothing" approach in the post-breach context than they are in the pre-breach context. Moreover, post-breach CI is frequently generated specifically with the guidance of outside counsel and in anticipation of litigation. Thus, treating the discoverability of post-breach CI under the guise of the influence of lawyers and litigation is at least less unrealistic for post-breach situations. A majority of the few cases in this area confirm this assessment: in the *Arby's, Target, New Albertson's,* and *Genesco* cases, courts protected almost

all the CI in dispute from disclosure based on counsel's involvement in the creation of that CI.[175] *Premera*, however, is a recent important exception that underscores the substantial uncertainty regarding the scope of disclosure protection even in the post-breach context and even where counsel is involved in the creation of the CI in question.[176] Even in the post-breach context, then, the current regime gives companies reason for concern

---

175. *Id.* (denying plaintiffs' motion to compel with respect to all documents except a few post-breach emails updating the Board of Directors on Target's "business related interests . . . in response to the breach"); Genesco, Inc. v. Visa U.S.A., Inc., 302 F.R.D. 168, 194 (2014) (barring discovery of all contested documents except those connected to "remedial measures that Genesco took in response to" the breach); *see also* New Albertson's, Inc. v. MasterCard Int'l, No. 17-04410, slip op. at 11–12 (Idaho 4th Dist. Ct., Ada Cty., May 31, 2019) (denying motion to compel as to all contested information, noting that certain underlying data had already been produced); *In re* Arby's Restaurant Group, Inc. Data Sec. Litig., No. 1:17-cv-00514, at 2–3 (N.D. Ga. Mar. 25, 2019) (denying discovery except as to certain underlying information used by cybersecurity consultants). Moreover, to the extent post-incident CI is not protected by the attorney-client privilege or work-product protection, it may nevertheless in many cases be inadmissible as a "subsequent remediation measure" under Federal Rule of Evidence 407 and its state analogs insofar as it relates to the company's efforts to remediate the breach. *See* FED. R. EVID. 407 ("When measures are taken that would have made an earlier injury or harm less likely to occur, evidence of the subsequent measures is not admissible to prove negligence, culpable conduct, a defect in a product or its design, or a need for a warning or instruction."). This aspect of the existing regime arguably reduces or eliminates whatever disincentive companies otherwise might have to take remediation measures in the wake of a data security incident.

176. *Premera I*, 296 F. Supp.3d 1230 (D. Or. 2017) (rejecting defendant's assertion that several categories of documents, including a forensic investigator's report, prepared post-breach after outside counsel was hired to investigate, were not protected work product because they served a primarily business purpose); *see also Premera II*, 329 F.R.D. 656, 666 (D. Or. 2019) (similar).

that anything and everything they do or say in their breach response efforts can potentially be used against them in a court of law, whether or not a lawyer has guided those efforts. That risk may make companies more circumspect than they otherwise would be about what internal statements they make and what internal actions they take in the course of their breach response efforts, and such circumspection could make those efforts slower and less effective than they otherwise would have been.

The post-breach context sometimes raises another perverse incentive. Ideally the rules for disclosure of CI would promote robust cooperation between the victims of criminal cyberattacks and the criminal law enforcement authorities responsible for investigating such crimes and catching the perpetrators. Yet under the limited protections the existing regime affords against disclosure of attorney-client privileged and work-product protected materials to third parties resulting in a waiver of the privilege or protection as to other third parties, cyberattack victims may be reluctant to disclose privileged or protected CI to law enforcement. Such cyberattack victims may justifiably be concerned that such disclosures will waive as to their actual and potential litigation and regulatory adversaries the privilege/protection that the CI otherwise would have enjoyed. To the extent such concerns result in criminal law enforcement authorities being denied access to CI that would have assisted their efforts to bring cyberattack perpetrators to justice (and/or delaying access while the victim figures out a "workaround" to share the CI without waiving the privilege or protection), the current regime will have operated against, rather than in support of, the goal of promoting robust cooperation between those authorities and the victims of the crimes they are investigating.

b. The Disadvantages of Involving Counsel in Creating CI

Courts addressing the protectability of CI have distinguished between reports developed under the direction of counsel (especially outside counsel) for purposes of legal advice or litigation, and those directed by security professionals. As a result, a consensus is emerging that to the extent that organizations want to shield CI from being discovered in litigation, they should seek to "cloak" all pre- and post-incident cybersecurity work under privilege and/or work-product protection by retaining outside counsel or using inside counsel to hire and direct these efforts.

There are some obvious disadvantages to so closely linking CI protection to attorney involvement. Specifically, the practice raises several practical and analytical problems:

- *Risk That Work Will Not Be Protected*. Even when counsel that is retained to provide legal advice and/or in anticipation of litigation with regard to a company's cybersecurity conducts or commissions the activities that generated the CI in question, the risk remains that those activities will be viewed by a court as primarily operational rather than legal, and therefore the CI is not protected from disclosure (as was the case with respect to several categories of CI in the *Premera* decisions). This risk is heightened in the pre-incident context because, as noted above, the activities that generate CI are not tied to any specific pending or anticipated legal action or investigation. Some have argued that the increasingly pervasive risk of a breach strengthens the case that all security-planning

activities are tied to assessing legal and regulatory risks, but no court has yet embraced that view. Moreover, that view undermines a core premise of both the work-product protection and the attorney-client privilege that courts can and should carefully distinguish between operational activities and legal advice and strategy when applying those doctrines. Routinely involving counsel in more data-security-related activities, especially activities with little or no concrete legal dimension, increases the risk that some or all of the CI generated by such activities will not be protected under either doctrine.

- *Increased Cost*. Involving counsel, in particular outside counsel, in generating CI often increases the costs of the activity in question. Retaining outside counsel incurs fees; involving inside counsel redirects resources.
- *Potential Duplication*. Even where an organization involves counsel to strengthen the case for protection of CI, there inevitably will be some duplication between the operational and legal processes. The dual track process that was used in the *Target* litigation is a prime example.
- *Inappropriate Expertise*. Inside and outside counsel may not always be the best qualified to lead many cybersecurity activities. The internal information-technology personnel or an outside security firm is a more appropriate choice to lead the effort in some instances.

c. The Disadvantages of Depriving Law Enforcement of Access to Privileged/Protected CI

To the extent that data holders withhold from criminal law enforcement authorities attorney-client privileged or work-product protected CI relevant to a cyberattack (or delay providing CI until they can figure out a "workaround" to share the CI without waiving its privilege or protection), law enforcement's efforts to investigate the attack could be significantly hampered. Such CI, either pre- or post-attack, is highly likely to provide detailed insights into the cybersecurity measures the attacked entity had in place, the vulnerabilities in those measures that the attacker exploited, and the data the attacker succeeded in compromising by means of those vulnerabilities. Such insights could be extremely valuable to the authorities investigating the crime and, just as important, quite difficult for those authorities to obtain from any source other than the privileged/protected CI. Depriving authorities of access to that CI, or delaying their access, thus stands to have a substantial negative impact on their investigatory efforts.

d. To What Extent the Current Regime Promotes Relevant Interests

Predictably, when it comes to protecting (or not protecting) CI from disclosure, the interests of data holders, law enforcement, the public, civil regulators, and individuals affected by a cyberattack cut in different and sometimes opposing ways. For data holders, the current regime may create incentives to avoid creating potentially damaging CI[177] that could be used by a

177. For example, often there is a misperception that engaging in a security assessment will be futile at best because it will be too expensive to meaningfully address any security gaps and counterproductive at worst because the assessment itself will provide damaging evidence in potential future

litigation adversary or a regulator to impose liability. Those same risks incentivize structuring information security programs to protect as much information as the current regime allows, even where doing so involves the above-mentioned negatives of incurring the additional cost of retaining counsel, potentially duplicating other information security efforts, and placing leadership of certain information security efforts in the hands of lawyers rather than technologists. At the same time, the relative difficulty of protecting CI created at the pre-breach stage and the still uncertain scope of privilege and work-product protection for even post-breach CI arguably should incentivize robust and proactive security efforts to avoid the heightened risk of liability and minimize the negative effects of disclosure. However, the potential discoverability of CI may discourage companies from conducting assessments of their security posture over and above those that are legally required, and in the post-breach context—where efforts to address the breach are normally a business imperative and often a legal one—the potential discovery of CI may cause companies to be unduly circumspect regarding the internal statements they make and internal actions they take in the course of their breach response efforts, making those efforts slower and less effective than they would have been had the companies not been worried about the chance of their post-breach CI being discovered.

Data holders' and criminal law enforcement authorities' interests, in theory, should largely align. Many data breaches are the result of criminal activity where data holders are the victim and therefore should have an interest in disclosing information

---

litigation. Likewise, some regulators have reported incidents where there is reason to believe that an entity involved in a breach has taken steps to actively avoid documenting the results of a forensic investigation specifically to avoid creating potentially damaging CI.

necessary to identify and apprehend the perpetrator. But the pervasive risk of civil liability and/or penalties imposed by a civil regulator following a security incident, and the risk of privilege waiver, especially the possibility for a broad subject-matter waiver, cuts strongly in favor of strictly limiting the information shared with law enforcement to non-privileged/protected CI and may disincentivize data holders from involving law enforcement at all when a breach occurs. Even where a concern about waiver does not result in withholding attorney-client privileged or work-product protected CI from law enforcement, it sometimes complicates the sharing of such CI. Data holders may request a formal subpoena before sharing such CI, so as to enhance the argument that the disclosure was compulsory and thus did not effect a waiver; data holders also may want to take additional time to separate privileged from non-privileged CI, again so as to reduce the risk of a waiver being found. To the extent law enforcement does not view data holders as adversaries, it may be inclined to allow data holders to take whatever steps appear necessary to protect CI from disclosure to others.

Civil regulators and plaintiffs present still different issues. These parties seek to enforce the law against data holders and therefore are both interested in CI and more likely to have requests for CI rebuffed. Companies, however, may have strategic incentives to disclose otherwise protected CI to regulators in the course of an investigation—for instance, in hopes that their cooperation will bring about a lighter sanction.[178] In addition, through pre-lawsuit subpoenas, civil regulators have tools for seeking CI that are not available to private plaintiffs.

178. *See* Eric J. Gorman and Brooke A. Winterhalter, *Protecting Attorney-Client Privilege and Attorney Work Product While Cooperating with the Government: Strategies to Minimize Risks During Cooperation (Part Two of Three)*, 3:4 CYBERSECURITY LAW REPORT (2017).

Nonetheless, the possibility that a private civil action will accompany an investigation, and the clear risk that disclosure in a regulatory investigation likely will waive privilege and work-product protection, combine to create significant incentives for data holders to resist disclosure of CI to regulators as much as possible.

Private plaintiffs lack the pre-litigation tools of civil regulators in seeking disclosure of CI. As the discussion in Part C explains, if defendants carefully structure post-incident analyses of security incidents, in particular by retaining counsel to direct those processes, they should be able to protect from disclosure much of the CI generated by those post-incident activities. On the flip side, the few decisions analyzing application of attorney-client privilege and work-product protection in this context suggest that courts will carefully distinguish between documents that are intended to assist in providing legal advice and/or preparing for litigation and those that are created for strategic and business purposes. Moreover, most pre-incident documents will be difficult to protect from disclosure, thus giving access to a potentially large amount of CI.

e. The Unique Importance of Cybersecurity and Cybercrime

American businesses and government agencies are under cyberattack twenty-four hours a day, seven days a week, from criminal third parties, and the federal government has declared this global cybercrime wave a compelling national security concern, particularly in the area of critical infrastructure. In this context, any regime regarding the discoverability of CI that creates disincentives for companies to engage in behavior that could enhance their network security, or interferes with law enforcement's efforts to catch the third-party criminals, arguably poses particularly significant threats to the national economy

and public safety. Under this line of argument, broader protections regarding the discoverability of CI are warranted in the cybersecurity context. At the same time, it is arguably more important in the cybersecurity context than in other public protection contexts for regulators and private litigants to be able to obtain companies' documents and communications so that laws governing cybersecurity can be enforced and companies have appropriate incentives to enhance the security of their networks. Under this line of argument, while the current regime's limited protections on the discoverability of a company's documents and communications might be acceptable in the context of enforcing laws as to the physical safety of consumer products, the cleanliness of the environment, and other potential dangers to public health and safety, those limits are not acceptable in the more important context of protecting the public against the economic and intangible (e.g., emotional) injuries people may incur from the misuse of their personal information.

The unique importance of cybersecurity and cybercrime raises the question whether the current regime's limited protections, by means of the attorney-client privilege and work-product protection, on the discoverability of a company's documents and communications, while acceptable in some other contexts, should either be broadened or narrowed in the cybersecurity context. In the section that follows, we assess some proposals under which the current regime might be modified to account for the unique importance of cybersecurity and cybercrime.

2. Proposals for Modifying the Current Regime

As discussed above, the current regime for determining the discoverability of CI makes the creation of CI more expensive for those who seek to ensure it will be protected from disclosure, and chills companies from creating the sort of CI that would be most efficacious in furthering their cybersecurity efforts. At the

same time, in many cases this model puts the creation of such documents in the wrong hands—attorneys know a lot about cybersecurity law, but perhaps not as much about other aspects of cybersecurity. In addition, even where it would be beneficial for law enforcement to view some CI, the current regime makes such disclosure less likely by increasing a data holder's liability exposure when it decides to disclose such information. These disadvantages may pose a greater threat to the public in the cybersecurity context than in other contexts because of the particularly compelling national interests in protecting the networks of American businesses and government agencies, catching cybercriminals, enforcing cybersecurity laws, and thereby protecting members of the public against injuries from the misuse of their personal information. All of these considerations warrant at least some consideration of whether an alternate regime should potentially govern the discoverability of CI.

In spite of the limitations just identified, the existing regime has some clear benefits. Most notably, because it is grounded on relatively settled attorney-client privilege and work-product protection, the current regime provides a fairly predictable framework within which to assess the actions that are likely to lead to documents and communications being protected, or not, from discovery. The various proposals for modifying the existing regime in the CI context discussed here inevitably bring with them uncertainty, simply because there are no precedents explaining precisely how the protection will work in this context.

a. Absolute Stand-Alone Cybersecurity Privilege Rejected

The unique issues that data breaches raise have led some to call for an independent, unqualified cybersecurity privilege as to at least some CI. The basic premise is that cybersecurity

investigations raise a similar set of concerns and require the same kind of confidential relationship that privileges in other contexts protect, such as attorney-client, therapist-patient, and others.[179] As discussed below, the unique mix of interests implicated by the increasing and pervasive risk of a data breach provides several persuasive arguments in favor of recognizing a new privilege in this area. But the conflicting nature of the relevant interests also provides counterarguments in favor of the status quo. At minimum, these conflicting interests counsel against making such a privilege unqualified and instead support careful calibration, including significant qualifications permitting disclosure of some otherwise protected CI under the right circumstances.

The case for an unqualified stand-alone cybersecurity privilege rests on the complex mix of concerns and the issues identified above: (1) the dramatic increase in cybersecurity attacks has created a significant and growing public interest in both preventing data breaches and ensuring prompt discovery and remediation of breaches when they occur; (2) existing privileges, including the attorney-client privilege, fail to adequately protect the full range of documents produced by a robust, proactive cybersecurity program against disclosure in litigation; and (3) the net result creates perverse incentives for organizations to tailor their efforts in ways that will reduce potential disclosure in litigation rather than pursue the most thorough and effective prevention and remediation measures. This situation, combined

179. *See, e.g.*, Jeff Kosseff, *The Cybersecurity Privilege*, 12:2 I/S J.L. & POL'Y FOR INFO. SOC'Y 261 (2016). Koseff develops the most extended argument in favor of an independent privilege for cybersecurity investigations. He proposes that courts should recognize a broad, unqualified privilege for all legal cybersecurity activities under Federal Rule of Evidence 502 or that Congress and state legislatures should do so through statute. *Id.* at 298–303.

with the unique importance of cybersecurity and cybercrime, it can be argued, creates a compelling case for a new privilege that closely tracks the justifications for, and hence the unqualified nature of, other common-law privileges, including the attorney-client privilege.[180]

As noted above, the case for an unqualified cybersecurity privilege is premised on the contestable assumption that the risk of disclosure in litigation creates disincentives for entities to develop robust and effective cybersecurity policies and practices. The opposite view assumes that these incentives align relatively well under the current regime because the substantial risk of disclosure of CI should make organizations more likely to expend sufficient resources and take proactive measures to prevent data breaches, because their security planning and implementation processes will be closely scrutinized in litigation if they suffer a breach. Which assumption is correct ultimately is an empirical question, the answer to which almost certainly will shift over time and likely depends on the relative maturity of an organization's cybersecurity posture.

Equally important, an unqualified cybersecurity privilege would take no account of the offsetting policy considerations just identified, including the data owner's interest in recourse for an entity's failure to take legally required security measures, and the risk that a lack of transparency would substantially frustrate the ability of regulators to enforce existing cybersecurity

180. *Id.* at 285–98. Notably, this article goes on to recognize that an absolute privilege may not be feasible and argues that in such a case "a qualified privilege would be an acceptable starting point." *Id.* at 303. As the author states in the article, while he would prefer an absolute privilege, even a qualified privilege "would help to encourage companies to invest in cybersecurity work and increase the likelihood that the cybersecurity professionals' work product would be protected from discovery. " *Id.*

laws. For these reasons, we believe any proposal for a stand-alone cybersecurity privilege should include qualifications on the privilege, including some restrictions on the CI that could qualify for the privilege, as well as some qualification that would permit opposing parties to obtain protected information under certain circumstances.

b. Proposed Qualified Stand-Alone Cybersecurity Privilege

We believe any stand-alone cybersecurity privilege should include the following features and qualifications:

- Workable standards (and limits) on what CI could qualify for the privilege
- Some ability to require disclosure (at least in a redacted form) of CI that qualifies for the cybersecurity privilege and is not otherwise privileged where a substantial need can be shown by the party seeking disclosure
- Documentation by the party asserting the privilege sufficient for an opposing party and the court to determine the basis for the privilege and to challenge that assertion

The attributes of a qualified stand-alone privilege just described track the kind of qualified protection provided to trial preparation materials by the work-product doctrine. But the existing work-product doctrine is unlikely to extend to the pre-incident context because of the "in anticipation of litigation" requirement. And even in the post-incident context, existing work-product doctrine requires some involvement of a lawyer in the creation of the document or communication in question for the protection to apply, whereas the idea of any stand-alone cybersecurity privilege, be it "broad" or "nuanced," is to

eliminate the protectability of CI being dependent on legal involvement.

Apart from its being limited to materials generated in anticipation of litigation, the work-product doctrine is a better model than the attorney-client privilege for a stand-alone cybersecurity privilege because unlike the attorney-client privilege, a requesting party can access otherwise protected documents where it can demonstrate both (a) substantial need and (b) undue burden in obtaining substantially equivalent information. One approach for developing a qualified stand-alone cybersecurity privilege would be to apply something akin to work-product protection to the CI context by eliminating or softening the work-product doctrine's requirement that materials must be created "in anticipation of litigation;" for instance, by reframing the requirement as "in anticipation of or in response to a cyberattack." This could happen through recognition of the endemic and pervasive risk of cyberattacks that would permit companies to assert protection for pre-incident and post-incident CI or some subset of them regardless of litigation concerns or what involvement lawyers had in creating it.

Having said that, a qualified stand-alone privilege that extended to *all* documents and tangible things prepared in anticipation of or in response to a cyberattack would potentially create a presumptive protection from discovery for any and every document concerning a company's cybersecurity efforts. This would include ordinary-course documents such as computer-generated logs and the results of automated vulnerability and anti-virus scans that do not in and of themselves disclose or reflect the *human* analyses, evaluations, and decisions that the current regime arguably chills and/or weakens. Addressing the concerns created by the current regime does not necessitate affording such ordinary-course documents enhanced protection against discovery. Rather, those concerns can be addressed by

limiting any such enhanced protection to documents and tangible things that reflect a person's (or its representative's) mental impressions, conclusions, opinions, assessments, evaluations, or theories concerning a cyberattack on that person, or the person's actual or potential actions in anticipation of or response to a cyberattack—in much the same way that Federal Rule 26(b)(3)(B) affords enhanced work-product protection to documents reflecting such mental impressions and the like.

Taking all of the foregoing into account, we propose that a qualified stand-alone cybersecurity privilege use the language of Federal Rule 26(b)(3) as a starting point and provide as follows:

> Materials Prepared in Anticipation of or in Response to a Cybersecurity Threat
>
> (A) *Documents and Tangible Things*. Ordinarily, a person may not utilize legal process to compel or require production of documents and tangible things that are prepared in anticipation of or in response to a cybersecurity threat by or for another person or its representative (including the other person's attorney, consultant, surety, indemnitor, insurer, or agent) and that are within the protection from disclosure set forth in Paragraph (B) below. But those materials may be discovered if:
>
> (1) they may otherwise be compelled or required to be produced by means of legal process under applicable law; and
>
> (2) the person seeking production shows it has substantial need for the materials and

cannot, without undue hardship, obtain their substantial equivalent by other means.

(B) *Protection Against Disclosure*. The protection against disclosure created by this rule shall extend only to the mental impressions, conclusions, opinions, assessments, evaluations, or theories of a person or its representative concerning (i) a cybersecurity threat or (ii) that person's actual or potential actions in anticipation of or in response to a cybersecurity threat. A court or other body having appropriate jurisdiction shall uphold a person's refusal under this rule to produce documents and tangible things that are prepared in anticipation of or in response to a cybersecurity threat only to the extent necessary to protect against disclosure of such mental impressions, conclusions, opinions, assessments, evaluations, or theories.

(C) *Information Withheld.* When a person withholds from production otherwise producible information by claiming that the information is subject to protection as material prepared in anticipation of or in response to a cybersecurity threat, the person must:

(1) expressly make the claim; and

(2) describe the nature of the documents or tangible things not produced or disclosed—and do so in a manner that, without revealing the protected information itself, will enable the person seeking production to assess the claim.

> (D) Definitions
>
> (1) "Cybersecurity threat" has the meaning given the term in section 102(5) of the Cybersecurity Information Sharing Act of 2015 (CISA), including the definition of the related term "information system," given in section 102(9) of CISA.[181]

Any stand-alone cybersecurity privilege modeled on the work-product doctrine need not, in our view, include a more

---

181. CISA's definitions fit the scope of activity we intend the qualified privilege to cover and also would allow for judicial interpretations of CISA's definitions to provide relevant authority for interpreting the scope of the privilege. We reproduce the full text of the relevant sections below.

> Section 102(5) CYBERSECURITY THREAT.—
>
> (A) IN GENERAL.—Except as provided in subparagraph (B), the term ''cybersecurity threat'' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.
>
> (B) EXCLUSION.—The term ''cybersecurity threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.
>
> Section 102(9) INFORMATION SYSTEM.—The term ''information system''—
>
> (A) has the meaning given the term in section 3502 of title 44, United States Code; and
>
> (B) includes industrial control systems such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

liberal undue-burden/substantial-need exception than the work-product doctrine's version of that exception. To begin with, much of the CI generated by a company will not fall within the above draft rule's limited presumptive protection against disclosure because it will not disclose a person's mental impressions and the like, and thus will not satisfy the requirements of Paragraph B of the proposed rule. Moreover, while we recognize that some kinds of CI within the draft rule's presumptive protection against disclosure will be essential and difficult to replicate through other evidence, the recent discussion of the undue-burden/substantial-need exception in the *Experian* case illustrates how the equivalent exception under our proposed rule can enable plaintiffs to obtain such CI when necessary.[182] There, the court denied plaintiffs access to the forensic report created by the defendants' outside expert *only* because it recognized that the plaintiffs could readily replicate the report themselves, since the report relied solely on server images that the plaintiffs could obtain in discovery.[183] By contrast, under both the work-product doctrine and the proposed qualified stand-alone cybersecurity privilege, where an organization generates materials that otherwise would be protected by the doctrine/privilege, but an opposing party has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain a substantial equivalent by other means, the party generating the materials could be required to provide that information to the opposing party.

In addition to providing a balanced alternative to an unqualified stand-alone cybersecurity privilege, a qualified stand-

182. *See* Order Denying Motion to Compel Production of Documents, *In re* Experian Data Breach Litigation, No. SACV 15-01592 AG (DFMx), (C.D. Cal. May 18, 2017).

183. *Id.* at 5.

alone cybersecurity privilege modeled on the work-product doctrine could result in parties more selectively asserting the blanket protection of attorney-client privilege to pre- and post-incident CI and would provide courts with a more nuanced set of tools to deal with competing arguments over the application of privilege in the cybersecurity context.

One concern raised in response to the public comment version of this proposal is that courts will need to determine what constitutes a "cybersecurity threat" as well as "mental impressions, conclusions, opinions, assessments, evaluations or theories" of nonlawyers, which could result in ancillary discovery disputes and inconsistent decisions by different courts.[184] As with any new legal rule, it will take some time for parties and courts to ascertain the precise boundaries of the qualified privilege, and disputes inevitably will arise in some instances.

The proposed language deliberately draws on existing legal models to reduce the risk of confusion. Moreover, as we discuss at length above, there already are substantial uncertainties surrounding the application of traditional attorney-client privilege and work-product protection in the cybersecurity context. This privilege could eliminate many of those disputes by providing a clear avenue to protect materials as to which parties otherwise might seek to stretch the boundaries of those doctrines and, thus, has the potential to reduce confusion in the aggregate.

Having said all that, while a qualified stand-alone cybersecurity privilege would provide more limited protection than an unqualified privilege modeled on traditional attorney-client privilege principles, and thereby better address the mix of

184. *See* Matthew Hamilton and Donna Fisher, *Evaluating Stand-Alone Privilege for Cybersecurity Info*, LAW360 (2019), https://www.law360.com/articles/1168625/print?section=technology.

interests implicated in the cybersecurity context, such a privilege would still protect a much greater range of CI from disclosure than does the current regime. The argument in favor of a qualified standalone cybersecurity privilege thus still rests on the contestable proposition that some currently unprotected CI really should be protected, even though it does not qualify for the attorney-client privilege or work-product protection. The new rule also inevitably will invite ancillary disputes regarding the appropriate scope of the protection both as a general matter and in individual cases where parties will take contrary views as to whether particular CI should be protected. Ultimately, then, the argument for even a qualified stand-alone cybersecurity privilege depends on whether concerns about cybersecurity and cybercrime are both unique and substantial enough to justify drawing the protection/non-protection line differently in the cybersecurity and CI context than where the current regime draws that line in all other contexts.

We are persuaded that concerns about cybersecurity and cybercrime are sufficient to justify a qualified stand-alone cybersecurity privilege along the lines of the above draft. The key foundation for this conclusion is our belief that (1) the language of Paragraph (B) of the draft rule would result in most of an organization's CI not even qualifying for the rule's presumptive protection against disclosure in the first place, and (2) the "substantial need" exception to the privilege would prevent the privilege from being used in a fashion that would impose undue hardship on regulators and private litigants in building and bringing cases against the victims of cyberattacks.

The narrow limitations the proposed privilege would impose on the discoverability of relevant CI in such cases are outweighed by the benefits the privilege would achieve. First, the proposed qualified privilege would enable parties to take robust actions to protect themselves against and respond to third-party

cyberattacks with greater (though not absolute) assurance that the CI they generate in the course of those efforts will not be used against them at some point down the road. In our view, affording parties such greater assurance treats the victims of third-party cyberattacks more fairly than does the current regime.

Second, the proposed qualified privilege would enable parties to obtain significant (though not absolute) protection against the discoverability of CI without using attorneys to lead their efforts to protect themselves against, and respond to, third-party cyberattacks. In our view, providing parties with greater discoverability protection lessens the incentive that the current regime creates for putting attorneys in charge of efforts to address being victimized by such criminal activities and/or taking other measures to avoid creating a discoverable record concerning those efforts (such as not conducting certain assessments that are not otherwise legally required, conducting such assessments less thoroughly, or not reducing them to writing). Thus, it lessens the risk that the current regime creates of those efforts being less efficacious and/or more costly than they would otherwise have been.

In this way, the proposed qualified privilege is analogous to the medical peer-review privilege recognized by the vast majority of U.S. states (although generally not by federal common law), which lessens hospitals and physicians' disincentives to thoroughly investigate medical incidents by shielding reports and other documents of their medical staff committees in connection with such investigations from discovery.[185] We recognize that in *University of Pennsylvania v. EEOC*, the U.S. Supreme

185. *See* LEONARD ET AL., THE NEW WIGMORE: A TREATISE ON EVIDENCE § 7.8 (3d ed. 2017).

Court declined to recognize a qualified common-law privilege against the disclosure of confidential university faculty peer-review materials.[186] We also recognize that several lower federal courts have relied on the Court's reasoning in that decision to refuse to recognize an analogous "self-critical analysis" or "self-evaluative" privilege that would protect confidential, nonfactual deliberative material such as opinions or recommendations that result from internal investigations, reviews, or audits conducted by public and private entities.[187]

The limited privilege we propose stands on much different footing than either the faculty peer-review process or the self-critical analysis privilege. The Supreme Court in *University of Pennsylvania* noted that confidentiality is not the norm in all faculty peer-review systems and expressed skepticism that disclosure of faculty peer reviews would actually have a chilling effect on the candidness of such reviews.[188] By contrast, corporations closely safeguard the confidentiality of their candid assessments of their own information security. As noted above, the current regime incentivizes companies to maintain that confidentiality by putting attorneys in charge of their efforts to address being victimized by cyberattacks and/or taking other measures to avoid creating a discoverable record concerning those efforts,

186. 493 U.S. 182 (1990).

187. *See, e.g.*, Lund v. City of Rockford, Case No. 3-17-cv-50035, 2017 WL 5891186 (N.D. Ill. Nov. 29, 2017), at *5–16 (*relying on* Univ. of Pa. v. EEOC , 493 U.S. 182 (1990), to reject the self-critical analysis privilege and surveying the "spotty history" of the privilege in federal court decisions).

188. *Univ. of Pa.*, 493 U.S. at 200–01 (noting that if peer reviews are discoverable, some academics, rather than being less candid, may simply ground their evaluations in specific examples and illustrations in order to deflect potential claims of bias or unfairness).

thereby raising the risk that those efforts will be less efficacious and/or more costly than they would otherwise have been.

The self-critical analysis privilege requires confidentiality and, like our proposal, limits the scope of protection to nonfactual information. Public interest in thorough and candid identification and assessment of potential shortcomings within an organization also justifies both privileges. Despite these similarities, the case for a qualified CI privilege is stronger for two reasons. First, the privilege covers a very narrow and specific situation—a "cybersecurity threat" as defined by CISA—that raises a set of public interests distinct in nature and urgency from the broad range of general compliance contexts covered by the self-critical evaluation privilege. Cybersecurity threats frequently involve criminal activity and, in some cases, foreign-nation-state support or tacit approval. Attacks that result in subsequent litigation where the privilege might be invoked always involve alleged compromise of third-party private information. As a result, the shared public interest in fostering robust proactive and remedial measures to improve cybersecurity is arguably much stronger than for other contexts.

Second, we propose that this qualified privilege be established through legislation at the federal and state level, rather than through common law. Courts understandably are reluctant to recognize new common-law privileges and generally cite the high burden for such recognition when rejecting the self-critical analysis privilege.[189] Establishing the privilege through legislation removes those concerns. While it is no simple task to pass legislation, there is growing bipartisan consensus that

189. *See Lund,* 2017 WL 5891186, at *5.

cybersecurity is a critical national priority that requires new and creative approaches.[190]

Accordingly, we are persuaded that the benefits of lessening the security risk that the current regime creates, coupled with the benefits of reducing the unfair manner in which the current regime treats victims of cyberattacks, are sufficient to justify the proposed qualified privilege, given that the privilege would not in our view impose undue hardship on regulators and private litigants in building and bringing cases against the victims of cyberattacks.

c. Proposed "No Waiver" Rule for Criminal Cybersecurity Investigations

One partial reform proposal that would address the current regime's disincentives for companies to share CI with criminal law enforcement is the creation of a limited form of protection against the waiver of attorney-client privilege and work-product protection for information shared in the course of a criminal investigation of a possible cybersecurity breach.

The arguments in favor of limiting waiver in this situation are not unique to the cybersecurity context. Others have advocated for a version of this protection, often called "selective waiver," for information shared in the course of civil regulatory investigations, and federal law provides a broad protection against privilege and work-product waiver for information

190. States in particular have been very active in seeking to address these issues. Through Nov. 6, 2018, at least 22 states had passed 52 cybersecurity-related bills, and at least 35 states, D.C. and Puerto Rico introduced/considered more than 265 bills or resolutions related to cybersecurity. *See Cybersecurity Legislation 2018*, NATIONAL COUNCIL OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx (last visited Nov. 20, 2019).

shared with banking regulators.[191] Several courts have recognized selective waiver on the basis that it encourages companies to fully investigate potential illegal conduct and to cooperate with regulatory agencies, thus protecting shareholders, customers, and the public.[192]

The majority of courts that have addressed whether to apply selective waiver in civil regulatory investigations, however, have not found either "the rationale of encouraging corporations to seek outside review of allegedly illegal corporate activities, nor that of encouraging them to cooperate with [regulatory] investigations" sufficient to justify the doctrine.[193] Courts that reject the doctrine note that organizations have ample incentive to seek candid advice from legal counsel regardless of

---

191. 2 PAUL R. RICE, ET AL., ATTORNEY-CLIENT PRIVILEGE IN THE U.S., LIMITED WAIVER—LOGIC OF LIMITED WAIVER § 9:91 (2018).

192. The seminal case supporting selective waiver is Diversified Indus., Inc. v. Meredith, 572 F.2d 596 (8th Cir. 1977) (en banc). In *Diversified*, a corporation responded to allegations that it had paid bribes to obtain business by forming an independent audit committee and retaining outside counsel to prepare an internal report on the issue. The internal report was subsequently produced to the Securities and Exchange Commission (SEC). The Eighth Circuit held that this disclosure constituted only a "limited waiver" that did not preclude the corporation from withholding the report from private litigants on the grounds of attorney-client privilege. *Id.* at 611. The Eighth Circuit explained: "To hold otherwise may have the effect of thwarting the developing procedure of corporations to employ independent outside counsel to investigate and advise them in order to protect stockholders, potential stockholders and customers." *Id.*; *see also* United States v. Shyres, 898 F.2d 647, 657 (8th Cir. 1990) (applying the reasoning of *Diversified*); McDonnell Douglas Corp. v. EEOC, 922 F. Supp. 235, 243 (E.D. Mo. 1996) (applying the reasoning of *Diversified*); Schnell v. Schnall, 550 F. Supp. 650, 652–53 (S.D.N.Y. 1982) (illustrating public policy of encouraging disclosure to SEC compels finding of selective waiver).

193. RICE, *supra* note 191.

whether a government regulator may require it to disclose that advice in an investigation. Moreover, the benefits an organization obtains from voluntary disclosure, in the form of more lenient sanctions resulting from an investigation, in most cases is sufficient incentive for cooperation with the regulator and not likely to be undermined by the risk of waiver of privilege or work-product protection.[194]

The case for selective waiver for disclosures in the course of a law enforcement investigation into a cybersecurity incident is arguably stronger than for civil regulatory investigations. The public's interest in obtaining complete information following a cybersecurity incident extends beyond ensuring full disclosure of potential legal violations to identifying information regarding potential cyber threats and actors that could help prevent those threats from affecting other organizations, individuals, and data. Compromises of the confidentiality, integrity, or availability of information or systems frequently result from criminal conduct by a third party. Permitting the affected entity to fully disclose information regarding a potential breach to law enforcement authorities without risk of waiving attorney-client privilege or work-product protection in a subsequent civil lawsuit or regulatory investigation would likely encourage such disclosures. This, in turn, could assist law enforcement in apprehending the criminal actors involved in the incident, thereby preventing that actor from similarly attacking other organizations.[195]

---

194. *See, e.g., In re* Steinhardt Partners, L.P., 9 F.3d 230, 236 (2d Cir. 1993); Permian Corp. v. United States, 665 F.2d 1214, 1221 n.13 (D.C. Cir. 1981).

195. Our collective experience suggests that many organizations either do not engage law enforcement or delay engagement following a data breach for a range of reasons, including concerns about waiver of attorney-client privilege and work-product protection. Our shared intuition is that while

A company that is the victim of a criminal cyberattack also sits in a much different position than one faced with an investigation into potential civil liability. First, the primary incentive for sharing information with law enforcement authorities is the possibility that law enforcement will apprehend the criminal actor, even though the victim may also receive some incidental benefits from the disclosure, such as being viewed slightly more favorably by regulators and the public, and/or receiving information from law enforcement to assist the victim's investigation and remediation efforts that it otherwise might not have received if it had not cooperated. But apprehension of cybercriminals is notoriously difficult and unlikely to undo the damage from the incident in any case. Second, permitting cybercrime victims to share otherwise privileged or protected information with law enforcement without fear of waiver would lessen the disincentive to do so created by the current regime, because such sharing would not increase the victim's potential liability exposure. Similar incentives do not exist when discussing selective waiver in the context of regulatory investigations.

i. Statutory Models

A statute providing selective waiver of privilege and work-product protection for information disclosed to criminal law enforcement could draw on waiver protections that exist in other contexts. Congress has created statutory limits on the waiver of

---

that reluctance in most instances is not driven primarily by waiver concerns, eliminating those concerns likely will encourage at least timelier, and possibly greater overall, cooperation and information sharing. Informal discussions with several federal law enforcement personnel actively involved in cybercrime matters confirmed that, in their experience, organizations often are reluctant to share information with law enforcement, and that legal liability concerns, including potential waiver of attorney-client privilege, frequently cause delays in the ability of law enforcement to obtain information.

the attorney-client privilege in two contexts: (1) a broad protection against waiver as to submissions made to banking regulators, and (2) as discussed in part C above, a protection against waiver for specific information shared through the processes prescribed by CISA.[196]

(a) Bank Examiner Waiver Protection

The protection against waiver of privilege for disclosing information to a bank examiner is provided by 12 U.S.C. § 1828(x):

> (x) Privileges not affected by disclosure to banking agency or supervisor
>
> (1) In general
>
> The submission by any person of any information to the Bureau of Consumer Financial Protection, any Federal banking agency, State bank supervisor, or foreign banking authority for any purpose in the course of any supervisory or regulatory process of such Bureau, agency, supervisor, or authority shall not be construed as waiving, destroying, or otherwise affecting any privilege such person may claim with respect to such information under Federal or State law as to any person or entity other than such Bureau, agency, supervisor, or authority.[197]

Very few courts have interpreted this provision, and it lacks any significant legislative history. The text leaves open several

196. Consolidated Appropriations Act, 2016, H.R. 2029, 114th Cong. (2015) (enacted).

197. 12 U.S.C. § 1828(x)(1).

important questions, including whether the bank examiner can waive an entity's privilege by disclosing the privileged material provided to it and how broadly to interpret "submission[s]," including whether material provided to a regulator during an enforcement action should be treated the same as submissions of more routine information.

Notably, bank regulators take the position that the bank-examiner regime does not merely permit, but requires, banks to disclose privileged information when requested by the regulator, given the compelling public interest in ensuring compliance with banking regulations.[198]

(b) CISA Waiver Protection

CISA creates a specific procedure for private organizations to share specific cyber threat information directly or indirectly with the Department of Homeland Security (DHS). As noted in Part C above, to incentivize voluntary information sharing with DHS, CISA provides a limited protection against waiver of privilege and other legal protections:

> Section 1504(d)(1) Information Shared With Or Provided To The Federal Government:
>
> (1) No waiver of privilege or protection. The provision of cyber threat indicators and defensive measures to the Federal Government under this subchapter shall not constitute a waiver of any applicable privilege or protection

198. *See, e.g.*, Consumer Financial Protection Bureau Final Rule, Confidential Treatment of Privileged Information (June 28, 2012) (effective Aug. 6, 2012), 77 FR 39617 (July 5, 2012).

> provided by law, including trade secret protection.[199]

As a practical matter, CISA's limits on the information that can be shared and the procedure required for sharing make it unlikely that either attorney-client privilege or work-product protection would apply to any shared information. The statute requires the entity sharing the information to strip out personally identifiable information and other protected information for its protections to apply. Nonetheless, like the bank-examiner provision, this protection recognizes the broad public interest in facilitating prompt and voluntary disclosure of certain kinds of CI—here cybersecurity threat information—to cybersecurity regulators and the need to adapt existing legal regimes, at least in limited ways, to protect and advance that interest.

ii. "No Waiver" Proposal and Explanation

We are persuaded that concerns about cybersecurity and cybercrime are sufficient to justify adoption of a "no waiver" rule in the cybersecurity context that would apply to disclosures made by a cyberattack victim to the criminal law enforcement authorities investigating the attack. A key foundation for this conclusion is our belief that such disclosures do not significantly undermine the policy rationale for finding a waiver of the attorney-client privilege and/or work-product protection in certain circumstances where the privileged/protected material in question is disclosed to a third party. Specifically, a frequently cited reason for such third-party disclosures being deemed to waive the privilege/protection to which the disclosed information otherwise would have been entitled is that the party making the disclosure usually has a self-interested motive in doing so—the

199. 6 U.S.C. § 1504(d)(1).

self-interest usually being that the disclosing party believes the disclosure will advance its position in the proceeding in which the disclosure is being made.[200] In that circumstance, it is not perceived as "unfair" to find that the disclosure waived the privilege/protection both as to the recipient of the information and as to other third parties; and both as to the disclosed information and other related information that otherwise would have qualified for the privilege/protection.[201] As the saying goes, finding a waiver of the privilege/protection in that circumstance is necessary to prevent the disclosing party from using the privilege/protection "both as a sword and a shield."[202] Whatever merit that policy rationale may have in the usual context of a self-interested disclosure of attorney-client privileged or work-product protected material, we do not see such a disclosure as being fairly thought of as "self-interested" when it is made by the victim of a criminal cyberattack to criminal law enforcement

---

200. *See In re* Columbia/HCA Healthcare Corp. Billing Practices Litig., 293 F.3d 289, 302 (6th Cir. 2002) (rejecting selective waiver on grounds that permitting such a selective waiver would "transform[] the attorney-client privilege into 'merely another brush on an attorney's palette, utilized and manipulated to gain tactical or strategic advantage.'" (citing *In re* Steinhardt Partners, L.P., 9 F.3d 230, 235 (2d Cir. 1993)).

201. *See* Permian Corp. v. United States, 665 F.2d at 1214, 1221 (refusing to recognize selective waiver because "the client cannot be permitted to pick and choose among his opponents, waiving the privilege for some and resurrecting the claim of confidentiality to obstruct others, or to invoke the privilege as to communications whose confidentiality he has already compromised for his own benefit. . . . The attorney-client privilege is not designed for such tactical deployment.").

202. *See In re Columbia/HCA*, 293 F.3d at 307 (refusing to recognize selective waiver for work-product doctrine because, "like attorney-client privilege, there is no reason to transform the work product doctrine into another 'brush on the attorney's palette,' used as a sword rather than a shield." (internal quotation and citation omitted).

authorities investigating that attack, even though the victim may receive some incidental benefits from the disclosure—such as being viewed slightly more favorably by regulators and the public, and/or receiving information from law enforcement to assist the victim's investigation and remediation efforts that the victim otherwise might not have received if it had not made the disclosure. As a result, we do not see that policy rationale as being significantly undermined by adoption of a "no waiver" rule in that circumstance. This same rationale does not exist for disclosure in regulatory investigations, where the disclosing party is waiving the privilege specifically to protect its interests.

We also do not believe that adoption of such a "no waiver" rule would impose undue hardship on regulators and private litigants in building and bringing cases against the victims of cyberattacks. To be sure, adoption of a no-waiver rule of this sort would result in regulators and private litigants being denied access to certain CI disclosed to law enforcement that, under the current regime, they would have access to. And we acknowledge that the CI in question could well be quite valuable to regulators and private litigants in the cases they are trying to build. But the reality is that even under the current regime, regulators and private litigants would in all likelihood not have access to the CI in question, because the cyberattack victim would be unlikely to disclose it to law enforcement out of concern that such disclosure would operate as a waiver of the privilege/protection as to regulators and private litigants. As a practical matter, then, we believe that adoption of a no-waiver rule will leave regulators and private litigants no worse off in their ability to obtain access to relevant CI than they are under the current regime.

Based on the above thinking, we conclude that whatever limitations such a no-waiver rule would impose on the discoverability of relevant CI in the cybersecurity context are outweighed

by the benefits that such a rule would achieve. And we see those benefits as being substantial. Adoption of a no-waiver rule that would apply to disclosures made by a cyberattack victim to criminal law enforcement authorities investigating the attack would result in authorities receiving a greater flow of CI regarding the attack than is currently the case. Moreover, because the CI included in the increased flow is highly likely to provide detailed insights into the cybersecurity measures the attacked entity had in place, the vulnerabilities in those measures that the attacker exploited, and the data the attacker succeeded in compromising by means of those vulnerabilities, the CI could provide substantial assistance to law enforcement in bringing the perpetrators to justice. Accordingly, we are persuaded that the benefits of a no-waiver rule of this sort are sufficient to justify its adoption, given that such a rule would not in our view impose undue hardship on regulators and private litigants in building and bringing cases against the victims of cyberattacks or provide those victims with any unfair advantage in defending those cases.

We therefore propose adoption of a "no waiver" rule in the cybersecurity context containing the following language:

> *No waiver of privilege or protection for information shared with law enforcement*—The submission by any person of any information to a law enforcement agency for any purpose in connection with a potential or existing criminal investigation or proceeding by the agency regarding the potential or actual unauthorized access, or attempted unauthorized access, to computerized data or systems shall not constitute a waiver of any applicable privilege or protection provided by law or otherwise affect any privilege or protection such person

> may claim with respect to such information under Federal or State law as to any person or entity.
> "Law enforcement agency" means any government agency that has authority to investigate or prosecute a crime regarding the potential or actual unauthorized access, or attempted unauthorized access, to computerized data or systems.

In developing this language, we carefully considered each of the following questions:

What entities are covered. Both the Bank Examiner and CISA statutes apply only to specific federal entities. Given the broad patchwork of cybersecurity laws, a proposed rule in this area could cover either the whole gamut of agencies that might request the relevant information or only those that more frequently conduct such investigations. For the reasons discussed in Part D.2.c, we are proposing waiver protection limited to information shared in connection with an existing or potential criminal investigation of a potential cybersecurity breach. The rationale for encouraging information sharing with law enforcement regarding a potential criminal attack applies to any law enforcement agency at both the state and federal level, and so we chose not to include a specific list of the agencies covered.

What incidents are covered. The operative language describing the incidents covered ("regarding the potential or actual unauthorized access, or attempted unauthorized access, to computerized data or systems") is adapted from similar language in the Computer Fraud and Abuse Act (CFAA).[203] We looked to the CFAA as a model for defining the relevant criminal conduct

203. 18 U.S.C. § 1030 ((a) Whoever—(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— . . .).

related to data access that would trigger the waiver protection but updated the CFAA's somewhat dated reference to "computers."

The rule we have proposed extends only to incidents involving access to computer records, and not paper, because the specific problem we seek to address is the pervasive and growing risk of cyberattacks.

What information is covered. We propose to protect against waiver "any information" disclosed "by any person" and "for any purpose in connection with a potential or existing criminal investigation or proceeding." This language is modeled on the similarly broad language in the Bank Examiner statute. Although the limited legislative history sheds no light on this issue, we surmise that the drafters chose not to attempt to limit the information that could be protected against waiver for two reasons: (1) the difficulty in defining the scope of information in the abstract; and (2) the relative lack of any incentive to disclose irrelevant information.

The universe of information this protection is aimed at is likely to be quite small: documents that both (1) are likely to be useful for apprehending the criminals involved and/or for other organizations to defend against similar attacks; and (2) are likely to qualify for attorney-client privilege and/or work-product protection. The imprecise nature of both the CI and the scope of privilege and work-product protection, however, combine to make it extremely difficult to define that universe in the abstract.

Equally important, we could identify no meaningful potential downside to extending the no-waiver rule broadly to "any information" otherwise meeting the statutory test. The rule we propose does not create a new privilege or substantively expand the scope of privilege or work-product protection; it merely

prevents waiver of them for documents that are otherwise protected. Therefore, it does not create any incentive to disclose information that is not useful to the investigation, because doing so does not protect otherwise unprivileged or unprotected information from disclosure. To be sure, as noted above, adoption of a no-waiver rule of this sort would result in regulators and private litigants being denied access to certain CI disclosed to law enforcement that, under the current regime, they would have access to upon its disclosure. But as discussed, even under the current regime, regulators and private litigants would in all likelihood not have access to the CI in question, because the cyberattack victim is unlikely to disclose that CI to law enforcement out of concern that it would operate as a waiver of the privilege/protection as to regulators and private litigants.

Compelled vs. voluntary disclosure. We propose a no-waiver rule that does not compel disclosure to law enforcement. A no-waiver rule could provide, as bank regulators contend is the case in the bank-examiner context, that a data holder is *required* to provide attorney-client privileged or work-product protected CI to the government entities covered by the statute when requested to do so, and that no waiver of the privilege/protection as to other persons or entities will result from doing so. Or it could provide that a data holder is free to decide whether to disclose information and does not risk waiver by doing so. The policy justifications and potential consequences of each approach are dramatically different. A voluntary disclosure regime would focus on the needs of data holders, seeking to address their perceived concerns with disclosing or not disclosing otherwise protected CI to the government. A mandatory disclosure regime would focus on the needs of government, seeking to address its perceived concerns with enforcing the law. While the rationale for waiver protection arguably could support mandatory disclosure, doing so would transform a protection intended to create

incentives to voluntarily share information with law enforcement into a powerful tool for demanding cooperation in circumstances where there otherwise is neither a legal requirement nor a strong incentive to do so.[204] Our proposed rule, accordingly, does not mandate disclosure to law enforcement of attorney-client privileged or work-product protected information, but instead is limited to permitting non-waiving disclosure of such information to law enforcement in connection with a potential or existing criminal investigation and is designed to encourage greater and more timely voluntary sharing of such information with law enforcement agencies.

Confidentiality agreement with law enforcement; subsequent disclosure by law enforcement. A hallmark of attorney-client privileged or work-product protected documents is that they are developed confidentially and shared as narrowly as possible. One issue sometimes raised in the court decisions discussing the selective-waiver doctrine is whether the doctrine requires that the disclosing party enter into a confidentiality agreement with a regulatory agency to effectively prevent waiver and, if so, what form that agreement should take.[205] Our proposed rule clearly

---

204. Even the voluntary cybersecurity threat information-sharing provisions in CISA raised significant concerns over individual privacy and civil liberties because of the possibility that the Department of Homeland Security might share private information with law enforcement without a warrant. *See, e.g.*, *CISA Security Bill Passes Senate with Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015, 5:30 p.m.), *available at* https://wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/. A mandatory disclosure regime that permits law enforcement to directly demand similar information following a cyberattack would raise even stronger potential objections.

205. *See, e.g.*, *In re* Mutual Funds Inv. Litig., 251 F.R.D. 185 (D. Md. 2008) (discussing *In re* Doe, 662 F.2d 1073 (4th Cir. 1981) and noting that the Fourth Circuit in that decision "explained that waiver of work product protection

establishes that disclosure to law enforcement in connection with an existing or potential criminal investigation of a potential cybersecurity breach does not waive privilege or work-product protection. Therefore, in our view, no additional measure, including entering into a confidentiality agreement, is necessary to prevent waiver under the rule we propose. For similar reasons, in our view, subsequent disclosure of the CI would not waive the attorney-client privilege or the work-product protection, as the privilege/protection would belong to the party that disclosed the information to law enforcement, not to law enforcement. Therefore, no unilateral action taken by law enforcement (such as disclosure of that information to a third party) could operate to waive the disclosing party's privilege/protection as to that information.

Who should adopt the rule, and how should they adopt it? For our proposed rule to achieve its maximum benefit, it would need to provide maximum certainty to data holders that their disclosure to law enforcement of attorney-client privileged or work-product protected CI would not waive the privilege or protection in question. To maximize such certainty, our proposed rule would need to be adopted in all U.S. states and inhabited territories, in Washington, D.C., and by the U.S. federal government. While that is our recommendation, we do not believe our proposed rule has no utility unless it is widely adopted. Rather, we are saying that our proposed rule will have more utility the more widely it is adopted. In terms of how our proposed rule should be adopted, we do not think it is reasonable to expect courts to judicially adopt our proposed rule through application of common-law principles. Instead we think it will be necessary for our proposed rule to be codified by the relevant authorities,

---

may occur in circumstances where the attorney 'cannot reasonably expect to limit the future use of the otherwise protected material.'" *Id.* at 187).

presumably by means of amendments to their existing rules of civil procedure and/or evidence.

E. CONCLUSION

Through an examination of how courts have and presumably will apply traditional attorney-client privilege and work-product protection law to CI, the *Commentary* discusses whether such application will incentivize and protect CI in accordance with the policy considerations accompanying the cybersecurity context. The *Commentary*'s consideration of various proposals explores the tradeoffs between the current regime and a modified one and arrives at suggesting two proposals that would remedy what appear to be issues with the current regime's operation in the cybersecurity context. As discussed above, a qualified stand-alone privilege could help address the current regime's chilling effect on conducting frank and pointed analyses of (or even undertaking) various cybersecurity measures. Second, because of the significant hazards—including the risk of waiver—for data holders in sharing CI with law enforcement, as well as the public interest in prompt and complete knowledge about cybersecurity incidents, the *Commentary* proposes that state and federal law recognize a "no waiver" doctrine providing that disclosure of CI to law enforcement would not waive any privilege or protection that might otherwise be claimed as to such CI in future civil litigation. The *Commentary* provides a roadmap to discuss these critical issues facing the discoverability and protection of CI and to provide concrete proposals for how policymakers and courts may wish to use current or new law to align the incentives with policy goals.

THE SEDONA CONFERENCE INCIDENT RESPONSE GUIDE

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editor-in-Chief:

Robert E. Cattanach

Editors:

M. James Daley
April Doss
Warren G. Kruse II
Kari M. Rollins
Jo Anne Schwendinger
Leon Silver
Joseph Swanson
Michael Whitt

Steering Committee Liaison:

Matthew Meade

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

The publication may be cited as follows:

> The Sedona Conference, *Incident Response Guide*, 21 SEDONA CONF. J. 125 (2020).

PREFACE

Welcome to the January 2020 final version of The Sedona Conference *Incident Response Guide*, a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages. We hope the *Incident Response Guide* will be of immediate and practical benefit to organizations, attorneys, and jurists.

The Sedona Conference acknowledges Editor-in-Chief Bob Cattanach for his leadership and commitment to the project. We also thank editors Jim Daley, April Doss, Warren Kruse, Kari Rollins, Jo Anne Schwendinger, Leon Silver, Joe Swanson, and Michael Whitt for their efforts. We acknowledge the significant contributions of Lauri Dolezal, as well as the assistance of Sam Bolstad, Elizabeth Snyder, Samir Islam, and Colman McCarthy. Finally, we also thank Matt Meade, who provided valuable counsel as Steering Committee liaison.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of the *Incident Response Guide* were the subject of dialogue. The publication was

also subject to a period of public comment. On behalf of The Sedona Conference, I thank all of them for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
January 2020

FOREWORD

The intent of the drafting team, which includes privacy and data protection lawyers from many different backgrounds, is to provide a comprehensive but practical guide to help practitioners deal with the multitude of legal, technical, and policy issues that arise whenever an incident occurs. The challenge of preparing any type of guide in such a rapidly evolving area of the law is that it is likely to be outdated, at least to some extent, by the time it is published, or soon thereafter. Nevertheless, the drafters believe that the value of this *Incident Response Guide* ("*Guide*") is not so much in being a definitive compendium of the law in this area, but rather to inform the process that an organization will likely engage in when it adopts the *Guide* for its own use.

The goal, therefore, is to provide those practicing in this space with not only a high-level overview of the key legal requirements that are relevant when an incident occurs, but with enough detail that the *Guide* can be employed largely as a single-source reference to guide the user through the various legal and operational steps necessary to respond to an incident. We address the foundational legal principles of breach notification requirements, principally by presenting those requirements grouped according to the types of obligations that U.S. jurisdictions typically impose, including subcategories for details such as the timing, content, and recipients for breach notifications. The reader may also want to keep in mind other more specific obligations that may exist depending on the industry sector involved, particularly health care and financial, as well as the requirements of other international jurisdictions, including the European Union with the advent of its General Data Protection Regulation (GDPR).[1]

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the

As noted in the body of the document, the target audience for this *Guide* is small- to medium-sized organizations, which we expect will not have unlimited resources to devote to incident responses. With this in mind, we have provided sample notification letters that can be used according to different jurisdictional requirements, as well as a very basic Model Incident Response Plan.

It goes without saying that any attempt to provide a document of this nature is by definition a compromise. This *Guide* attempts to strike a balance between being reasonably complete, but at the same time, not so voluminous and legal-authority laden that it is not practical to use during the exigencies of an incident response. As will become evident to the reader, one of the principal values of this document will be to assist practitioners in the *process* of preparing for an incident response, especially including key leaders in the company as part of the incident response team, which, based on our experience, promotes cross-functional ownership of the pre-incident planning that will be indispensable when it comes time to respond to an actual breach.

Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119/1) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents [hereinafter GDPR].

TABLE OF CONTENTS

I. INTRODUCTION

In today's connected world, compromise of electronically stored information (ESI) is inevitable—even for the most prepared organization. An effective and efficient response is critical to expediting recovery and minimizing the resulting harm to the organization and other interested parties, especially affected consumers. The best time to plan such a response is before an incident occurs.

This *Incident Response Guide* ("*Guide*") is intended to help organizations prepare and implement an incident response plan and, more generally, to understand the information that drives the development of such a plan. It has been created by thought leaders in the industry, including privacy counsel from Fortune 500 companies, government attorneys, and attorneys from several of the nation's most prominent law firms. It reflects both the practical lessons learned and legal experience gained by the drafters from direct experience responding to incidents, from representation of affected clients, and from the promulgation of rules and guidelines on national and international levels, and is intended to provide general guidance on the topic.

This *Guide* is designed as a reference tool only and is not a substitute for applying independent analysis and good legal judgment in light of the needs of the organization. The reader should note that this *Guide* is up-to-date only as of the date of publication. This is a rapidly changing area of law, so care should be taken to understand and comply with the most current requirements. Nothing contained in this *Guide* is intended to establish a legal standard or a yardstick against which to measure compliance with legal obligations. A reader should neither assume that following this *Guide* will insulate it from potential liability, nor that failure to adhere to this *Guide* will give rise to liability. Rather, the purpose is to identify in detail issues that should be considered when addressing the preparation and

implementation of an incident response that is suitable to his or her organization.

While this *Guide* was drafted with small to medium-sized organizations in mind, it is anticipated that the breadth of topics covered and the chronological sequence of the material will prove a useful reference for even the most experienced cybersecurity lawyer and sophisticated organization.

II. PRE-INCIDENT PLANNING

A. Identifying and Mapping Data and Legal Obligations

The foundation for any Incident Response Plan ("IRP") requires careful advance planning. The first step for the organization is to identify what format of data (digital, paper, and other tangible data) it has, and where that data is located.

Tangible data is typically located in offices, filing cabinets, and at remote storage locations, while digital data is more widely dispersed, in on-premises servers, servers located in the cloud, and on hard drives, discs, and flash drives. It is also constantly flowing into, through, and from a variety of physical and logical "locations." Because legal obligations differ depending on data type (e.g., trade secrets, confidential information, personally identifiable information (PII), protected health information (PHI), and payment card information (PCI)), data maps that identify data type as well as data location facilitate analysis of legal obligations.

Once the organization's data is mapped, the organization will need to identify the legal and contractual obligations that apply to the data. An index of legal obligations should include both regulatory requirements as well as contractual undertakings that may apply to various data types, at the locations where they exist. This can help assess legal obligations in the ordinary course of business, as well as when an incident occurs. The organization's information governance efforts typically form the cornerstone of this process.

Basic data governance considerations will focus on collection, security, use, retention, transfer, and secure destruction of data at end of life. In the statutory and regulatory realm, data security requirements may include specific requirements, like encryption of PHI under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or more general data

security requirements based on reasonableness or industry standard practices. Contractual undertakings may adopt these data security requirements by reference, or impose additional obligations.

Irrespective of the origin of a security requirement, there should be a process for assigning responsibility for data security by function and position, assessing and tracking compliance, and conducting periodic audits.

B. Supply Chain Security

Digitization is increasingly pervasive. Data that is captured at remote locations is transmitted and processed at various central hubs and increasingly stored off-premises, where it can be accessed later for analytic, reporting, or other business purposes. Sensors now capture data at every turn, especially via controllers embedded within equipment that operate at facilities, as well as the entire facility itself. Given the ubiquity of data and increasing subcontracting and outsourcing of functions, it is common for third parties to have access to the organization's data, systems, or networks to perform routine activities, including maintenance and trouble-shooting. Organizations also routinely share data with third parties, including suppliers, contractors, consultants, auditors, and law firms, collectively "Vendors."

An organization should conduct due diligence on the security practices of any proposed Vendor that will have access to its data in order to assess whether that Vendor has the policies and procedures in place to appropriately protect the data that will be entrusted to the Vendor, as well as make risk allocation decisions that should be reflected in the language of the contract with that Vendor. Organization-specific due diligence checklists for vendor assessment can be an efficient tool, and may include the following questions:

- Does the Vendor have security certifications such as International Standards Organization (ISO) 27001?
- Does the Vendor follow a National Institute of Standards and Technology (NIST) or another cybersecurity framework?
- Does the Vendor have adequate insurance, including cyber liability coverage?
- What is the Vendor's history of data security events?
- Will the Vendor permit security audits or provide copies of its external security audit reports?
- What due diligence does the Vendor conduct for its own employees, subcontractors, suppliers, and other third parties, especially those that might have access to the organization's data?
- What access controls and related data security measures does the Vendor employ?
- What are the Vendor's encryption practices, at rest and in transit?
- If the Vendor will house the organization's data, where will it be located and how and where will it be transferred, and how much notice will the organization receive if it is to be relocated?
- What are the Vendor's backup and recovery plans?
- Does the Vendor have an IRP?

A due diligence checklist should be regularly updated to reflect changes in legal and regulatory requirements, the nature of security threats, and standard industry practices.

Vendors that pass due-diligence screening should be contractually required to comply with the organization's security policies, guidelines, and practices, and to assist the organization

with reasonable investigation requests if an incident occurs. Ideally, the Vendor agreement should include information-sharing and notice requirements, including when the Vendor must notify the organization of its own data incidents, and changes to its security, data location, or regulatory jurisdiction(s). Unfortunately, this may not always be possible with many of the larger cloud Vendors, whose bargaining power often allows them to offer services on a "take it or leave it" basis, so the organization must factor in the consequences of this concession into their overall security approach.

Vendor access to the organization's networks and other secure assets should be limited to tasks necessary to complete its obligations. Certain types of data (confidential or privileged information, intellectual property, sensitive personal information, and protected health information) should be encrypted, and the Vendor's access to and, if necessary, retention of any encrypted data should reflect this protection. A Vendor should be able to access the organization's data and systems only after appropriate training and acknowledgement of its commitment to the organization's security practices. The Vendor's actual access should be logged and auditable, with any irregularities or concerns promptly addressed. Depending on the sensitivity of the information involved, retaining a consultant to validate training and security practices may be a prudent investment. If a Vendor holds the data of the organization, the Vendor should be legally obligated (by contract, law, professional responsibility, or otherwise) to keep the data secure to at least the same standard as the organization will be held.

Other contractual provisions to consider include limits on subcontractors and other third parties; restrictions on the use of data except for the purposes of the organization; audit rights; notice in case of a Vendor data incident; indemnification; carveouts from limitation of liability and waiver of consequential

damages; data return and destruction; and periodic or ongoing oversight and monitoring.

The organization's Vendor management practices should ensure that Vendor access is terminated for individuals when there are changes in Vendor personnel, and in its entirety upon completion of the agreement. Finally, post-termination data access and assistance should be addressed (for those instances where, post-term, the Vendor's assistance is required to mitigate or manage incidents or regulatory requirements such as investigations).

III. THE INCIDENT RESPONSE PLAN

The IRP provides the standard procedures and protocols for responding to and recovering from an incident. To promote maximum visibility and commitment within the organization, the core components of the IRP should be developed collectively by the members of an Incident Response Team ("IRT"), rather than simply assigned to the Information Technology (IT) department or an outside resource to draft.

The first step in any IRP is to apply agreed-upon criteria that define when an event should be considered only an IT-related incident (e.g., malware infection or detection of routine port scans by external parties) and when the event actually triggers the IRP. The IRP should also identify the responsibilities of each IRT member at the time the incident is first discovered, including how the team leader is designated for each expected type of incident. In addition, the IRP should describe how the team should be modified as a situation evolves and define the criteria for escalations. Basic protocols should include the logging of all critical events, commencing with how the organization learned of the incident, how and when the IRT was notified, as well as the why, what, and how for all responses, particularly escalations to more senior members of the management team and the organization's board of directors.

The IRP should define severity levels with business and legal-impact-based criteria. Clear and consistent communications are one of the most essential pillars of any IRP. The IRP should specify how information should be communicated once an incident is discovered, who should communicate it, and how those communications are coordinated. Protocols should also be established to ensure compliance with reporting mechanisms, which may also include a compliance hotline.

There is no one-size-fits-all IRP. To provide some framework for smaller and even some medium-sized organizations, see the

Model Incident Response Plan at Appendix A, *infra*. The IRP should be scaled in sophistication and scope to the nature of the organization. Larger organizations may have business units with their own plans because of regulatory or other considerations (e.g., financial services subsidiary, health care services, and foreign regulatory requirements). In those instances where a business unit may have its own plan, careful thought must be given as to how that plan will interconnect with the organization's crisis management plan, and the overall management structure for coordinating incident responses.

The use of counsel in responding to an incident is an important consideration. Counsel is likely to be most familiar with the legal consequences attendant to an incident, such as reporting obligations. Counsel's involvement in communications regarding the incident may also affect the ability to protect those communications by the attorney-client privilege and/or the work-product doctrine—which is itself a topic for more comprehensive discussion. To be clear, however, the mere presence of counsel as part of the process does not necessarily equate to qualifying any communication as privileged.

With regard to this latter point, communications and other written materials generated as a result of an incident often contain frank assessments regarding the organization's preparedness, vulnerabilities, and potential liability. Accordingly, those materials may be demanded in future litigation or enforcement proceedings. Whether those communications and other written materials will be shielded from disclosure is a complex issue that involves a number of factors, one of which is whether counsel was an essential party to the communications. Further, the law on this issue in the data breach context is still developing. For a more thorough treatment of this issue, please consult The Sedona Conference *Commentary on Application of Attorney-Client Privilege and Work Product Protection to Documents and*

Communications Generated in the Data Security Context.[2] For the purposes of this *Guide*, suffice it to say that counsel is likely to play a significant role in responding to any incident.

2. The Sedona Conference, *Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Data Security Context*, 21 SEDONA CONF. J. 1 (2020), available at https://thesedonaconference.org/publication/Commentary_on_Application_of_Attorney-Client_Privilege_and_Work-Product_Protection_to_Documents_and_Communications_Generated_in_the_Cybersecurity_Context.

IV. EXECUTING THE INCIDENT RESPONSE PLAN

A. Initial Assessment of the Incident ("C-I-A")

The IRP is triggered when a "threat actor"[3] initiates an action that disrupts the organization's cyber infrastructure[4] by compromising the:

- **C**onfidentiality or privacy of information in the organization's care;
- **I**ntegrity of the organization's data or computing/communications systems; or
- **A**vailability of the organization's data or computing/communications systems by authorized users.

The organization then becomes aware of the disruption—often after a significant amount of time has elapsed. Typically, this awareness will originate from:

- the organization's IT or security personnel noticing or being alerted to suspicious or anomalous system or user behaviors;
- a user within the organization noticing a system anomaly, unusual user behavior, or data flaw; or
- the organization being contacted by a third party such as law enforcement or a regulator, a client or

3. Threat actors are human or human-directed, and generally fall into classes such as: insider, whether negligent or malicious; unsophisticated "script kiddies"; socially motivated hacktivists; criminals; competitors; or state-sponsored actors.

4. Cyber infrastructure consists of computing and communications systems including those with data and data-processing capability, web presence, etc., whether owned and operated by the organization or by others for the organization.

customer, a Vendor, a member of the press (social media or conventional press), or even the malicious actor itself.

The IT group typically will conduct a scoping investigation of the disruption and attempt to determine its cause, time frame, and which systems or information are at risk. If the disruption is minor, and the risk of harm is determined to be low, the IT group may simply document the situation, repair the disruption, and bring systems back to normal operations. Depending on the severity and cause, the group may inform the full IRT and even senior management. Typically, the thresholds between minor disruptions and disruptions requiring escalation are predetermined as part of a comprehensive written information security plan or the IRP. Typically, the IRT establishes a maximum time period for the IT group to determine if the incident is minor and needs no escalation, prior to the incident defaulting to a more serious status.

B. Activating the Incident Response Team

The incident should be escalated to the IRT if the disruption is not minor and threatens continued operations, or the risk of harm is determined to exceed organizational comfort levels (often by referring to the Enterprise Risk Management protocols or policies). The incident should also be escalated to the IRT if, as indicated earlier, the IT group has been unable to characterize the incident as minor within a pre-set default period of time, or if such escalation is otherwise legally required.

An essential step in the IRP is to identify, individually, each member of the IRT. The IRT should include both internal and external resources that are reasonably likely to be involved in responding to an incident. At a minimum, the IRT should include representatives from the following business areas to the extent they are staffed internally by the organization:

- IT
- Cybersecurity
- Legal
- Compliance
- Privacy
- Human Resources
- Risk Management
- Communications / Public Relations / Investor Relations
- Physical Security
- Law Enforcement Liaison
- Supporting external resources (e.g., outside counsel, forensic experts, law enforcement contacts, and crisis management)

Each IRT designee should have a designated backup, with 24x7 contact information available for both the designees and the backups, to ensure that the unanticipated—but inevitable—absence of one key IRT member does not stall or hamstring the process.

As indicated in Section III, each IRT member has predetermined responsibilities. Using the "C-I-A" analysis above, for example, the IT group determines preliminarily what (if any) data has been compromised ("C"), whether systems or data integrity have been affected ("I"), and whether the availability of the organization's data or computing/communications systems has been affected ("A") to assess, at least initially, the scope of the problem. It may also be possible to gain some insight into the identity of the threat actor, the target of and motivation for the attack, the extent of the attack or breach, and whether it can be

quickly contained and mitigated or more significant effort will be required.[5]

C. First Steps of Incident Response and Escalations

The IRP should define data events in terms of severity levels and specify which severity levels require referral to the full IRT. The first point of contact on the IRT should be controlled according to the IRP. That person convenes the IRT per the procedures defined by the IRP. Having counsel (inside or outside) integrally involved in directing these initial steps will help ensure that the IRT is cognizant of its legal obligations. Counsel's involvement may also assist the organization in later asserting that the process—and any communications made as part of that process—should be protected under the attorney-client privilege or the work-product doctrine, as noted earlier in Section III.

The IRT should recognize that the facts will be incomplete. Nevertheless, the IRP can provide a checklist or decision-analysis guide that will direct the IRT to take preliminarily responsive actions based on the facts available, as well as provide a framework for identifying what additional facts need to be obtained in order to proceed.

As the investigation unfolds, and more facts are divulged, the process should continue under the instruction of counsel as much as reasonably possible to ensure that the organization complies with:

- regulatory and other legally required reporting requirements;
- insurance policy requirements;
- contractual-reporting or information-sharing requirements;

---

5. This information should be conveyed immediately to the IRT, consistent with the IRP.

- legal-hold requirements and obligations to preserve evidence;
- insider trading protocols; and
- internal policy.

In particular, the IRT should be aware of possible time-sensitive requirements and be prepared to assess at regular intervals whether the facts known at that juncture are sufficient to "start the clock" on any of them, including, in particular, breach-notification requirements or notices to insurance carriers. The IRP should include communication protocols dictating how and to whom information is communicated once an incident occurs and provide clear guidance to the IRT on what circumstances may trigger external communications and escalation to the C-suite and, if necessary, any Board committees (e.g., Audit or Risk), if not the full Board of Directors.

D. Evolution of the Incident Response

At the beginning of any incident, necessary information is unavoidably incomplete. After activation of the IRT, next steps include initial assessment of the incident's cause and scope, its severity and potential consequences, whether there may be ongoing vulnerabilities or continuing risks, and the status of system security. Once these are determined, the first round of communication to key decision makers in the organization can commence.

Sometimes the cadence for these initial steps, especially the process of communicating the initial assessment, may be measured in several hours, depending on the situation. For more complicated incidents—especially if it is suspected that the organization's information may have been exfiltrated—the process required to obtain a reasonably accurate assessment may take several weeks, if not months. Just as with the initial response, as more facts become available, legal counsel should remain

integrally involved in the direction and evolution of the response as the legal consequences associated with those additional facts are assessed. Legal advice regarding regulatory-reporting obligations, contractual requirements, and compliance with internal management protocols will be a critical consideration during the execution of the IRP. Organizations should recognize that inevitably there will be a tension between the desire to protect the communication of legally sensitive information on the one hand, and the importance of transparent and open communication among the key players on the other. One of the more difficult decisions to be made will be the extent to which counsel should be involved in the process of generating or evaluating information that could potentially trigger legal consequences, and the extent to which that involvement enhances the ability to claim attorney-client privilege or work product, which is by no means guaranteed merely by counsel's involvement. Counterbalancing that consideration is the need to disseminate critical information throughout the IRT as quickly and efficiently as possible. Unstructured dissemination risks forfeiting privilege and work-product protections, because such communications may later be determined not to qualify for protection.

To be clear, not all communications with counsel qualify for protection; only those communications necessary for counsel to provide legal advice, or prepare for litigation, will be protected. The intent to seek legal advice should be used to determine which communications should initially be directed to counsel.

In addition to legal requirements, operational concerns need to be considered. Once the initial security aspects of the incident have been assessed, the IRT will face enormous pressure to alert key stakeholders, and potentially respond to inquiries from the media or public discourse on social media. The pressure to "get out ahead" of the story on the one hand, and "get it right" on the other, invariably creates tensions. The ubiquitous nature of

social media can challenge even the most thoughtful and disciplined communication plan. Social media is a powerful tool and, if handled correctly, can provide an enormously helpful channel for messaging; but if handled incorrectly, it can also result in misinformation and mistrust, which will be extremely difficult to overcome.

E. Communications Required Because of Third-Party Relationships or Contracts

The organization may also have contractual or relationship obligations to alert other interested parties and stakeholders. The IRP should catalogue potential parties that may have to be alerted to the incident, including:

- employees;
- contractors;
- clients or customers;
- vendors; and
- lenders, banks, and other financial institutions.

For large organizations or large IRTs, the importance of clearly defining who is the "voice" of the IRT for communications to senior management will be essential to avoid confusing, duplicative, or unclear communications. This is particularly true for significant incidents where the investigation and remediation are factually complex, where the stakes for the organization are quite high, and where the nature of the incident brings particular urgency to finding a resolution.

V. KEY COLLATERAL ISSUES

A. When and How to Engage Law Enforcement

In many cases, a data breach will involve actions by someone—whether inside or outside the organization—that could be considered a violation of U.S. federal or state law, or the laws of another nation or jurisdiction. One of three circumstances will typically lead to the involvement of law enforcement:

- There is a legal requirement to report the matter to law enforcement authorities.
- Reporting the matter to law enforcement is discretionary, with the affected organization retaining some latitude to decide whether reporting the incident seems, overall, to be consistent with the organization's best interests.
- The first notice that an organization has of a potential breach is outreach from a law enforcement authority, contacting the victim organization to inform them of activity that law enforcement has discovered.

There are a number of factors to consider in determining whether and how to engage law enforcement, including:

- the nature of the data that was potentially compromised;
- the need for assistance of law enforcement in investigating or mitigating the incident;
- the country and/or state of residence of any persons whose information is implicated in the incident;
- whether any specific regulatory scheme or statutory framework applies to the particular data or business operations at issue; and

- the locations where the organization is headquartered, has operations, or does business.

There can be a policy dimension to the decision on whether to engage law enforcement that is tied to the organization's culture. Some organizations voluntarily notify law enforcement out of a sense that good corporate citizenship obligates them to pass along information that might help authorities investigate crimes or even prevent other organizations from falling victim to the same crimes. Other organizations may be skeptical of triggering government involvement and less inclined to see advantages in passing information on to law enforcement entities. Although these intangible factors tend to be matters of organizational culture and policy, rather than strictly legal questions, it is important that organizations consider these decisions at a level of management commensurate with the potential consequences. Senior leadership will want to consider shareholder expectations, the reactions of customers and business partners, past public relations and public policy positions, or other factors that are unique to the organization.

Some organizations may be concerned that notifying law enforcement could trigger an investigation into their own information security practices and are therefore hesitant to make that outreach. The best approach to this issue is to establish, either directly or through outside counsel, a relationship with key law enforcement entities in advance of an incident, so that any reporting to law enforcement can occur within the context of a relationship built on some measure of trust, enabling the organization to consider more objectively whether the fear of heightened investigative scrutiny is well-founded in any particular instance.

Any checklist an organization might prepare regarding the decision whether to report to law enforcement should include:

- whether the organization could be exposed to legal liability for failing to report the incident (for example, when failure to report could constitute an independent violation of law);
- whether there is specific benefit to notifying law enforcement, such as when an incident involves breach of PII of victims in states where breach laws provide for a delay of notification if law enforcement determines that notification will impede a criminal investigation;
- the potential benefit to law enforcement and to other victims;[6]
- whether a law enforcement investigation could disrupt business operations;[7] and
- the philosophy of the organization.

At a minimum, organizations should identify in advance which federal and state laws require notification to governmental entities in the event of a breach. Critical to that assessment will be whether an organization has customer, employee, or other data that, if compromised, would trigger a requirement to notify a state attorney general or similar regulatory entity. The nature of the incident may influence whether federal, state, and/or local law enforcement is likely to have interest in the incident.

---

6. A single organization rarely has the insight to be able to adequately assess whether the cyber activity affecting them is part of a larger effort by organized crime, terrorists, or others who use malicious cyber activity as a means of financing their own operations (such as terrorist attacks, political destabilization, illegal arms trade, or other matters that affect the security of individuals and nations around the world).

7. Here, it should be noted that many law enforcement agencies are committed to carrying out investigations in a manner that causes as little disruption as possible to the organization.

1. Employee Theft

For example, if the incident involves a terminated employee who stole property (such as a laptop computer) that results in a data compromise (the laptop contains sensitive personal information), state or local law enforcement agencies may be best suited to investigate the theft as a local law enforcement matter and aid in recovery of the information.

2. Other Employee Misconduct

Employee actions can also combine criminal activity with computer security threats in different ways. For example, employees may use the organization's computing resources for unauthorized activity on the internet, such as sale of illegal drugs, human trafficking, or downloading of child pornography. Because of the nature of the websites and the communities of interest who engage in these activities on the internet, these activities can also increase the risk that malicious code will be imported into the organization's computer systems—which might result in the risk of downloading ransomware, or of giving an external hacker access to sensitive PII or intellectual property on the organization's network. In some cases, the illegal activity will lead to discovery of the breach; in others, discovery of the malicious code is what causes the organization to realize that this illegal activity is taking place. In such cases that involve a mix of a data security incident and serious criminal activity, the organization should report the matter to the appropriate law enforcement authorities, as failure to do so could result in independent civil liability or criminal charges for the organization. The organization can expect to become involved in a criminal investigation of what actions were taken on the organization's networks and by whom.

3. External Hacking

In incidents involving external hacking into an organization's network, federal law enforcement may be better suited to handle the matter than state or local authorities. First, state and local law enforcement agencies vary greatly in their capacity to respond to cyber incidents. Some have well-resourced and sophisticated components dedicated to computer crimes, while others have few, if any, resources available to handle these types of investigations. Second, in many instances, the hacking activity will constitute a violation of federal law, such as the Computer Fraud and Abuse Act. Consequently, the malicious activity is likely to fall within the jurisdiction of, and be of interest to, federal law enforcement agencies.

The U.S. Federal Bureau of Investigation (FBI) and U.S. Secret Service Electronic Crimes Task Force generally lead federal law enforcement investigations of cyber crimes. If nothing else, these federal agencies can help direct an organization to state or local law enforcement if the matter does not meet the federal agencies' thresholds. Interacting with the FBI and U.S. Secret Service is described in more detail below.

There are a number of guidelines to consult for reporting cyber crimes The FBI and Department of Homeland Security (which includes the U.S. Secret Service) have issued unified guidance to state, local, tribal, and territorial law enforcement agencies on how to report potential cyber crimes to the federal government.[8] The FBI works through its Cyber Division and its Cyber Task Forces, located in each of its 56 field offices.[9]

---

8. FED. BUREAU OF INVESTIGATION, LAW ENFORCEMENT CYBER INCIDENT REPORTING (2017), *available at* https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view.

9. Anecdotally, the FBI has been more than willing to meet with organizations to help them understand the threat landscape even before any

Organizations should also be cognizant of reporting to law enforcement authorities outside the U.S., as multinational cooperation on cyber crime continues to increase. For example, Europol has become increasingly involved in investigation of cyber crimes through its European Cybercrime Centre (EC3), which was established in 2013 with a stated purpose to "strengthen the law enforcement response to cyber-crime in the EU and thus to help protect European citizens, businesses and governments from online crime."[10]

In addition to multinational efforts such as Europol, most nations have some form of national law enforcement effort against cyber crime, and many nations also have subordinate local or regional law enforcement efforts directed against cyber crime. Organizations with a substantial business presence outside the U.S. should ensure they are familiar with the law enforcement entities that may have jurisdiction of cyber-related criminal activity that affects the organization's activities in those countries or regions.

At the beginning of an incident, it is often difficult to tell whether a criminal prosecution is likely to result. For that reason, it is important that the organization carry out its investigation in a manner that preserves the chain of custody for any evidence that may later be relied upon in court. This is important for potential civil litigation as well. Technology professionals who are

---

potential incident, and when appropriate conduct post-incident assessments (e.g., obtaining the internet protocol (IP) address of the financial account to which fraudulent transfers of funds have been directed). However, as a practical matter, absent extraordinary circumstances, the FBI typically lacks the resources to pursue aggressively the swelling tide of "run-of-the-mill" data breaches and related schemes, including "business email compromise."

10. *European Cybercrime Centre—EC3*, EUROPOL, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last visited Dec. 2, 2019).

assisting with the incident response should be particularly careful to avoid taking actions that might obscure the evidence of any unauthorized actions taken on the network. This will typically include preservation of system log files and full and precise imaging of system components. The scope of this work can be both painstaking and complex, depending on the nature of the organization's technology architecture and the type of incident.

Preserving this evidence and preserving the chain of custody that allows it to be admissible in court frequently requires a specialized set of experience and skills that may be beyond the expertise of in-house computer security professionals. Organizations that do not have personnel specifically trained in this kind of activity—and perhaps even those that do—should strongly consider engaging outside consultants who have experience in performing this work. Most often, the organization will want to engage those consultants through counsel, so that the work is better positioned to be carried out within the scope of the attorney-client privilege and/or the work-product doctrine, and preferably engage them well before an incident occurs through pre-negotiated Master Services Agreements.

The critical point that organizations should remember is that these considerations need to be built into the IRP for the very first moment that a suspected incident is identified; once network actions have been taken (including remedial actions like isolating infected servers or devices), it is often already too late to preserve the evidence in a form that would be admissible in court.

For example, in many traditional networks, disconnecting power from a server will not be an appropriate means of preserving evidence. In some situations, it may be appropriate for the server or other hardware to remain powered on but the network connection severed (by unplugging an Ethernet cord or turning off wireless connectivity to that device). Certain

standard response actions for certain specified events might be set forth in the IRP; nonstandard events will require more careful thought before taking responsive action.

This is merely one example, however, as cloud computing, third-party data hosting, use of service-oriented architectures, automated data aging, handling and storing backup data, and many other factors will affect the specific actions that are most appropriate in a particular case. For these reasons, it is essential that the organization rely on the advice of skilled technology professionals who have specific expertise in preservation of systems and data for forensic investigation purposes, whether those professionals are employees of the organization or hired as outside consultants.

B. Notice to Insurance Carriers

The notice required by an organization's insurance carrier should be set forth in the organization's insurance policy and carefully followed.

C. Alternative Communications Channels

In the event of a significant cybersecurity incident or intrusion, as with other emergency situations, it is essential to have reliable communication channels available to keep key players and essential stakeholders informed, and to lead and manage the incident response. In some cases, this may require alternative (and secure) communications channels. As with other incident response preparations, alternative communications channels should be planned and provisioned in advance to handle situations where corporate communications systems have been completely disrupted.

Assuming that the disruption of communications is limited to the organization's systems, and that third-party provider systems are still functioning, national telecommunication

companies and internet service providers will be able to provide alternative communications channels for voice, text, and email. Organizations that cannot sustain a loss of internal communication systems without risking material compromise to their ability to function should, at a minimum, explore advance arrangements for standby communications channels for their mission-critical functions. Secure emergency online portals, such as systems provided by "ERMS Emergency Notification and Mass Communication," can also be used as standby methods to broadcast information to users or selected groups and to share documents among a specific group of people.

With any alternative communications channels, there are certain caveats to be observed:

- Careful thought must be given to ensuring the security of the devices used by persons authorized to access the alternative communications channels.

  Personal cellphones or home phones may be a possibility, but if phone numbers for those devices were available on the organization's network at the time of an intrusion (as is often the case), it may be prudent, at least at the outset, to assume that those devices may have been compromised as well.

  The more advisable course may be to maintain a stock of emergency cellphones, tablets, and laptops, preinstalled with appropriate security (e.g., two-factor authentication), for distribution as appropriate in the event of an emergency, especially for use by members of the IRT and senior management of the target organization.
- Preexisting email addresses and phone numbers should not be used (or permitted) to access the alternative communications channels. Instead,

alternative email addresses (for example, name@xxxx.yyyy.com) and non-office phone numbers, all previously unused, should be issued for use with devices permitted to access the alternative communications channels.

In addition, the new (emergency) email addresses and phone numbers should *not* be kept online in any form (e.g., listed in the official IRP) to prevent that information from falling into the hands of the attackers. Instead, a hard-copy list (such as a wallet card) should be distributed only to members of the IRT and the organization's senior management who are expected to use the alternative communications channels.

- Consider face-to-face "in-person" meetings and communications as part of the alternative communications channels, and make arrangements for an emergency room or "war room," which can accommodate the IRT and senior management, for fact review, analysis, and decision-making.

  Situating an emergency room in one of the organization's offices may be sufficiently secure, but it may be more prudent to plan an alternative location in a different building. As with emergency email addresses and phone numbers, the alternative location should be revealed only to those who need to know.

- To ensure that the capabilities of alternative communications channels are maximized, it is also essential to document and periodically review relevant processes. This should include regular maintenance (and when changes are made, redistribution) of the off-line list of emergency email

addresses and phone numbers, as well as documentation in the IRP of how to use the emergency tools and how to contact critical resources like forensic consultants, external counsel, public relations consultants, law enforcement authorities, insurance companies, and key external stakeholders.

- Finally, to avoid alerting the threat actors that alternative communications channels have been activated, it may be appropriate to continue selective use of preexisting communications channels by some personnel with nonsensitive information (and possibly with "misinformation").

D. Terminating Unauthorized Access

Various studies have consistently shown that a significant percentage of cyber incidents have been caused by trusted insiders. In many cases, those studies conclude that insiders are responsible for over half of all incidents, through a combination of carelessness or risky behavior with unintended consequences, and deliberate incidents, such as theft of information, impairment of computer equipment and systems, or otherwise.

All computer and network access should be terminated as soon as possible for employees who no longer work for an organization, particularly in instances in which an employee has been fired or laid off. When an employee is being fired or laid off, the best practice is to revoke systems access immediately prior to notifying the employee of the administrative action about to be taken; this prevents the employee from being able to take retaliatory action on the network in response to the employer's action.

It is also essential for organizations with suspected malware to carefully and quickly examine whether there may be any unauthorized access that is persisting on the network. It is not

uncommon for sophisticated hackers to leave backdoors that are not readily identifiable; an organization may believe it has closed the vulnerability, not recognizing that additional code remains elsewhere in the network or in devices that can be used as a launching point for further unauthorized access. Unfortunately, it may not be apparent at the time that incident response begins whether the incident was caused by an advanced persistent threat (a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time, rather than causing immediate damage to the network or organization) or other sophisticated actor. Consequently, this risk is another reason why organizations should consider engaging external consultants who specialize in remediating cyber incidents to work with in-house computer security personnel to ensure that network security has been restored against both known and less obvious threats.

E. Engaging Outside Vendors

1. Pre-engaged Vendors

The IRP that was prepared and tested in advance should include consideration of outside Vendors for several purposes: computer forensics (to determine the nature and scope of an incident and the degree of ongoing vulnerability); continuous monitoring (some organizations will choose to contract with outside Vendors to provide ongoing security monitoring of their networks); breach notification (some Vendors are well-practiced in providing multi-jurisdictional incident notifications to victims; an organization with complex, multi-jurisdictional PII of customers or employees may wish to consider using a consultant to streamline and facilitate the process of breach notification, to include written notification and customer call center services); and crisis communications or media relations (depending on the

nature of the incident, public relations can be a key factor in successfully navigating a breach).

2. Considerations in the Use of Vendors

Whether to use Vendors can be a particularly difficult decision for small and mid-sized organizations whose business model does not include a large standing budget for incident response. The decision is a particularly difficult one in the early days of an incident, when there are still limited facts about what might have happened and the organization is struggling with the question of whether its own IT services staff (whether in-house or provided by a Vendor) can handle the incident investigation on its own. For smaller organizations in particular, there can be a tendency to first try to handle the investigation in-house, due to concerns that the cost of hiring an external computer security consultant will be unduly damaging to the organization's overall budget and fiscal health.

3. Cost and Resource Issues for Vendors

In their preparedness efforts, small and mid-sized organizations concerned about these matters should have specific conversations with cybersecurity consultants about their rates and services. Like the organizations they serve, consulting firms come in a variety of sizes. Mid-sized and smaller organizations that are considering incident response planning should not be deterred by concerns that large consulting firms have a business model that falls outside of their price range, as both large and small firms are able to provide sophisticated services across a wide range of price points to meet the needs of organizations that are faced with actual or potential cybersecurity incidents.

4. Attorney-Client Privilege and Technical Consultants

As noted earlier, consideration should be given to having legal counsel engage technical consultants to facilitate the provision of legal analysis and advice, and potentially protect that process by the attorney-client privilege and/or the work-product doctrine. This topic is addressed in greater detail in The Sedona Conference *Commentary on Application of Attorney-Client Privilege and Work Product Protection to Documents and Communications Generated in the Data Security Context*,[11] but among the issues to consider here are the language of the engagement letter with the technical consultant and whether counsel will be the intermediary between the consultant and the organization.

5. Engaging Technical Consultants at the Time of Breach

If there is no pre-arrangement with technical consultants, organizations that experience an incident should consult with in-house or outside counsel on the value and feasibility of bringing in technical consultants. Many law firms have existing relationships with consultants whose services they can engage or recommend, and many consultants are available on extremely short notice to respond to an incident, even if there haven't been previous discussions with the organization that is affected by the incident. As organizations increasingly purchase some form of insurance coverage for cybersecurity incidents, those carriers frequently have pre-approved panels of legal counsel and technical consultants available for immediate assistance.

11. *Commentary on Application of Attorney-Client Privilege and Work Product Protection to Documents and Communications Generated in the Data Security Context*, *supra* note 2.

F. Credit Monitoring and Identity Theft Considerations

Credit monitoring has been part of the data-breach landscape for many years, most often through voluntary action by the organization that suffered the breach, or as part of a consent decree with a regulator (such as the Federal Trade Commission (FTC)) or settlement among parties to litigation.

For the reasons discussed in detail below, however, organizations should carefully evaluate the decision to offer—and if so, to what extent—credit monitoring to impacted individuals in connection with a data breach. At least one court, the Seventh Circuit, has interpreted an offer of credit monitoring in a credit card breach as a sign that the risk was real, not "ephemeral," and, therefore, qualified as a concrete injury:

> It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk *is so ephemeral that it can safely be disregarded.* These credit-monitoring services come at a price that is more than *de minimis*. For instance, Experian offers credit monitoring for $4.95 a month for the first month, and then $19.95 per month thereafter. See https://www.experian.com/consumer-products/credit-monitoring.html. *That easily qualifies as a concrete injury.*[12]

12. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015) (emphasis added).

The clear message from *Neiman Marcus* is that offering credit monitoring is a factor that the court will consider in connection with establishing standing.

Second, credit monitoring only partially addresses the consequences of the potential theft of personal information. Some commentators have opined that it gives "consumers limited help with a very small percentage of the crimes that can be inflicted on them."[13] "Breached companies . . . like to offer it as a good [public relations] move even though it does absolutely nothing to compensate for the fact that a criminal stole credit card mag stripe account data."[14] A spokesman for the Privacy Rights Clearinghouse recently stated: "Fraudulent use of a stolen card number won't show up on a credit report because they don't show individual charges. And credit reports don't show debit card information at all."[15]

Third, offering credit monitoring when, for example, the breach involves medical data such as diagnoses, doctors' notes, and x-rays absent Social Security numbers, may arouse suspicion among those impacted that the breach is more comprehensive than the breached organization has disclosed in its notice. For example, if the breach notice informs the consumer that no Social Security numbers were accessed or subject to unauthorized use as a result of the incident, a recipient naturally might wonder why he or she is being offered credit monitoring. Credit monitoring will not tell you if someone has "hijacked your

13. Brian Krebs, *Are Credit Monitoring Services Worth It?*, KREBS ON SECURITY (Mar. 19, 2014), https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it (quoting Avivah Litan, fraud analyst at Gartner, Inc.).

14. *Id.*

15. Gregory Karp, *Why Credit Monitoring Will Not Help You After a Data Breach*, CHI. TRIB. (Aug. 15, 2014, 8:00 PM), http://www.chicagotribune.com/business/chi-why-credit-monitoring-will-not-help-you-after-a-data-breach-20140815-story.html.

identity for nonfinancial purposes, i.e., to get a new driver's license, passport, or other identity document."[16] Moreover, credit monitoring will not tell you if someone is using your medical information to get free medical care or medication.

A number of states have adopted a stricter approach to offering credit monitoring. In 2014, California amended its breach notification law as follows:

> If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).[17]

California's amended law states that identity theft protection services should be used for breaches involving Social Security numbers, driver's license numbers, or California identification card numbers. Noticeably excluded from the types of personal information where identity theft protection should be offered are breaches involving: account numbers or credit or debit card numbers, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; health insurance information; and information or data collected through the use or

16. Krebs, *supra* note 13 (quoting Avivah Litan, fraud analyst at Gartner, Inc.).

17. CAL. CIV. CODE § 1798.82(d)(2)(G).

operation of an automated license plate recognition system, as defined in Section 1798.90.5.[18]

In 2015, Connecticut followed California and passed a law affirmatively requiring: "appropriate identity theft prevention services and, if applicable, identity theft mitigation services" for at least one year, and, later, effective October 1, 2018, extended that obligation to twenty-four months.[19] It is important to note that the Connecticut law, like California, **does not require** credit monitoring in all cases, but instead requires "appropriate identity theft prevention services."[20] Connecticut's former Attorney General George Jepsen stated the following, in connection with the announcement of the 2015 version of the Connecticut law:

> The bill also calls for companies who experience breaches to provide no less than one year [as of October 1, 2018, twenty-four months] of identity theft prevention services. This requirement sets a floor for the duration of the protection and *does not state explicitly what features the free protection must include.* I continue to have enforcement authority to seek more than one year's protection—and to seek broader kinds of protection—where circumstances warrant. Indeed, in matters involving breaches of highly sensitive information, like Social Security numbers, my practice has been to demand two years of protections. I intend to continue to that practice.[21]

---

18. *Id.* § 1798.82(h).

19. CONN. GEN. STAT. § 36a-701b(b)(2)(B).

20. *Id*.

21. George Jepsen, *Statement from [former] AG Jepsen on Final Passage of Data Breach Notification and Consumer Protection Legislation*, STATE OF CONN. OFFICE OF THE ATTORNEY GEN. (June 2, 2015), https://portal.ct.gov/AG/Press-

The clear message from the Connecticut law, and one which appears to be gaining additional traction in this space, is that organizations should not necessarily rely solely on credit monitoring and need to determine what identity theft prevention service would be appropriate under the circumstances.

It should be noted, however, that breach notification laws across jurisdictions change frequently, and organizations should be sure to include a review of potentially applicable credit monitoring requirements in their incident response. Regardless of whether the credit monitoring services are voluntarily offered or required, organizations should consider incorporating into their IRPs a budget line to cover the cost of providing credit monitoring services to affected persons. If, however, credit monitoring is not appropriate, then the significant cost of the service can be reallocated to enhanced employee training, cyber enhancements, and the completion of a thorough risk assessment of cyber vulnerabilities.

G. PCI-Related Considerations

In May of 2018, the Payment Card Industry Security Standards Council promulgated Version 3.2.1 of the Data Security Standard ("PCI DSS" or "Standard") with requirements regarding actions to take in the event of a breach of payment card-related information. Not all provisions are listed here, but, for those subject to PCI DSS, there are key provisions worth mentioning. For instance, the Standard reminds entities handling payment card industry information of the importance of adhering to PCI DSS Requirement 12.10: "Implement an incident response plan. Be prepared to respond immediately to a system

---

Releases-Archived/2015-Press-Releases/Statement-from-AG-Jepsen-on-Final-Passage-of-Data-Breach-Notification-and-Consumer-Protection-Legisl (emphasis added).

breach."[22] The guidance for Requirement 12.10 goes on to state, "Without a thorough security incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as new legal liabilities."[23] Requirement 12.10.2 requires that the plan be reviewed and tested at least annually.[24]

The PCI DSS requirements are widely accepted as industry-standard best practices. Under fact patterns where they apply, they are likely to be viewed as setting a baseline for reasonableness in the handling of payment card information. Consequently, organizations and their counsel should take particular care to assess whether an organization's handling of payment card information complies with them.

---

22. PAYMENT CARD INDUS. SEC. STANDARDS COUNCIL, DATA SECURITY STANDARD 113 (Ver. 3.2.1 May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1510781420590.

23. *Id*.

24. *Id.* Seemingly implicit in these standards is the assumption that organizations will be able, within their own systems, to isolate or mitigate a breach without causing loss of evidence; have protocols for notifying business partners, such as payment card brands, merchant banks, and others whose notification is required by contract or law; and have a process for engaging a Payment Card Industry Forensics Investigator ("PFI") prior to any occurrence, so that the PFI can be notified immediately upon recognition of a breach. Importantly, the PFI must be on a PCI-DSS-approved list, and—to ensure independence—cannot be already providing PCI services to the organization experiencing the breach.

VI. BASIC NOTIFICATION REQUIREMENTS

A. Introduction

In most cases, the determination of whether a data breach has occurred and whether notice is required will depend upon the dictates of applicable state data breach notification laws. In turn, the applicability of state data breach notification laws will depend upon the residency of the individuals impacted by the data incident, and not, as one might think, the organization's state of incorporation or principal place of business.

Once the organization has determined the residency of all impacted individuals, then it can determine which state data breach notification laws apply and whether, after investigation, the facts of the incident support a conclusion that a data breach has occurred as defined by state law. If the data incident does rise to the level of a data breach, then several questions follow:

- Is notification required?
- To whom must notification be made?
- When must notification be made?
- What must be included in the notification?

The next section offers guidance in answering these questions and navigating key notice logistics. In reviewing the guidance offered below, please note that the summary and overview of state notice requirements is only current as of the date of this publication. Given the recent regularity with which state legislators and (derivatively) regulators have been amending data breach notification laws, organizations should scrutinize the relevant state statutes and state websites for information regarding any changes or amendments to the requirements and rules discussed below.

B. *Has a Breach of Personally Identifiable Information Occurred that Requires Notification?*

In evaluating whether a breach (as defined by law) has occurred that requires notification, an important threshold consideration is whether the incident involves PII as defined by applicable state law. The definition of PII varies among states and continues to evolve. For instance, biometric data is treated as PII in some states, but not in others. And some states treat a credit card number as PII, while others do so only if the credit card number is accessed or acquired in combination with the PIN, access code, expiration date, or security code (i.e., CVV). Further, some states exclude from the definition of PII social security numbers that have been truncated or partially redacted (i.e., only the last 4 digits are visible). These are just a few examples of the variances in the definition of PII across state laws. Accordingly, when analyzing whether a "breach" has occurred that requires notification, it is imperative to evaluate the current definition of PII in each applicable jurisdiction.

After evaluating whether protected PII has been impacted by the data incident, the next question to answer is whether the protected PII has been "breached," as defined by relevant law. Not surprisingly, the definition of "breach" varies state by state and similarly continues to evolve. That said, most states define a "breach" *generally* as the unauthorized *acquisition* of protected PII.[25] However, several states and Puerto Rico consider the

25. *See* ALA. CODE § 8-38-2(1); ALASKA STAT. § 45.48.090(1); ARIZ. REV. STAT. § 18-551(1); ARK. CODE ANN. § 4-110-103(1); CAL. CIV. CODE § 1798.82(g); COLO. REV. STAT. § 6-1-716(1)(h); CONN. GEN. STAT. § 36a-701b(a)(1); DEL. CODE ANN. tit. 6, § 12B-101(1); D.C. CODE § 28-3851(1); GA. CODE ANN. § 10-1-911(1) (applies only to Information Brokers and Data Collectors); HAW. REV. STAT. § 487N-1; IDAHO CODE § 28-51-104(2); 815 ILL. COMP. STAT. 530/5; IND. CODE § 24-4.9-2-2(a); IOWA CODE § 715C.1(1); KAN. STAT. ANN. § 50-7a01(h); KY. REV. STAT. ANN. § 365.732(1)(a); LA. STAT. ANN. § 51:3073(2); ME.

unauthorized *access* to (versus the full scale acquisition of) protected PII alone sufficient to constitute a "breach."[26] And, yet, another small handful of states include in their "breach" definition (in addition to the unauthorized acquisition of) the unauthorized use, illegal use, or unauthorized release of protected PII.[27] Therefore, once it is determined that protected PII has been impacted by the data incident, analysis must be performed to assess whether the facts and forensic findings of the data incident establish, or at least indicate, that the protected PII was accessed, acquired, used, or released without authorization, and whether such access, acquisition, use, or release triggers a "breach" under relevant state law.

After establishing unauthorized access or acquisition, the majority of states require the "breach" analysis to be taken one step further—to assess whether the unauthorized access or acquisition has compromised the security, confidentiality, or

---

REV. STAT. ANN. tit. 10, § 1347(1); MD. CODE ANN., COM. LAW § 14-3504(a); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.63(b); MINN. STAT. § 325E.61(1)(d); MISS. CODE ANN. § 75-24-29(2)(a); MO. ANN. STAT. § 407.1500(1)(1); MONT. CODE ANN. § 30-14-1704(4)(a); NEB. REV. STAT. § 87-802(1); NEV. REV. STAT. ANN. § 603A.020; N.H. REV. STAT. ANN. § 359-C:19(V); N.M. STAT. ANN. § 57-12C-2(D); N.C. GEN. STAT. § 75-61(14); N.D. CENT. CODE § 51-30-01(1); OHIO REV. CODE ANN. § 1349.19(A)(1); OKLA. STAT. tit. 24, § 162(1); OR. REV. STAT. § 646A.602(1); 73 PA. CONS. STAT. § 2302; 11 R.I. GEN. LAWS § 11-49.3-3(a)(1); S.C. CODE ANN. § 39-1-90(D)(1); S.D. CODIFIED LAWS § 22-40-19(1); TENN. CODE ANN. § 47-18-2107(a)(1); TEX. BUS. & COM. CODE ANN. § 521.053(a); UTAH CODE ANN. § 13-44-102(1); VT. STAT. ANN. tit. 9, § 2430(12)(A); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(1)(2) (eff. 3/1/2020); W. VA. CODE § 46A-2A-101(1), (6); WIS. STAT. § 134.98(2); WYO. STAT. ANN. § 40-12-501(a)(i).

26. *See* CONN. GEN. STAT. § 36a-701b(a)(1); FLA. STAT. § 501.171(1)(a); N.J. STAT. ANN. § 56:8-161; N.Y. GEN. BUS. LAW § 899-aa(1)(c); P.R. LAWS ANN. tit. 10, § 4051(c); 11 R.I. GEN. LAWS § 11-49.3-3(a)(1).

27. *See* ME. REV. STAT. ANN. tit. 10, § 1347(1); MASS. GEN. LAWS ch. 93H, § 1(a); N.C. GEN. STAT. § 75-61(14); P.R. LAWS ANN. tit. 10, § 4051(c).

integrity of the protected PII. In these states, a "breach" only occurs where there has been the unauthorized access or acquisition of protected PII *that compromises* the security, confidentiality, or integrity of that PII.[28] If the facts indicate there has been no compromise to the security, confidentiality, or integrity of the PII resulting from the unauthorized access or acquisition, then it is possible to conclude no "breach" has occurred;[29] however, such

---

28. *See* ALASKA STAT. § 45.48.090(1); ARIZ. REV. STAT. § 18-551(1); ARK. CODE ANN. § 4-110-103(1); CAL. CIV. CODE § 1798.82(g); COLO. REV. STAT. § 6-1-716(1)(h); DEL. CODE ANN. tit. 6, § 12B-101(1); D.C. CODE § 28-3851(1); GA. CODE ANN. § 10-1-911(1) (applies only to Information Brokers and Data Collectors); IDAHO CODE § 28-51-104(2); 815 ILL. COMP. STAT. 530/5; IND. CODE § 24-4.9-2-2(a); IOWA CODE § 715C.1(1); KAN. STAT. ANN. § 50-7a01(h); KY. REV. STAT. ANN. § 365.732(1)(a); LA. STAT. ANN. § 51:3073(2); ME. REV. STAT. ANN. tit. 10, § 1347(1); MD. CODE ANN., COM. LAW § 14-3504(a); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.63(b); MINN. STAT. § 325E.61(1)(d); MO. ANN. STAT. § 407.1500(1)(1); MONT. CODE ANN. § 30-14-1704(4)(a); NEB. REV. STAT. § 87-802(1), (5); NEV. REV. STAT. ANN. § 603A.020; N.H. REV. STAT. ANN. § 359-C:19(V); N.J. STAT. ANN. § 56:8-161; N.M. STAT. ANN. § 57-12C-2(D); N.Y. GEN. BUS. LAW § 899-aa(1)(c); OHIO REV. CODE ANN. § 1349.19(A)(1); OKLA. STAT. tit. 24, § 162(1); OR. REV. STAT. § 646A.602(1); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4051(c); 11 R.I. GEN. LAWS § 11-49.3-3(a)(1); S.C. CODE ANN. § 39-1-90(D)(1); S.D. CODIFIED LAWS § 22-40-19(1); TENN. CODE ANN. § 47-18-2107(a)(1); TEX. BUS. & COM. CODE ANN. § 521.053(a); UTAH CODE ANN. § 13-44-102(1); VT. STAT. ANN. tit. 9, § 2430(12)(A); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(1)—(2); W. VA. CODE § 46A-2A-101(1), (6); WYO. STAT. ANN. § 40-12-501(a)(i).

29. There are a few states—namely, Alabama, Connecticut, Florida, Hawaii, Mississippi, North Carolina, North Dakota, and Wisconsin—that do not require an evaluation of "compromise" (as a concept separate from "harm" as discussed in the following section), but instead deem unauthorized access to or acquisition of the protected PII alone sufficient to constitute a "breach"—barring other exceptions (as discussed in the following sections). *See* ALA. CODE § 8-38-2(1); CONN. GEN. STAT. § 36a-701b(a)(1); FLA. STAT. § 501.171(1)(a); HAW. REV. STAT. § 487N-1; MISS. CODE ANN. § 75-24-29(2)(a);

a conclusion necessitates caution and close scrutiny of the facts, because in many instances the mere fact that there was *unauthorized* access to or acquisition of the protected PII means necessarily the security, confidentiality, or integrity of that PII has been arguably compromised.

But analysis must not stop there. Even though an investigation may have revealed facts that suggest a data "breach" has likely occurred, several common exceptions may apply that could place the data incident squarely outside the definition of a data breach and/or that obviate the need for notification under the law. These include: there is no reasonable likelihood of harm; the personal information impacted was encrypted; and the data breach was the result of the good-faith access or acquisition by an employee or agent of the organization. Each of these is discussed in greater detail below. Finally, other exceptions may apply depending on the specific state law or the type of organization (e.g., if the organization has an internal policy; if the organization is a financial institution; if the organization is an insurance company; or if the organization falls under the purview of the Gramm-Leach-Bliley Act (GLBA) or HIPAA)).

1. No Reasonable Likelihood of Harm Exists

In many states, notification may be avoided if, *after investigation*, the organization has established or has a reasonable basis to conclude that there is no reasonable likelihood that harm to the impacted individuals has resulted or will result from the breach. Thirty-six states recognize some form of this exception[30] (*see* Table VI.B.1(A) immediately below).

N.C. GEN. STAT. § 75-61(14); N.D. CENT. CODE § 51-30-01(1); WIS. STAT. § 134.98(2).

30. *See* ALA. CODE § 8-38-5(a); ALASKA STAT. § 45.48.010(c); ARIZ. REV. STAT. § 18-552(J); ARK. CODE ANN. § 4-110-105(d); COLO. REV. STAT. § 6-1-716(2)(a); CONN. GEN. STAT. § 36a-701b(b)(1); DEL. CODE ANN. tit. 6, § 12B-102(a); FLA.

Table VI.B.1(A):
"No Reasonable Likelihood of Harm" Exception

States recognizing the no-reasonable-likelihood-of-harm exception	Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Mississippi, Missouri, Nebraska, New Hampshire, New Jersey, New York, North Carolina, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, Wyoming

As discussed in greater detail below, what constitutes "reasonable likelihood of harm" varies from state to state, with some states offering greater guidance and others offering none (*see* Table VI.B.1(B): Varying Degrees of Specificity Regarding the Meaning of "Reasonable Likelihood of Harm").

STAT. § 501.171(4)(c); HAW. REV. STAT. § 487N-1; IDAHO CODE § 28-51-105(1); IND. CODE § 24-4.9-3-1(a); IOWA CODE § 715C.2(6); KAN. STAT. ANN. § 50-7a01(h); LA. STAT. ANN. § 51:3074(I); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW § 14-3504(b)(1)—(2); MICH. COMP. LAWS § 445.72(1); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(5); NEB. REV. STAT. § 87-803(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(a); N.C. GEN. STAT. § 75-61(14); OKLA. STAT. tit. 24, § 163(A)—(B); OR. REV. STAT. § 646A.604(7); 73 PA. CONS. STAT. § 2302; 11 R.I. GEN. LAWS § 11-49.3-4(a)(1); S.C. CODE ANN. § 39-1-90(A); S.D. CODIFIED LAWS § 22-40-20; UTAH CODE ANN. § 13-44-202(1)(a)—(b); VT. STAT. ANN. tit. 9, § 2435(d); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(1); W. VA. CODE § 46A-2A-102(a)—(b); WIS. STAT. § 134.98(2)(cm)(1); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

On one end of the spectrum, ten states offer little to no guidance on the meaning of "reasonable likelihood of harm": Alabama, Alaska, Arkansas, Connecticut, Louisiana, Mississippi, Oregon, Pennsylvania, South Dakota, and Washington.[31] These states provide only generally that notification is *not* required if, after reasonable investigation, the organization determines "there is not a reasonable likelihood of harm" to the impacted individuals. As the determination of whether there is reasonable likelihood of harm to the impacted individuals in these ten states is left to the organization, such a determination should be made on a case-by-case basis within the context of the facts of the incident and the findings of the forensic investigation. Notably, in the case of Connecticut, the organization must make such determination in consultation with relevant local, state, or federal law enforcement.

Other states offer more clarity as it relates to the "no harm" exception. For example, Florida, Hawaii, Indiana, Kansas, Michigan, Missouri, North Carolina, Oklahoma, Rhode Island, South Carolina, Utah, Vermont, Virginia, West Virginia, and Wisconsin define "harm" in terms of identity theft, fraud, or other illegal use.[32] In these fifteen states, notification is not required if, after reasonable investigation, the organization determines the breach

---

31. *See* ALA. CODE § 8-38-5(a); ALASKA STAT. § 45.48.010(c); ARK. CODE ANN. § 4-110-105(d); CONN. GEN. STAT. § 36a-701b(b)(1); LA. STAT. ANN. § 51:3074(I); MISS. CODE ANN. § 75-24-29(3); OR. REV. STAT. § 646A.604(8); 73 PA. CONS. STAT. § 2302; S.D. CODIFIED LAWS § 22-40-20; WASH. REV. CODE § 19.255.010(1-2).

32. FLA. STAT. § 501.171(4)(c); HAW. REV. STAT. § 487N-1; IND. CODE § 24-4.9-3-1(a); KAN. STAT. ANN. § 50-7a01(h); MICH. COMP. LAWS § 445.72(1); MO. ANN. STAT. § 407.1500(2)(5); N.M. STAT. ANN. § 57-12C-6(C); N.C. GEN. STAT. § 75-61(14); OKLA. STAT. tit. 24, § 163(A)(B); 11 R.I. GEN. LAWS § 11-49.3-4(a)(1); S.C. CODE ANN. § 39-1-90(A); UTAH CODE ANN. § 13-44-202(1)(a)—(b); VT. STAT. ANN. tit. 9, § 2435(d); VA. CODE ANN. § 18.2-186.6(B); W. VA. CODE § 46A-2A-102(a)—(b); WIS. STAT. § 134.98(2)(cm).

has not resulted or is not reasonably likely to result in identity theft, fraud, or other illegal use. Arizona, Iowa, and Florida, tie "harm" to economic loss.[33] In these three states, a data incident only rises to the level of an actionable "breach" if it "materially" compromises the security or confidentiality of the personal information *and* is reasonably likely to cause economic loss or financial harm to an individual.

Eleven other states use a slightly different metric. In Colorado, Delaware, Idaho, Maine, Maryland, Nebraska, New Hampshire, New Jersey, New York, Vermont, and Wyoming, the "no harm" exception is generally defined by the actual or potential misuse of the personal information.[34] In these eleven states, notice is *not* required if, after reasonable investigation, the organization simply determines that the misuse of the personal information has not occurred and/or is not reasonably likely to occur.

33. ARIZ. REV. STAT. § 18-552(J); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2(6).

34. COLO. REV. STAT. § 6-1-716(2)(a); DEL. CODE ANN. tit. 6, § 12B-102(a); IDAHO CODE § 28-51-105(1); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW § 14-3504(b)(2); NEB. REV. STAT. § 87-803(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(a); N.Y. GEN. BUS. LAW § 899-aa (1)(c), (2)(a); VT. STAT. ANN. tit. 9, § 2435(d); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

Table VI.B.1(B): Varying Degrees of Specificity Regarding the Meaning of "Reasonable Likelihood of Harm"

Meaning of "Reasonable Likelihood of Harm"	**States**
Reasonable likelihood of harm = **not defined**, explained, or qualified	Alabama, Alaska, Arkansas, Connecticut, Louisiana, Mississippi, Oregon, Pennsylvania, South Dakota, Washington[35]
Reasonable likelihood of harm = reasonably likely the personal information has been or will be **misused**	Colorado, Delaware, Idaho, Maine, Maryland, Nebraska, New Hampshire, New Jersey, Vermont, Wyoming[36]

35. *See* ALA. CODE § 8-38-5(a); ALASKA STAT. § 45.48.010(c); ARK. CODE ANN. § 4-110-105(d); CONN. GEN. STAT. § 36a-701b(b)(1); LA. STAT. ANN. § 51:3074(I); MISS. CODE ANN. § 75-24-29(3); OR. REV. STAT. § 646A.604(7); 73 PA. CONS. STAT. § 2302; S.D. CODIFIED LAWS § 22-40-20; WASH. REV. CODE § 19.255.010(-2).

36. COLO. REV. STAT. § 6-1-716(2)(a); DEL. CODE ANN. tit. 6, § 12B-102(a); IDAHO CODE § 28-51-105(1); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW § 14-3504(b)(2); NEB. REV. STAT. § 87-803(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(a); VT. STAT. ANN. tit. 9, § 2435(d); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

Meaning of "Reasonable Likelihood of Harm"	**States**
Reasonable likelihood of harm = reasonably likely to result in **identity theft, fraud**, or other **illegal use** of the personal information	Florida, Hawaii, Indiana, Kansas, Massachusetts, Michigan, Missouri, New Mexico, New York, North Carolina, Oklahoma, Rhode Island, South Carolina, Utah, Vermont, Virginia, West Virginia, Wisconsin[37]
Reasonable likelihood of harm = reasonably likely to cause substantial **economic loss** or **financial harm** to the individual	Arizona, Florida, Iowa[38]

As always, careful scrutiny should be paid to each applicable state law and the nuances that may exist among state laws regarding this exception, especially if the incident impacts residents in more than one state.

If, after investigation, the organization determines there is no reasonable likelihood of harm and, consistent with that conclusion, decides not to notify impacted individuals, twelve states

37. FLA. STAT. § 501.171(4)(c); HAW. REV. STAT. § 487N-1; IND. CODE § 24-4.9-3-1(a); KAN. STAT. ANN. § 50-7a01(h); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(1); MO. ANN. STAT. § 407.1500(2)(5); N.M. STAT. ANN. § 57-12C-6(C); N.Y. GEN. BUS. LAW § 899-aa (1)(c), (2)(a); N.C. GEN. STAT. § 75-61(14); OKLA. STAT. tit. 24, § 163(A)(B); 11 R.I. GEN. LAWS § 11-49.3-4(a)(1); S.C. CODE ANN. § 39-1-90(A); UTAH CODE ANN. § 13-44-202(1)(a)—(b); VT. STAT. ANN. tit. 9, § 2435(d); VA. CODE ANN. § 18.2-186.6(B); W. VA. CODE § 46A-2A-102(a)—(b); WIS. STAT. § 134.98(2)(cm).

38. ARIZ. REV. STAT. § 18-552(J); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2(6).

require the organization to document that determination and maintain that written record for three to five years, depending on the state (*see* Table VI.B.1(C) immediately below).

Table VI.B.1(C): States Requiring Documentation of "No Reasonable Likelihood of Harm" Determination

States Requiring Documentation	Length of Document Retention
Maryland, South Dakota	3 years[39]
Alabama, Alaska, Arkansas, Florida, Iowa, Louisiana, Missouri, New Jersey, New York, Oregon	5 years[40]

Some states, however, require more than internal documentation when this exception applies. For example, in Connecticut and Florida, the organization must actually "consult with" "relevant federal, state, and local agencies responsible for law enforcement" in arriving at the conclusion that the breach is not likely to result in harm to the impacted individuals.[41] In Alaska, South Dakota, and Vermont, even though an organization need not notify impacted individuals, the organization must nevertheless notify the state attorney general in writing of its determination that there is no reasonable likelihood of harm to the

39. *See* MD. CODE ANN., COM. LAW § 14-3504(b)(4); S.D. CODIFIED LAWS § 22-40-20.

40. *See* ALA. CODE § 8-38-5(f); ALASKA STAT. § 45.48.010(c); ARK. CODE ANN. § 4-110-105(g(1)); FLA. STAT. § 501.171(4)(c); IOWA CODE § 715C.2(6); LA. STAT. ANN. § 51:3074(I); MO. ANN. STAT. § 407.1500(2)(5); N.J. STAT. ANN. § 56:8-163(a); N.Y. GEN. BUS. LAW § 899-aa (1)(c), (2)(a); OR. REV. STAT. § 646A.604(7).

41. CONN. GEN. STAT. § 36a-701b(b)(1); FLA. STAT. § 501.171(4)(c); OR. REV. STAT. § 646A.604(7) ("may" consult, not required).

impacted individuals.[42] In Florida, after consultation with law enforcement, the organization is to notify the Florida Department of Legal Affairs of the "no harm" determination in writing within thirty days of making the determination.[43] Importantly, the notification and consultation required by these very few states may not be considered part of the public record and may not be open to inspection by the public, even upon request.

While it is beyond the scope of this publication generally, the European Union's General Data Protection Regulation (GDPR)[44] breach notification requirements merit mention here, especially for those entities subject to the jurisdiction of both the U.S. and the EU. Article 33 of the GDPR requires notification to the supervisory authority of a data breach "*unless* the personal data breach is *unlikely to result in a risk to the rights and freedoms of natural persons.*"[45] Article 34, the counterpart to Article 33 with regard to the notification obligations to individuals, requires notification of a data breach to the data subjects whose information was compromised *only* "[w]hen the personal data breach is *likely to result in a high risk* to the rights and freedoms of natural persons."[46]

Briefly summarized for comparative context, the GDPR uses different substantive standards for triggering notifications, to some extent incorporating the U.S. standard of "no likely risk of harm" exception followed in many states. The important distinction, however, is that Article 33 establishes a *presumption of harm,* which would have to be rebutted in order *not* to trigger notification to supervisory authorities under Article 33, whereas Article

42. ALASKA STAT. § 45.48.010(c); S.D. CODIFIED LAWS § 22-40-20; VT. STAT. ANN. tit. 9, § 2435(d).

43. FLA. STAT. § 501.171(4)(c).

44. GDPR, *supra* note 1.

45. *Id.*, Art. 33(1).

46. *Id.*, Art. 34(1).

34 allows for a more traditional risk-of-harm analysis *before* notification obligations to the individual are triggered. In addition, in contrast to U.S. state data breach notification statutes, which prioritize and place greater importance on notification to the impacted individuals, GDPR, with its presumption of harm and shorter notification window (discussed below) applicable for notification to regulators, appears to prioritize and place greater importance on notification to the supervisory authority than impacted individuals. Indeed, notification to impacted individuals is only required if the data breach is likely to result in a "high risk" to the rights and freedoms of the impacted individuals.

2. The Personal Information Was Encrypted

Because of advancements in encryption technology, virtually all U.S. jurisdictions now generally distinguish between encrypted and unencrypted personal information when defining what constitutes a "data breach" requiring notification.[47]

---

47. *See* ALA. CODE § 8-38-2(6)(b)(2); ALASKA STAT. § 45.48.090(7); ARIZ. REV. STAT. §18-551(1)(a),(3); ARK. CODE ANN. § 4-110-103(7); CAL. CIV. CODE § 1798.82(a); COLO. REV. STAT. § 6-1-716(1)(d), (g)(I)(A), (h); CONN. GEN. STAT. § 36a-701b(a); DEL. CODE ANN. tit. 6, § 12B-101(1); D.C. CODE § 28-3851(1); FLA. STAT. § 501.171(1)(g)(2); GA. CODE ANN. § 10-1-911(6); HAW. REV. STAT. § 487N-1; IDAHO CODE § 28-51-104(5); 815 ILL. COMP. STAT. 530/5; IND. CODE § 24-4.9-2-2(b)(2); IOWA CODE § 715C.1(11); KAN. STAT. ANN. § 50-7a01(b), (g)—(h); KY. REV. STAT. ANN. § 365.732(1)(a); LA. STAT. ANN. § 51:3073(4); ME. REV. STAT. ANN. tit. 10, § 1347(6); MD. CODE ANN., COM. LAW § 14-3501(c), (e)(1)(i); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(1); MINN. STAT. § 325E.61(1)(a)(e); MISS. CODE ANN. § 75-24-29(2)(a); MO. ANN. STAT. § 407.1500(1)(9); MONT. CODE ANN. § 30-14-1704(1); NEB. REV. STAT. § 87-802(1), (5); NEV. REV. STAT. ANN. § 603A.040; N.H. REV. STAT. ANN. § 359-C:19(IV)(a); N.J. STAT. ANN. § 56:8-161(10); N.M. STAT. ANN. § 57-12C-2(C)(1), (D); N.Y. GEN. BUS. LAW § 899-aa(1)(b); N.C. GEN. STAT. § 75-61(14); N.D. CENT. CODE § 51-30-01(1); OHIO REV. CODE ANN. § 1349.19(A)(7); OKLA. STAT. tit. 24, § 162(1), (3), (6); OR. REV. STAT. § 646A.602(11)(a); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4051(a); 11 R.I. GEN. LAWS § 11-

If personal information (or some element of personal information) was "encrypted" when breached, depending on the state law, then: (a) such encrypted personal information is excluded from the definition of triggering personal information; (b) the data incident falls outside the definition of a "data breach;" *or* (c) the data incident is exempted from any disclosure obligation. Although varying definitions exist, encryption generally refers to the use of a security technology or methodology that renders electronic data unusable, unreadable, or indecipherable without the use of a confidential process or key. Although all states differentiate between encrypted and unencrypted data, their treatment of such encrypted or unencrypted data may differ and, therefore, the relevant state statute should be consulted when evaluating whether notice is required in instances where encrypted data has been impacted by a data incident. Importantly, in many states, encrypted data is not considered "encrypted" or exempted from notice if the decryption key was or is reasonably believed to have been accessed or acquired during the breach.

3. The "Good Faith" Exception for Employees and Agents

Almost all states and the District of Columbia (D.C.) have an exception for the "good faith" access to, or acquisition of, personal information by employees or agents of the organization.[48]

49.3-3(a)(1), (8); S.C. CODE ANN. § 39-1-90(A), (D); S.D. CODIFIED LAWS § 22-40-19(1)—(2); TENN. CODE ANN. § 47-18-2107(a)(1), (2); TEX. BUS. & COM. CODE ANN. §§ 521.002(a)(2), 521.053(a); UTAH CODE ANN. § 13-44-102(4); VT. STAT. ANN. tit. 9, § 2430(5); VA. CODE ANN. § 18.2-186.6(A-C); WASH. REV. CODE § 19.255.010(1)—(2); W. VA. CODE § 46A-2A-101(1),(3),(6); WIS. STAT. § 134.98(1)(b); WYO. STAT. ANN. § 40-12-501(a)(vii).

48. *See* ALA. CODE § 8-38-2(1)(a); ALASKA STAT. § 45.48.050; ARIZ. REV. STAT. § 18-551(1)(b); ARK. CODE ANN. § 4-110-103(1)(B); CAL. CIV. CODE § 1798.82(g); COLO. REV. STAT. § 6-1-716(1)(h); DEL. CODE ANN. tit. 6, § 12B-101(1); D.C. CODE § 28-3851(1); FLA. STAT. § 501.171(1)(a); GA. CODE ANN.

Generally, under this exception, facts that might otherwise cause the organization to conclude that a "data breach" has occurred are neutralized if an investigation reveals that the "breach" was the result of "good faith"—though unauthorized—access to or acquisition of personal information by an employee or agent of the organization. However, in most instances, this exception only applies if: (1) the personal information was not used for a purpose unrelated to the organization's business, and (2) the employee or agent does not make a further willful unauthorized disclosure.

C. Notice Logistics: Audience, Timing, and Content

In the event an exception does not apply, and/or the organization otherwise decides notification is required, the organization must undertake several determinations to ensure that logistics-related requirements, such as audience, timing, and content, have been satisfied under the applicable data breach notification

---

§ 10-1-911(1); HAW. REV. STAT. § 487N-1; IDAHO CODE § 28-51-104(2); 815 ILL. COMP. STAT. 530/5; IND. CODE § 24-4.9-2-2(b)(1); IOWA CODE § 715C.1(1); KAN. STAT. ANN. § 50-7a01(h); KY. REV. STAT. ANN. § 365.732(1)(a); LA. STAT. ANN. § 51:3073(2); ME. REV. STAT. ANN. tit. 10, § 1347(1); MD. CODE ANN., COM. LAW § 14-3504(a)(2); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.63(3)(b); MINN. STAT. § 325E.61(1)(d); MO. ANN. STAT. § 407.1500(1)(1); MONT. CODE ANN. § 30-14-1704(4)(a); NEB. REV. STAT. § 87-802(1); NEV. REV. STAT. ANN. § 603A.020; N.H. REV. STAT. ANN. § 359-C:19(V); N.J. STAT. ANN. § 56:8-161(10);); N.M. STAT. ANN. § 57-12C-2(D); N.Y. GEN. BUS. LAW § 899-aa(1)(c); N.C. GEN. STAT. § 75-61(14); N.D. CENT. CODE § 51-30-01(1); OHIO REV. CODE ANN. § 1349.19(A)(1); OKLA. STAT. tit. 24, § 162(1); OR. REV. STAT. § 646A.602(1)(b); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4051(c); 11 R.I. GEN. LAWS § 11-49.3-3(a)(1); S.C. CODE ANN. § 39-1-90(D)(1); S.D. CODIFIED LAWS § 22-40-19(1); TENN. CODE ANN. § 47-18-2107(a)(1); TEX. BUS. & COM. CODE ANN. § 521.053(a); UTAH CODE ANN. § 13-44-102(1)(b); VT. STAT. ANN. tit. 9, § 2430(8)(B); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.005(1); W. VA. CODE § 46A-2A-101(1); WIS. STAT. § 134.98(2)(cm)(2); WYO. STAT. ANN. § 40-12-501(a)(i).

laws. These logistics-related considerations include: (1) to whom notice must be provided (e.g., individuals, state attorneys general, etc.); (2) whether notice must be provided within a specific period of time (e.g., thirty days) and in a specific sequence; and (3) the method and content required for the notice (or notices, if more than one is required). These logistics-related requirements are important aspects of notice—aspects that most state regulators scrutinize with exacting detail. Violation of certain notice-related requirements can result in fines or consumer lawsuits. As such, and especially given state law variations and nuances, organizations should consult the specific language of the applicable state statute(s) and take care in complying with each of these aspects.

1. To Whom Notice Must Be Provided

Generally, there are three groups to whom notice may be required: (1) the individuals who had their personal information accessed or acquired without authorization during the breach; (2) state or other government regulators; and/or (3) credit or consumer reporting agencies.

Depending on the circumstances of the breach, other third parties—such as Vendors, credit card companies, and insurers––may also require notification; however, notification to these other third parties is generally necessitated not by applicable law, but instead by contract. [49] This section discusses notice

49. Depending on the applicable state law, third-party vendors and third-party data brokers, collectors, processors, or aggregators (collectively "third-party vendors") may have notification obligations to the entity that owns or licenses the personal information if the third-party vendors suffer a data incident or breach that impacts the personal information of the owner or licensor (or the owner or licensor's customers or employees). If you are a third-party vendor, and you suffer a data incident or breach, you should consult the applicable state statutes to assess whether you have a statutory obligation

obligations only as provided by relevant state law. It is important to note, though, that when a data incident occurs, as with the organization's investigation into the incident and resulting notice obligations, the organization should consider whether and when it should notify these equally important other third parties. And to the extent contracts exist governing the organization's relationship with these other third parties, it is recommended that these contracts be pulled and closely reviewed at the outset of any data incident.[50]

- Notice to Individuals

  Regardless of the number of state residents impacted, all states require the organization to provide notice to *any* individual impacted by the breach. As discussed in greater detail below, the timing and content of the notice to the impacted individuals varies by state.

- Notice to Regulators

  Unlike notice to individuals, whether the organization must also provide notice to its state or other regulators varies by state and may depend upon the number of state residents impacted by the breach and/or whether the organization is a specially regulated entity. This section will focus on organizations that are *not* specially regulated (e.g., entities that are not financial institutions, or covered entities under HIPAA, etc.). Organizations that are specially regulated should refer to

to notify the data owner or licensor of a data incident or breach (beyond any contractual obligations you may have).

50. A contracts management process that collects metadata on notice requirements contained in Vendor and other third-party agreements can accelerate the review process at the time of an incident.

> the specific state statutes, as well as any applicable federal statutes, to assess whether and when notice to state and/or federal regulators is required.

With regard to organizations that are not specially regulated, the following thirty-two U.S. states and territories have laws with requirements regarding notification to regulators: Alabama, Arizona, California, Colorado, Connecticut, Florida, Hawaii, Illinois, Indiana, Iowa, Louisiana, Maine, Maryland, Massachusetts, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oregon, Rhode Island, South Carolina, South Dakota, Texas, Vermont, Virginia, Washington, and Puerto Rico[51] (*see also* Table VI.C.1(A): U.S. Jurisdictions Requiring Notice to Regulators).

As detailed in Table VI.C.1(A) below, depending on the laws of the jurisdiction(s) implicated by the breach, relevant regulators to whom notice may be required may include: (1) the state attorney general's office; (2) the consumer affairs or consumer protection divisions; and/or (3) the state police.

Of the U.S. states and territories requiring notice to relevant regulators, fourteen require notice to the relevant regulator

---

51. ALA. CODE § 8-38-6; ARIZ. REV. STAT. § 18-552(B)(2)(b); CAL. CIV. CODE § 1798.82(f); COLO. REV. STAT. § 6-1-716(2)(f); CONN. GEN. STAT. § 36a-701b(b)(2); FLA. STAT. § 501.171(3)(a); HAW. REV. STAT. § 487N-2(f); IND. CODE § 24-4.9-3-1(c); IOWA CODE § 715C.2(8); LA. ADMIN. CODE tit. 16, § 701.A; ME. REV. STAT. ANN. tit. 10, § 1348(5); MD. CODE ANN., COM. LAW § 14-3504(h); MASS. GEN. LAWS ch. 93H, § 3(b); MO. ANN. STAT. § 407.1500(2)(8); MONT. CODE ANN. § 30-14-1704(8); NEB. REV. STAT. § 87-803; N.H. REV. STAT. ANN. § 359-C:20(I)(b); N.J. STAT. ANN. § 56:8-163(12)(c); N.M. STAT. ANN. § 57-12C-10); N.Y. GEN. BUS. LAW § 899-aa(8)(a); N.C. GEN. STAT. § 75-65(e1); N.D. CENT. CODE § 51-30-02; OR. REV. STAT. § 646A.604(1)(b); P.R. LAWS ANN. tit. 10, § 4052; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); S.D. CODIFIED LAWS § 22-40-20; VT. STAT. ANN. tit. 9, § 2435(b)(3); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(2)(7).

regardless of how many residents have been impacted by the breach[52] (*see* Table VI.C.1(A): U.S. Jurisdictions Requiring Notice to Regulators). The other eighteen, however, require notice to the relevant regulator *only if* a certain minimum number of residents have been impacted by the data breach (*see* Table VI.C.1(A): U.S. Jurisdictions Requiring Notice to Regulators). These minimum thresholds range from 250 residents to 1000 or more residents.[53]

Table VI.C.1(A):
U.S. Jurisdictions Requiring Notice to Regulators

U.S. Jurisdiction	**Minimum Threshold Required**	**To Whom Regulator Notice Must Be Made**
Alabama[54]	1000+ residents	Office of the Attorney General

52. CONN. GEN. STAT. § 36a-701b(b)(2); IND. CODE § 24-4.9-3-1(c); LA. ADMIN. CODE tit. 16, § 701.A; ME. REV. STAT. ANN. tit. 10, § 1348(5); MD. CODE ANN., COM. LAW § 14-3504(h); MASS. GEN. LAWS ch. 93H, § 3(b); MONT. CODE ANN. § 30-14-1704(8); NEB. REV. STAT. § 87-803(2); N.H. REV. STAT. ANN. § 359-C:20(I)(b); N.J. STAT. ANN. § 56:8-163(12)(c); N.Y. GEN. BUS. LAW § 899-aa(8)(a); N.C. GEN. STAT. § 75-65(e1); P.R. LAWS ANN. tit. 10, § 4052; VT. STAT. ANN. tit. 9, § 2435(b)(3).

53. Ala. Code § 8-38-6(a); ARIZ. REV. STAT. § 18-552(B)(2)(b); CAL. CIV. CODE § 1798.82(f); COLO. REV. STAT. § 6-1-716(2)(f); FLA. STAT. § 501.171(3)(a); HAW. REV. STAT. § 487N-2(f); IOWA CODE § 715C.2(8); MO. ANN. STAT. § 407.1500(2)(8); N.D. CENT. CODE § 51-30-02; OR. REV. STAT. § 646A.604(1)(b); 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); S.D. Codified Laws § 22-40-20; VA. CODE ANN. § 18.2-186.6(E); WASH. REV. CODE § 19.255.010(15).

54. ALA. CODE § 8-38-6(a).

U.S. Jurisdiction	**Minimum Threshold Required**	**To Whom Regulator Notice Must Be Made**
Arizona[55]	1000+ residents	Office of the Attorney General
California[56]	500+ residents	Office of the Attorney General
Colorado[57]	500+ residents	Office of the Attorney General
Connecticut[58]	No minimum / 1+ resident	Office of the Attorney General
Florida[59]	500+ residents	Department of Legal Affairs of the Office of Attorney General
Hawaii[60]	1,000+ residents	Office of Consumer Protection
Illinois[61]	500+ residents	Office of Attorney General
Indiana[62]	No minimum / 1+ resident	Office of the Attorney General

55. ARIZ. REV. STAT. § 18-552(B)(2)(b).
56. CAL. CIV. CODE § 1798.82(f).
57. COLO. REV. STAT. § 6-1-716(2)(f).
58. CONN. GEN. STAT. § 36a-701b(b)(2).
59. FLA. STAT. § 501.171(3)(a).
60. HAW. REV. STAT. § 487N-2(f).
61. 815 ILL. COMP. STAT. 530/10
62. IND. CODE § 24-4.9-3-1(c).

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
Iowa[63]	500+ residents	Director of the Consumer Protection Division of the Iowa Office of Attorney General
Louisiana[64]	No minimum / 1+ resident	Consumer Protection Section of the Louisiana Office of the Attorney General
Maine[65]	No minimum / 1+ resident	Office of the Attorney General
Maryland[66]	No minimum / 1+ resident	Office of the Attorney General
Massachusetts[67]	No minimum / 1+ resident	Office of the Attorney General Director of Consumer Affairs and Business Regulation
Missouri[68]	1,000+ residents	Office of the Attorney General

63. IOWA CODE § 715C.2(8).
64. LA. ADMIN. CODE tit. 16, § 701.A.
65. ME. REV. STAT. ANN. tit. 10, § 1348(5).
66. MD. CODE ANN., COM. LAW § 14-3504(h).
67. MASS. GEN. LAWS ch. 93H, § 3(b).
68. MO. ANN. STAT. § 407.1500(2)(8).

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
Montana[69]	No minimum / 1+ resident	Consumer Protection Division of the Montana Office of the Attorney General
Nebraska[70]	No minimum / 1+ resident	Office of the Attorney General
New Hampshire[71]	No minimum / 1+ resident	Office of the Attorney General
New Jersey[72]	No minimum / 1+ resident	Division of State Police in the Department of Law and Public Safety of the State of New Jersey
New Mexico[73]	1,000+ residents	Office of the Attorney General
New York[74]	No minimum / 1+ resident	Office of the Attorney General; New York State Consumer Protection Board of the Department of State; Division of State Police

69. MONT. CODE ANN. § 30-14-1704(8).
70. NEB. REV. STAT. § 87-803(2).
71. N.H. REV. STAT. ANN. § 359-C:20(I)(b).
72. N.J. STAT. ANN. § 56:8-163(12)(c).
73. N.M. STAT. ANN. § 57-12C-10.
74. N.Y. GEN. BUS. LAW § 899-aa(8)(a).

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
North Carolina[75]	No minimum / 1+ resident	Consumer Protection Division of the Office of the Attorney General
North Dakota[76]	250+ residents	Office of the Attorney General
Oregon[77]	250+ residents	Oregon Attorney General's Office
Puerto Rico[78]	No minimum / 1+ resident	Department of Consumer Affairs for Puerto Rico
Rhode Island[79]	500+ residents	Office of the Attorney General
South Carolina[80]	1,000+ residents	Consumer Protection Division of the Department of Consumer Affairs for South Carolina

75. N.C. GEN. STAT. § 75-65(e1).
76. N.D. CENT. CODE § 51-30-02.
77. OR. REV. STAT. § 646A.604(1)(b).
78. P.R. LAWS ANN. tit. 10, § 4052.
79. 11 R.I. GEN. LAWS § 11-49.3-4(a)(2).
80. S.C. CODE ANN. § 39-1-90(K).

U.S. Jurisdiction	Minimum Threshold Required	To Whom Regulator Notice Must Be Made
South Dakota[81]	250+ residents	Office of the Attorney General
Texas[82]	250+ residents	Office of the Attorney General
Vermont[83]	No minimum / 1+ resident	Office of the Attorney General
Virginia[84]	1000+ residents	Office of the Attorney General
Washington[85]	500+ residents	Office of the Attorney General

Beyond minimum thresholds and timing requirements (discussed below), the majority of states and territories requiring notice to relevant regulators also dictate specific or minimum content requirements for these regulator notices. Colorado, Iowa, Puerto Rico, and South Dakota are the only U.S. states or territories (of the thirty-two that require notice to regulators) that do *not* specify what the organization's notice to the relevant regulator should contain in terms of content.[86] As discussed in greater detail below, because the content requirements vary by

81. S.D. CODIFIED LAWS § 22-40-20.

82. TEX. BUS. & COM. CODE ANN. § 521.053(i).

83. VT. STAT. ANN. tit. 9, § 2435(b)(3).

84. VA. CODE ANN. § 18.2-186.6(E).

85. WASH. REV. CODE § 19.255.010(2)(7).

86. COLO. REV. STAT. § 6-1-716(2)(f); IOWA CODE § 715C.2(8); P.R. LAWS ANN. tit. 10, § 4052; S.D. CODIFIED LAWS § 22-40-20.

jurisdiction, organizations should carefully review the relevant statutes when drafting notices to the relevant regulators.

Finally, when preparing for and making notice to a relevant regulator, in addition to the specific statute, the organization should also consult the relevant regulator's website. Consultation with the relevant regulator's website is equally as important as consulting the specific statutory language because regulator websites often have detailed information regarding notice logistics not included in the statutes. For example, the New Jersey State Police website contains a webpage devoted to cyber crimes that contains specific instructions, a telephone number, and a hyperlink for organizations making notice to the Division of State Police that are not contained in the New Jersey data breach notification statute.[87] The North Carolina data breach statute states that the organization must provide notice to the Consumer Protection Division of the North Carolina Attorney General's Office but does not specify how that notice should be made.[88] The website for the Attorney General's Office contains several webpages devoted to security breaches, including one webpage that explains that submission of any notice to the Consumer Protection Division of the Attorney General's Office must be made via the specially designated online form and portal created by the division for such notices.[89]

87. STATE OF N.J. OFFICE OF THE ATTORNEY GEN., CYBER CRIMES UNIT, N.J. STATE POLICE, http://www.njsp.org/division/investigations/cyber-crimes.shtml (last visited Dec. 2, 2019).

88. N.C. GEN. STAT. § 75-65(e1).

89. *See* JOSH STEIN, ATTORNEY GENERAL, *REPORT A SECURITY BREACH*, N.C. DEP'T OF JUST., https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id-theft/report-a-security-breach/ (last visited Dec. 2, 2019).

- Notice to Credit/Consumer Reporting Agencies

  In providing notice to consumers, and to state regulators in some instances, some jurisdictions also require the organization to contemporaneously provide notice to all credit or consumer reporting agencies, such as Experian, Equifax, and TransUnion. Whether the organization must provide notice to the credit reporting agencies varies by jurisdiction and depends upon the number of residents impacted by the breach and/or whether the organization is a specially regulated entity. This section will focus on organizations that are *not* specially regulated (e.g., entities that are not financial institutions, or covered entities under HIPAA, etc.). Organizations that are specially regulated should refer to the specific federal, state, or territorial statutes to assess whether and when notice to the credit reporting agencies may be required.

With regard to organizations that are not specially regulated, the following states and D.C. have laws with requirements regarding notification to credit or consumer reporting agencies: Alabama, Alaska, Arizona, Colorado, Florida, Georgia,[90] Hawaii, Indiana, Kansas, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, South

90. Importantly, Georgia's data breach notification laws pertain only to entities who qualify as "data collectors" or "information brokers," as defined by the statute; these are generally entities that, for a fee, are in the business of collecting, aggregating, and analyzing personal information for third parties. GA. CODE ANN. § 10-1-912(a).

Dakota, Tennessee, Texas, Vermont, Virginia, West Virginia, and Wisconsin.[91]

With the exception of Massachusetts and South Dakota, these jurisdictions require notification to the credit or consumer reporting agencies *only if* a certain minimum number of residents have been impacted by the data breach. This minimum threshold ranges from 500 to 10,000 or more and varies by jurisdiction (*see* Table VI.C.1(B): U.S. Jurisdictions Requiring Notice to Credit/Consumer Reporting Agencies). Unlike all the other states and D.C., Massachusetts requires the organization to provide notice to the credit or consumer reporting agencies *only if so directed* by the Director of Consumer Affairs and Business Regulation.[92] South Dakota, on the other hand, requires notification to

91. ALA. CODE § 8-38-7; ALASKA STAT. § 45.48.040(a); ARIZ. REV. STAT. § 18-552(B)(2)(a); COLO. REV. STAT. § 6-1-716(2)(d); D.C. CODE § 28-3852(c); FLA. STAT. § 501.171(5); GA. CODE ANN. § 10-1-912(d); HAW. REV. STAT. § 487N-2(f); IND. CODE § 24-4.9-3-1(b); KAN. STAT. ANN. § 50-7a02(f); KY. REV. STAT. ANN. § 365.732(7); ME. REV. STAT. ANN. tit. 10, § 1348(4); MD. CODE ANN., COM. LAW § 14-3506(a); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS § 445.72(8); MINN. STAT. § 325E.61(2); MO. ANN. STAT. § 407.1500(2)(8); MONT. CODE ANN. § 30-14-1704(7); NEV. REV. STAT. ANN. § 603A.220(6); N.H. REV. STAT. ANN. § 359-C:20(VI)(a); N.J. STAT. ANN. § 56:8-163(12)(f); N.M. STAT. ANN. § 57-12C-10; N.Y. GEN. BUS. LAW § 899-aa(8)(b); N.C. GEN. STAT. § 75-65(f); OHIO REV. CODE ANN. § 1349.19(G); OR. REV. STAT. § 646A.604(6); 73 PA. CONS. STAT. § 2305; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); S.D. CODIFIED LAWS § 22-40-24; TENN. CODE ANN. § 47-18-2107(g); TEX. BUS. & COM. CODE ANN. § 521.053(h); VT. STAT. ANN. tit. 9, § 2435(c); VA. CODE ANN. § 18.2-186.6(E); W. VA. CODE § 46A-2A-102(f); WIS. STAT. § 134.98(2)(br).

92. MASS. GEN. LAWS ch. 93H, § 3(b). In this sense the Massachusetts Statute appears to be an anomaly, as it is difficult to envision many circumstances in which such notice would not be directed. Given that it would be reasonable to assume that the Director of Consumer Affairs would almost always require such notice, it may be more expedient simply to notify consumer reporting agencies as a matter of course.

the consumer reporting agencies if just one South Dakota resident is impacted by the data breach.[93]

Table VI.C.1(B): U.S. Jurisdictions Requiring Notice to Credit/Consumer Reporting Agencies

U.S. Jurisdictions	Minimum Threshold Required
Minnesota, Rhode Island[94]	500+ residents
Alabama, Alaska, Arizona, Colorado, D.C., Florida, Hawaii, Indiana, Kansas, Kentucky, Maine, Maryland, Michigan, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee, Vermont, Virginia, West Virginia, Wisconsin[95]	1,000+ residents

93. S.D. CODIFIED LAWS § 22-40-24.

94. MINN. STAT. § 325E.61(2); 11 R.I. GEN. LAWS § 11-49.3-4(a)(2).

95. ALA. CODE § 8-38-7; ALASKA STAT. § 45.48.040(a); ARIZ. REV. STAT. § 18-552(B)(2)(a); COLO. REV. STAT. § 6-1-716(2)(d); D.C. CODE § 28-3852(c); FLA. STAT. § 501.171(5); HAW. REV. STAT. § 487N-2(f); IND. CODE § 24-4.9-3-1(b); KAN. STAT. ANN. § 50-7a02(f); KY. REV. STAT. ANN. § 365.732(7); ME. REV. STAT. ANN. tit. 10, § 1348(4); MD. CODE ANN., COM. LAW § 14-3506(a); MICH. COMP. LAWS § 445.72(8); MO. ANN. STAT. § 407.1500(2)(8); NEV. REV. STAT. ANN. § 603A.220(6); N.H. REV. STAT. ANN. § 359-C:20(VI)(a); N.J. STAT. ANN. § 56:8-163(f); N.M. STAT. ANN. § 57-12C-10; N.C. GEN. STAT. § 75-65(f); OHIO REV. CODE ANN. § 1349.19(G); OR. REV. STAT. § 646A.604(6); 73 PA. CONS. STAT. § 2305; S.C. CODE ANN. § 39-1-90(K); TENN. CODE ANN. § 47-18-2107(g); VT. STAT. ANN. tit. 9, § 2435(c); VA. CODE ANN. § 18.2-186.6(E); W. VA. CODE § 46A-2A-102(f); WIS. STAT. § 134.98(2)(br).

U.S. Jurisdictions	**Minimum Threshold Required**
New York[96]	5,000+ residents
Georgia, Texas[97]	10,000+ residents
Massachusetts[98]	No minimum—*only if so directed* by Director of Consumer Affairs and Business Regulation
South Dakota[99]	No minimum/1+ resident

In all of these states and D.C., assuming the minimum thresholds for impacted residents are met, if PII is compromised, the organization is required to provide notice to "all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis."[100] These "consumer reporting agencies"

96. N.Y. GEN. BUS. LAW § 899-aa(8)(b).

97. GA. CODE ANN. § 10-1-912(d); TEX. BUS. & COM. CODE ANN. § 521.053(h).

98. MASS. GEN. LAWS ch. 93H, § 3(b).

99. S.D. CODIFIED LAWS § 22-40-24.

100. ALA. CODE § 8-38-7; ALASKA STAT. § 45.48.040(a); ARIZ. REV. STAT. § 18-552(B)(2)(a); COLO. REV. STAT. § 6-1-716(2)(d); D.C. CODE § 28-3852(c); FLA. STAT. § 501.171(5); GA. CODE ANN. § 10-1-912(d); HAW. REV. STAT. § 487N-2(f); IND. CODE § 24-4.9-3-1(b); KAN. STAT. ANN. § 50-7a02(f); KY. REV. STAT. ANN. § 365.732(7); ME. REV. STAT. ANN. tit. 10, § 1348(4); MD. CODE ANN., COM. LAW § 14-3506(a); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS § 445.72(8); MINN. STAT. § 325E.61(2); MO. ANN. STAT. § 407.1500(2)(8); NEV. REV. STAT. ANN. § 603A.220(6); N.H. REV. STAT. ANN. § 359-C:20(VI)(a); N.J. STAT. ANN. § 56:8-163(12)(f); N.M. STAT. ANN. § 57-12C-10; N.Y. GEN. BUS. LAW § 899-aa(8)(b); N.C. GEN. STAT. § 75-65(f); OHIO REV. CODE ANN. § 1349.19(G); OR. REV. STAT. § 646A.604(6); 73 PA. CONS. STAT. § 2305; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(K); S.D. CODIFIED LAWS § 22-40-24; TENN. CODE ANN. § 47-18-2107(g); TEX. BUS. & COM. CODE ANN. § 521.053(h);

include Experian, Equifax, and TransUnion. For the most part, the content required for these notices to credit reporting agencies is the same under all state statutes, and includes information on the timing, distribution, and content of the individual consumer notices. However, a few states (Colorado, Maine, and Michigan) also require the notice to the agencies to include the number of impacted residents to whom notice was or will be made.[101] Further, in providing notice to these agencies, state regulations make clear that the organization should not provide the agencies with the names or other PII of the breach notice recipients.

2. Timing of Notice

When investigating and responding to a data incident, timing is always of paramount importance. Even though few states impose specific time periods to notify impacted individuals, regulators first scrutinize the timing of notification when evaluating whether the organization has satisfied data breach notification laws. It is also one of the very first things consumers and plaintiffs' attorneys scrutinize. Indeed, in regulatory inquiries and privacy litigation alike, the timing of notification to impacted individuals is often one of the most criticized aspects of a data breach, with the impacted individuals wanting to know why the organization didn't notify them sooner.

As such, when determining how swiftly notification must be made (and, therefore, how swiftly the investigation into the data incident must be conducted), there are generally two questions to answer:

- When does the notification clock start to run?

VT. STAT. ANN. tit. 9, § 2435(c); VA. CODE ANN. § 18.2-186.6(E); W. VA. CODE § 46A-2A-102(f); WIS. STAT. § 134.98(2)(br).

101. COLO. REV. STAT. § 6-1-716(2)(d); ME. REV. STAT. ANN. tit. 10, § 1348(4); MICH. COMP. LAWS § 445.72(8).

- Once the clock starts to run, how long does the organization have before it must notify impacted individuals?

Both of these criteria are subject to interpretation in most states, as explained below.

- When does the notification clock start to run?

  To reasonably assess when notification must be provided, the point from which the clock starts to run must first be determined by the organization. Though notification laws vary by U.S. jurisdiction, there are generally two points in time during a data incident from which the notification clock could start to run: (1) when the organization first discovers or is first notified of the breach; or (2) after the organization completes a reasonable and prompt investigation to determine whether, in fact, the data incident rises to the level of a "breach."

Thirty-three states, D.C., and Puerto Rico start the notification clock when the organization first discovers or is first notified of the breach and following the determination of the scope of the breach. The states joining D.C. and Puerto Rico include: Alaska, Arkansas, California, Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia and Wisconsin.[102]

102. ALASKA STAT. § 45.48.010(a)(b); ARK. CODE ANN. § 4-110-105(a)(1)(2); CAL. CIV. CODE § 1798.82(a); D.C. CODE § 28-3852(a); FLA. STAT. § 501.171(4); GA. CODE ANN. § 10-1-912(a); HAW. REV. STAT. § 487N-2(a); 815 ILL. COMP. STAT. 530/10(a); IND. CODE ANN. § 24-4.9-3-3(a); IOWA CODE § 715C.2(1); KY.

Generally, those laws provide that notice shall be provided to the impacted individuals *after* "discovering or being notified of the breach"[103] or, alternatively, *after* the organization "knows or has reason to know of a breach of security."[104]

The remaining U.S. states explicitly start the notification clock running after completion of a reasonable and prompt investigation to determine whether, in fact, a "breach" has occurred. These U.S. states include: Alabama, Arizona, Colorado, Connecticut, Delaware, Idaho, Kansas, Maine, Maryland, Mississippi, Missouri, Nebraska, New Hampshire, New Mexico, South Dakota, Utah, and Wyoming.[105] The key here is the point in time when the investigation reasonably determines that personal information belonging to residents has been "breached" as defined by the relevant law of the U.S. jurisdiction.

REV. STAT. ANN. § 365.732(2); LA. STAT. ANN. § 51:3074(E) MASS. GEN. LAWS ch. 93H, § 3(a)(b); MICH. COMP. LAWS ANN. § 445.72(4); MINN. STAT. § 325E.61(1); MONT. CODE ANN. § 30-14-1704(1); NEV. REV. STAT. ANN. § 603A.220(1); N.J. STAT. ANN. § 56:8-163(12)(a); N.Y. GEN. BUS. LAW § 899-aa(2); N.C. GEN. STAT. § 75-65(a)(b); N.D. CENT. CODE § 51-30-02; OHIO REV. CODE ANN. § 1349.19(B); OKLA. STAT. tit. 24, § 163(A); OR. REV. STAT. § 646A.604(3); 73 PA. CONS. STAT. § 2303(a); P.R. LAWS ANN. tit. 10, § 4052; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(A); TENN. CODE ANN. § 47-18-2107(b)(c); TEX. BUS. & COM. CODE ANN. § 521.053(b); VT. STAT. ANN. tit. 9, § 2435(b)(1); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(2)(8); W. VA. CODE § 46A-2A-102(a)(c); WIS. STAT. § 134.98(3).

103. *See, e.g.*, ALASKA STAT. § 45.48.010(a).

104. *See, e.g.*, MASS. GEN. LAWS ch. 93H, § 3.

105. ALA. CODE § 8-38-4(a),5(b); ARIZ. REV. STAT. § 18-552(A-B); COLO. REV. STAT. § 6-1-716(2)(a); CONN. GEN. STAT. § 36a-701b(b)(1); DEL. CODE ANN. tit. 6, § 12B-102(a); ; IDAHO CODE § 28-51-105(1); KAN. STAT. ANN. § 50-7a02(a); ME. REV. STAT. ANN. tit. 10, § 1348(1); MD. CODE ANN., COM. LAW § 14-3504(b)(1)(2); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(1)(C), (5); NEB. REV. STAT. § 87-803(1); N.H. REV. STAT. ANN. § 359-C:20(1)(a); N.M. STAT. ANN. § 57-12C-6(B)(C); ; S.D. CODIFIED LAWS § 22-40-20; UTAH CODE ANN. § 13-44-202(1)(a)(b); WYO. STAT. ANN. § 40-12-502(a).

Table VI.C.2(A):
When Does the Notification Clock Start to Run?

The notification clock is triggered after discovery or notification that personal information of residents has been improperly accessed or compromised, or after the organization knows or has reason to know of a breach of security. Notification in these states must be made without unreasonable delay and in the most expeditious time possible, allowing for the determination of the scope of the breach, and/or determination of the individuals to be contacted, to restore the reasonable integrity of the information system, and consistent with the needs of law enforcement.	Alaska, Arkansas, California, D.C., Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia, Washington, West Virginia, Wisconsin[106]
The notification clock is triggered after completion of a reasonable and prompt investigation of the security incident to determine whether, in fact, a "breach" has occurred. In these states, the statutes explicitly allow for a reasonable investigation.	Alabama, Arizona, Colorado, Connecticut, Delaware, Idaho, Kansas, Maine, Maryland, Mississippi, Missouri, Nebraska, New Hampshire, New Mexico, South Dakota, Utah, Wyoming[107]

- How long does the organization have before it must make notification to impacted individuals?

  As with many other aspects of notice, the timing requirements for notification vary by jurisdiction and depend upon whether the organization is otherwise specially regulated (e.g., as a financial institution, as an insurance company, or as a covered entity under HIPAA). This section will focus on organizations that are *not* specially regulated. Organizations that are specially regulated should refer to the specific federal, state, and territorial statutes to

---

106. ALASKA STAT. § 45.48.010(a)(b); ARK. CODE ANN. § 4-110-105(a)(1)(2); CAL. CIV. CODE § 1798.82(a); D.C. CODE § 28-3852(a); FLA. STAT. § 501.171(4); GA. CODE ANN. § 10-1-912(a); HAW. REV. STAT. § 487N-2(a); 815 ILL. COMP. STAT. 530/10(a); IND. CODE ANN. § 24-4.9-3-3(a); IOWA CODE § 715C.2(1); KY. REV. STAT. ANN. § 365.732(2); LA. STAT. ANN. § 51:3074(E) MASS. GEN. LAWS ch. 93H, § 3(a)(b); MICH. COMP. LAWS ANN. § 445.72(4); MINN. STAT. § 325E.61(1); MONT. CODE ANN. § 30-14-1704(1); NEV. REV. STAT. ANN. § 603A.220(1); N.J. STAT. ANN. § 56:8-163(12)(a); N.Y. GEN. BUS. LAW § 899-aa(2); N.C. GEN. STAT. § 75-65(a)(b); N.D. CENT. CODE § 51-30-02; OHIO REV. CODE ANN. § 1349.19(B); OKLA. STAT. tit. 24, § 163(A); OR. REV. STAT. § 646A.604(3); 73 PA. CONS. STAT. § 2303(a); P.R. LAWS ANN. tit. 10, § 4052; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); S.C. CODE ANN. § 39-1-90(A); TENN. CODE ANN. § 47-18-2107(b)(c); TEX. BUS. & COM. CODE ANN. § 521.053(b); VT. STAT. ANN. tit. 9, § 2435(b)(1); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(2)(8); W. VA. CODE § 46A-2A-102(a)(c); WIS. STAT. § 134.98(3).

107. ALA. CODE § 8-38-5(b); ARIZ. REV. STAT. § 18-552(B)(1); COLO. REV. STAT. § 6-1-716(2)(a); CONN. GEN. STAT. § 36a-701b(b)(1); DEL. CODE ANN. tit. 6, § 12B-102(a); IDAHO CODE § 28-51-105(1); KAN. STAT. ANN. § 50-7a02(a); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MD. CODE ANN., COM. LAW § 14-3504(b)(1)—(2); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(1)(C), (5); NEB. REV. STAT. § 87-803(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.M. STAT. ANN. § 57-12C-6(B)(C); S.D. CODIFIED LAWS § 22-40-20; UTAH CODE ANN. § 13-44-202(1)(a)—(b); WYO. STAT. ANN. § 40-12-502(a).

determine the timing requirements for notification.

Interestingly, once the notification clock starts to run, the vast majority of data breach notification laws actually do *not* place a specific time limit by which notification must be made. Instead, they require—rather ambiguously—that notification must be provided to impacted individuals "*in the most expeditious time possible*" and "*without unreasonable delay*."[108] In addition to D.C., U.S. states and territories providing only this vague timing expectation include: Alaska, Arkansas, California, Delaware, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Pennsylvania, Puerto Rico, South Carolina, Texas, Utah, Virginia, West Virginia, and Wyoming.[109] In these jurisdictions, while notice must be made without undue or unreasonable delay, the timing of such notice may account for the time it takes the organization to determine the scope of the breach and/or to restore

108. *See, e.g.*, ALASKA STAT. § 45.48.010(b).

109. *Id.*; ARK. CODE ANN. § 4-110-105(a)(2); CAL. CIV. CODE § 1798.82(a); DEL. CODE ANN. tit. 6, § 12B-102(a); D.C. CODE § 28-3852(a); GA. CODE ANN. § 10-1-912(a); HAW. REV. STAT. § 487N-2(a); IDAHO CODE § 28-51-105(1); 815 ILL. COMP. STAT. 530/10(a); IND. CODE § 24-4.9-3-3(a-b) IOWA CODE § 715C.2(1); KAN. STAT. ANN. § 50-7a02(a); KY. REV. STAT. ANN. § 365.732(2); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS § 445.72(1); MINN. STAT. § 325E.61(1); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(1); MONT. CODE ANN. § 30-14-1704(1); NEB. REV. STAT. § 87-803(1); NEV. REV. STAT. ANN. § 603A.220(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(12)(a); N.Y. GEN. BUS. LAW § 899-aa(2); N.C. GEN. STAT. § 75-65(a); N.D. CENT. CODE § 51-30-02; OKLA. STAT. tit. 24, § 163(A); 73 PA. CONS. STAT. § 2303(a); P.R. LAWS ANN. tit. 10, § 4052; S.C. CODE ANN. § 39-1-90(A); TEX. BUS. & COM. CODE ANN. § 521.053(b); UTAH CODE ANN. § 13-44-202(2); VA. CODE ANN. § 18.2-186.6(B); W. VA. CODE § 46A-2A-102(a)—(b); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

the reasonable integrity of the system breached (as discussed above). And, though beyond the scope of this *Guide*, notification to impacted individuals under GDPR (if required) similarly must be made "without undue delay."[110]

Though these jurisdictions do not specify an exact number of days by which notice must be provided, the organization does not have license to remain idle following the discovery or notification of a data incident. Practically speaking, this still means the organization must work as swiftly and efficiently as possible to investigate the incident, determine the scope, and restore the integrity of the breached network. As discussed in prior sections, an investigation into the facts of the data incident should begin *immediately* to determine whether the facts give rise to a "breach" as defined by applicable state law. Similarly, the moment an investigation reveals that the personal information of residents has been "breached," the organization should move as quickly as possible to provide the requisite notice to impacted individuals. Indeed, regulators may—and likely will—scrutinize in close detail when and how long it took the organization to determine the scope of the breach and/or restore network integrity and the length of time it took the organization to notify impacted individuals thereafter. Delayed notification could result in fines and litigation. Historically, regulators have not shied away from imposing such fines or initiating investigations when, among other things, the regulator determined that notification had been unreasonably or unjustifiably delayed. These cases show that in jurisdictions where timing is unspecified, there is no magic number (e.g., two weeks, one month, or two months could be too long); instead, the inquiry is fact-specific, and the organization will need to be able to show that it was moving as quickly as possible to investigate and notify.

110. GDPR, *supra* note 1, Art. 34(1).

Eighteen states actually specify a time period during which notice to impacted individuals must be made: Alabama (forty-five days), Arizona (forty-five days), Colorado (thirty days), Connecticut (ninety days), Delaware (sixty days), Florida (thirty days), Louisiana (sixty days), Maryland (forty-five days), New Mexico (forty-five days), Ohio (forty-five days), Oregon (forty-five days), Rhode Island (forty-five days), South Dakota (sixty days), Texas (sixty days), Tennessee (forty-five days), Vermont (forty-five days), Washington (thirty days), and Wisconsin (forty-five days). In Connecticut, for example, notice to impacted individuals must be made without unreasonable delay "*but not later than ninety days after* the discovery of such breach unless a shorter time is required under federal law."[111] As summarized above, in Delaware, Louisiana, South Dakota, and soon Texas, notice to impacted individuals must be made in the most expedient time possible and without unreasonable delay, "*but not later than sixty days* from the discovery of the breach."[112] In Alabama, Arizona, Maryland, New Mexico, Ohio, Oregon, Rhode Island, Tennessee, Vermont, and Wisconsin, notice to the impacted individual(s) must be made in the most expedient time possible and/or without unreasonable delay *but within or not later than forty-five days following* the organization's discovery, determination, or notification from a third-party that a breach has occurred.[113] In Florida, Colorado, and Washington, notice to impacted individuals must be made as expeditiously as practicable and without unreasonable delay "*but no [or not] later than 30 days*

111. CONN. GEN. STAT. § 36a-701b(b)(1) (emphasis added).

112. DEL. CODE ANN. tit. 6, § 12B-102(c); LA. STAT. ANN. § 51:3074(E); S.D. Codified Laws § 22-40-20, TEX. BUS. & COM. CODE ANN. § 521.053(b).

113. ALA. CODE § 8-38-5(b); ARIZ. REV. STAT. § 18-552(B); MD. CODE ANN., COM. LAW § 14-3504(b)(3); OHIO REV. CODE ANN. § 1349.19(B)(2); OR. REV. STAT. § 646A.604(3); 11 R.I. GEN. LAWS § 11-49.3-4(a)(2); TENN. CODE ANN. § 47-18-2107(b); VT. STAT. ANN. tit. 9, § 2435(b)(1); WIS. STAT. § 134.98(3).

after" the determination or discovery of a breach.[114] In South Dakota, notice to impacted individuals must be made "*not later than sixty days from*" the discovery or notification from a third-party that a breach has occurred.[115] In each of these states, the time period stipulated for notification is *subject to* the legitimate needs of law enforcement, thereby signaling that the needs of law enforcement may supersede and justifiably delay notice beyond the statutory time period.

Table VI.C.2(B):
Timing by Which Notification Must be Made to Impacted Individuals Once Notification Clock is Triggered

Notice must be made "in the most expeditious time possible" and "without undue delay."	Alaska, Arkansas, California, D.C., Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Pennsylvania, Puerto Rico, South Carolina, Utah, Virginia, West Virginia, Wyoming[116]

114. COLO. REV. STAT. § 6-1-716(2)(a); FLA. STAT. § 501.171(4)(a); WASH. REV. CODE § 19.255.010(2)(8).

115. S.D. Codified Laws § 22-40-20.

116. ALASKA STAT. § 45.48.010(b); ARK. CODE ANN. § 4-110-105(a)(2); CAL. CIV. CODE § 1798.82(a); D.C. CODE § 28-3852(a); GA. CODE ANN. § 10-1-912(a); HAW. REV. STAT. § 487N-2(a); IDAHO CODE § 28-51-105(1); 815 ILL. COMP. STAT.

Notice must be made without unreasonable delay *but "no later than ninety days after* the discovery of the breach unless a shorter time is required under federal law."	Connecticut[117]
Notice must be made in the most expedient time possible and without unreasonable delay *but "not later than* [sixty] *days*" from the discovery or notification of the breach.	Delaware, Louisiana, South Dakota, Texas[118]

530/10(a); IND. CODE § 24-4.9-3-3(a-b); IOWA CODE § 715C.2(1); KAN. STAT. ANN. § 50-7a02(a); KY. REV. STAT. ANN. § 365.732(2); ME. REV. STAT. ANN. tit. 10, § 1348(1)(B); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS § 445.72(4); MINN. STAT. § 325E.61(1); MISS. CODE ANN. § 75-24-29(3); MO. ANN. STAT. § 407.1500(2)(1); MONT. CODE ANN. § 30-14-1704(1); NEB. REV. STAT. § 87-803(1); NEV. REV. STAT. ANN. § 603A.220(1); N.H. REV. STAT. ANN. § 359-C:20(I)(a); N.J. STAT. ANN. § 56:8-163(a); N.Y. GEN. BUS. LAW § 899-aa(2); N.C. GEN. STAT. § 75-65(a); N.D. CENT. CODE § 51-30-02; OKLA. STAT. tit. 24, § 163(A); 73 PA. CONS. STAT. § 2303(a); P.R. LAWS ANN. tit. 10, § 4052; S.C. CODE ANN. § 39-1-90(A);; UTAH CODE ANN. § 13-44-202(2); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(16); W. VA. CODE § 46A-2A-102(a)—(c); WYO. STAT. ANN. §§ 40-12-501(a)(i), 40-12-502(a).

117. CONN. GEN. STAT. § 36a-701b(b)(1).

118. DEL. CODE ANN. tit. 6, § 12B-102(c); LA. STAT. ANN. § 51:3074(E); S.D. CODIFIED LAWS § 22-40-20, TEX. BUS. & COM. CODE ANN. § 521.053(b).

Notice must be made in the most expedient time possible and without unreasonable delay *but "not later than* [forty-five] *days*" from the discovery of the breach.	Alabama, Arizona, Maryland, New Mexico, Ohio, Oregon, Rhode Island, Tennessee, Vermont (if the collector has previously submitted to the Vermont Attorney General a sworn statement regarding the data collector's data security policies), Wisconsin[119]
Notice must be made as expeditiously as practicable and without unreasonable delay *but "no later than thirty days after"* the determination of a breach.	Colorado, Florida, Washington[120]

- If required, when should notice be made to regulators?

  The majority of jurisdictions with requirements regarding notification to relevant regulators generally require, either implicitly or explicitly, that notice be made contemporaneously with notice to the impacted residents. However, a few jurisdictions have enunciated timing-specific requirements for notice to regulators.

119. ALA. CODE § 8-38-5(b); ARIZ. REV. STAT. § 18-552(B); MD. CODE ANN., COM. LAW § 14-3504(b)(3); N.M. STAT. ANN. § 57-12C-6(A)(C); OHIO REV. CODE ANN. § 1349.19(B)(2); OR. REV. STAT. § 646A.604(3)(a); R.I. GEN. LAWS § 11-49.3-4(a)(2); TENN. CODE ANN. § 47-18-2107(b); VT. STAT. ANN. tit. 9, § 2435(b)(1); WIS. STAT. § 134.98(3).

120. COLO. REV. STAT. § 6-1-716(2)(a); FLA. STAT. § 501.171(4)(a); WASH. REV. CODE § 19.255.010(2)(8).

In Maryland and New Jersey, notice to the relevant state regulators, if required, must always be made *prior to* the organization's notice to impacted individuals.[121] In Vermont, notification to the Attorney General is required within fourteen business days of the discovery of the breach or when the entity gives notification to impacted individuals, whichever is sooner.[122] If, however, the organization has previously filed a sworn submission with the Vermont Attorney General attesting to the organization's written information security and incident response policies and procedures, then it need only notify the Attorney General prior to notifying impacted individuals (which thereby obviates the fourteen-business-day notification rule, assuming notification to impacted individuals occurs more than fourteen business days from the date of discovering the breach).[123] In Alabama, Arizona, Colorado, Florida, Iowa, Louisiana, South Dakota, Vermont, and Washington, notice must be made within a specified time after either the determination of the breach or the notice to impacted individuals.[124]

121. MD. CODE ANN., COM. LAW § 14-3504(h); N.J. STAT. ANN. § 56:8-163(12)(c)(1).

122. VT. STAT. ANN. tit. 9, § 2435(b)(3)(B)(i).

123. VT. STAT. ANN. tit. 9, § 2435(b)(3)(B)(i)—(ii).

124. ALA. CODE § 8-38-6(a); ARIZ. REV. STAT. § 18-552(B)(2)(b); FLA. STAT. § 501.171(3)(a); IOWA CODE § 715C.2(8); LA. ADMIN. CODE tit. 16, § 701(B); VT. STAT. ANN. tit. 9, § 2435(b)(3).

Table VI.C.2(C):
Timing by Which Notification Must be Made to State Regulatory Authorities (If Specified by Statute)

Notice *Prior to* Notice to Individuals	Maryland,[125] New Jersey, Vermont (unless requisite sworn statement previously submitted to Attorney General)[126]
Within five business days after giving notice of the breach of security to any consumer	Iowa
Within ten days of distribution of notice to residents	Louisiana[127]
Within fourteen business days of "discovery of the security breach or when the data collector provides notice to consumers," whichever is sooner (if no previously sworn statement filed with Vermont Attorney General)	Vermont[128]

125. MD. CODE ANN., COM. LAW § 14-3504(h); N.J. STAT. ANN. § 56:8-163(12)(c)(1).

126. VT. STAT. ANN. tit. 9, § 2435(b)(3)(B)(i)—(ii).

127. LA. ADMIN. CODE tit. 16, § 701(B).

128. VT. STAT. ANN. tit. 9, § 2435(b)(3)(B)(i)—(ii).

No later than thirty days after discovery of or determination that breach occurred.	Colorado, Florida, Washington[129]
Within forty-five days after determination that a breach has occurred.	Arizona, New Mexico, Rhode Island[130]
Within forty-five days of "notice from a third-party agent that a breach has occurred or upon the entity's determination that a breach has occurred and is reasonably likely to cause substantial harm."	Alabama[131]
Within 60 days "from the discovery or notification of the breach of system security."	South Dakota, Texas[132]

Again, though beyond the scope of the *Guide*, and in stark contrast to the timing requirements of U.S. state data breach notification laws, the GDPR mandates notification of a data breach to the applicable EU supervisory authority "without undue delay and, where feasible, *not later than 72 hours after* having

129. COLO. REV. STAT. § 6-1-716(2)(f); FLA. STAT. § 501.171(3)(a); WASH. REV. CODE § 19.255.010(2)(8).

130. ARIZ. REV. STAT. § 18-552(B)(2)(b); N.M. STAT. ANN. § 57-12C-10; 11 R.I. GEN. LAWS § 11-49.3-4(a)(2).

131. ALA. CODE § 8-38-6(a).

132. S.D. CODIFIED LAWS § 22-40-20; TEX. BUS. & COM. CODE ANN. § 521.053(b).

become aware" of the breach.[133] As discussed above, this mandate, again, appears to prioritize and place greater importance on notification to the supervisory authority than the impacted individuals—requiring notification to be made to the authorities not later than seventy-two hours after becoming aware of a breach, in contrast to the requirement that notification to impacted individuals need only be made (if at all) "without undue delay." Not surprisingly, the question of when an entity "becomes aware" of a "breach" (which is defined broadly to encompass any manner of data incidents) and, thus, when the seventy-two-hour clock starts running has caused much anxiety and debate among practitioners and organizations alike.

The GDPR's notification requirements are extremely important for U.S. practitioners to keep in mind when taking into account more nuanced incident response considerations for organizations subject to both GDPR and U.S. data breach laws. For example, in the initial run-up to the effective date of GDPR, some consultants reportedly advised that an incident response plan should invoke automatic notification under any circumstance that even suggests a data compromise, in order to avoid any risk of enforcement in the EU under Article 33. An incident response plan incorporating that default trigger could, however, create other unintended consequences for multinational public companies also doing business in the U.S. Specifically, a more nuanced incident response plan may want to consider more carefully the merits of an automatic notification default at the first hint of data compromise, since that notification might in turn require similar notifications in the U.S. (with potentially only seventy-two hours to contemplate the consequences). This concern would be especially important when assessing the other potential disclosure

133. GDPR, *supra* note 1, Art. 33(1).

consequences that must be considered by publicly traded companies.

- If required, when should notice be made to credit reporting agencies?

  With the exception of Arizona, Minnesota, and New Mexico, there is no specific period of time within which notice to the credit reporting agencies must be made. Generally, the jurisdiction's statutes provide that notice, if required, should be made to the credit reporting agencies contemporaneously with individual consumer notices and "without unreasonable delay." In Arizona and New Mexico, consistent with the timing requirements for notification to individuals and the state attorneys general, notification to credit reporting agencies must be made "within forty-five days after" the determination that a breach has occurred.[134] Minnesota, on the other hand, requires notice to be made to the credit reporting agencies within forty-eight hours of when a "person discovers circumstances requiring notification" for breaches involving more than 500 residents.[135] Arguably, Minnesota's unusual phrasing could be read to require notifications to credit reporting agencies within forty-eight hours after the breach is first discovered, well in advance of any required notice to impacted residents.[136]

134. ARIZ. REV. STAT. § 18-552(B)(2)(a); N.M. STAT. ANN. § 57-12C-10.

135. MINN. STAT. § 325E.61(2).

136. *Id*.

- Delay of notice due to law enforcement

  Across all U.S. jurisdictions, regardless of whether the data breach notification laws contain vague or very specific timing requirements or permit notification to occur after a reasonable investigation to determine the scope of the breach or restore the integrity of impacted systems, there is generally only one justifiable reason for delaying notification: if law enforcement has determined that notification will impede or interfere with an ongoing investigation. Indeed, delay arguably could be mandatory in Alabama, Connecticut, Delaware, Florida, Hawaii, Mississippi, New Jersey, North Carolina, Vermont, and Wisconsin, as noted in the table below.[137] In other jurisdictions, however, delaying notification after law enforcement has made a determination that notification will impede or interfere with an ongoing investigation is merely optional, including in Alaska, Arizona, Arkansas, California, Colorado, D.C., Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West

137. ALA. CODE § 8-38-5(c); CONN. GEN. STAT. § 36a-701b(2)(d) DEL. CODE ANN. tit. 6, § 12B-102(c)(2); FLA. STAT. § 501.171(4)(b); HAW. REV. STAT. § 487N-2(c); MISS. CODE ANN. § 75-24-29(5); N.J. STAT. ANN. 56:8-163(12)(c)(2); N.C. GEN. STAT. § 75-65(c); VT. STAT. ANN. tit. 9, § 2435(b)(4); WIS. STAT. §134.98(5).

Virginia, and Wyoming.[138] In fact, there may be some very good practical, nonlegal reasons *not* to delay notification and, therefore, the organization will want to strategically consider whether to delay notification when it is optional.

138. ALASKA STAT. § 45.48.020; ARIZ. REV. STAT. § 18-552(D); ARK. CODE ANN. § 4-110-105(c); CAL. CIV. CODE § 1798.82(c); COLO. REV. STAT. § 6-1-716(2)(c); D.C. CODE § 28-3852(d); GA. CODE ANN. § 10-1-912(c); IDAHO CODE § 28-51-105(3); 815 ILL. COMP. STAT. 530/10(b-5); IND. CODE ANN. § 24-4.9-3-3(a)(3); IOWA CODE § 715C.2(3)); KAN. STAT. ANN. § 50-7a02(c); KY. REV. STAT. ANN. § 365.732(4); LA. STAT. ANN. § 51:3074(F); ME. REV. STAT. ANN. tit. 10, § 1348(3); MD. CODE ANN., COM. LAW § 14-3504(d); MASS. GEN. LAWS ch. 93H, § 4; MICH. COMP. LAWS ANN. § 445.72(4); MINN. STAT. § 325E.61(1)(c); MO. ANN. STAT. § 407.1500(2)(3); MONT. CODE ANN. § 30-14-1704(3); NEB. REV. STAT. § 87-803(4); NEV. REV. STAT. ANN. § 603A.220(3); N.H. REV. STAT. ANN. § 359-C:20(II); N.M. Stat. Ann. § 57-12C-9(A); N.Y. GEN. BUS. LAW § 899-aa(4); N.D. CENT. CODE § 51-30-04; OHIO REV. CODE ANN. § 1349.19(D); OKLA. STAT. tit. 24, § 163(D); OR. REV. STAT. § 646A.604(3)(c); 73 PA. CONS. STAT. § 2304; 11 R.I. GEN. LAWS § 11-49.3-4(b); S.C. CODE ANN. § 39-1-90(C); S.D. Codified Laws § 22-40-21; TENN. CODE ANN. § 47-18-2107(d); TEX. BUS. & COM. CODE ANN. § 521.053(d); UTAH CODE ANN. § 13-44-202(4); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(2)(3); W. VA. CODE § 46A-2A-102(e); WIS. STAT. §134.98(5); WYO. STAT. ANN. § 40-12-502(b).

Table VI.C.2(D): U.S. Jurisdictions That Allow Delay of Notice Due to Law Enforcement

Notice must be delayed if law enforcement determines that notice may impede or interfere with an ongoing investigation.	Alabama, Connecticut, Delaware, Florida, Hawaii, Mississippi, New Jersey, North Carolina, Vermont, Wisconsin[139]
Notice may be delayed if law enforcement determines that notice may impede or interfere with an ongoing investigation.	Alaska, Arizona, Arkansas, California, Colorado, D.C., Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wyoming[140]

3. Method and Content of Notice

Much like the other logistics-related notice requirements, the method and content requirements for notification varies by

139. ALA. CODE § 8-38-5(c); CONN. GEN. STAT. § 36a-701b(2)(d); DEL. CODE ANN. tit. 6, § 12B-102©(2)); FLA. STAT. § 501.171(4)(b); HAW. REV. STAT. § 487N-2(c); MISS. CODE ANN. § 75-24-29(5); N.J. STAT. ANN. 56:8-163(12)(c)(2); N.C. GEN. STAT. § 75-65(c); VT. STAT. ANN. tit. 9, § 2435(b)(4); WIS. STAT. §134.98(5).

jurisdiction and, therefore, the organization must carefully review the applicable statutory language to ensure compliance with the law of the jurisdiction, especially if the breach implicates individuals from more than one jurisdiction. Again, as with prior sections, this section addresses only those content requirements for organizations that are not specially regulated. Organizations that are specially regulated (e.g., via HIPAA or the GLBA) should refer to the specific statutes of states, territories, and D.C., as well as any applicable federal statutes, to determine the form and content requirements for notification.

- Method of Notice to Impacted Individuals

  Notice can be made to impacted individuals in one of several ways, depending on the facts and the applicable laws in each jurisdiction: (1) via written letter, (2) via email, (3) by telephone, or (4) via "substitute" notice. Not just one method need be employed; the facts and circumstances of a

140. ALASKA STAT. § 45.48.020; ARIZ. REV. STAT. § 18-552(D); ARK. CODE ANN. § 4-110-105(c); CAL. CIV. CODE § 1798.82(c); COLO. REV. STAT. § 6-1-716(2)(c); D.C. CODE § 28-3852(d); GA. CODE ANN. § 10-1-912(c); IDAHO CODE § 28-51-105(3); 815 ILL. COMP. STAT. 530/10(b-5); IND. CODE § 24-4.9-3-3(a)(3); IOWA CODE § 715C.2(3); KAN. STAT. ANN. § 50-7a02(c); KY. REV. STAT. ANN. § 365.732(4); LA. STAT. ANN. § 51:3074(F); ME. REV. STAT. ANN. tit. 10, § 1348(3); MD. CODE ANN., COM. LAW § 14-3504(d); MASS. GEN. LAWS ch. 93H, § 4; MICH. COMP. LAWS § 445.72(4); MINN. STAT. § 325E.61(1)(c); MO. ANN. STAT. § 407.1500(2)(3); MONT. CODE ANN. § 30-14-1704(3); NEB. REV. STAT. § 87-803(4); NEV. REV. STAT. ANN. § 603A.220(3); N.H. REV. STAT. ANN. § 359-C:20(II); N.M. STAT. ANN. § 57-12C-9(A); N.Y. GEN. BUS. LAW § 899-aa(4); N.D. CENT. CODE § 51-30-04; OHIO REV. CODE ANN. § 1349.19(D); OKLA. STAT. tit. 24, § 163(D); OR. REV. STAT. § 646A.604(3)(b); 73 PA. CONS. STAT. § 2304; 11 R.I. GEN. LAWS § 11-49.3-4(b); S.C. CODE ANN. § 39-1-90(C); S.D. CODIFIED LAWS § 22-40-21; TENN. CODE ANN. § 47-18-2107(d); TEX. BUS. & COM. CODE ANN. § 521.053(d); UTAH CODE ANN. § 13-44-202(4); VA. CODE ANN. § 18.2-186.6(B); WASH. REV. CODE § 19.255.010(2)(3); W. VA. CODE § 46A-2A-102(e); WYO. STAT. ANN. § 40-12-502(b).

particular data breach may necessitate the use of one or more of the above methods.

- Letter Notice

  Every jurisdiction that has a data breach notification law permits notice to be made to impacted individuals by direct, written letter via U.S. mail. To utilize this direct method of notice, the organization will need to have contact information for the impacted individuals. Thus, whether the organization will be able to send written notice will depend upon whether the organization was able to identify with certainty all of the individuals impacted by the breach and has contact information for those identifiable individuals. As discussed in greater detail below, to the extent the impacted individual resides in a jurisdiction that has enunciated specific content for the notice, the written notice letter will need to include that statutory content.

- Email Notice

  Email notice is generally permissible in almost all jurisdictions with data breach notification laws; however, depending on the jurisdiction, certain criteria may need to be satisfied first before email can be utilized as a method of notice. These criteria could include: (1) if the organization has a preexisting business relationship with the impacted individual(s);[141] (2) if the impacted individual(s) has expressly consented to receive electronic notices under the Electronic Signatures in Global and

141. MICH. COMP. LAWS § 445.72(5)(b); 73 PA. CONS. STAT. § 2302; VA. CODE ANN. § 18.2-186.6(B).

National Commerce Act, codified at 15 U.S.C. §§ 7001–7031 ("ESIGN"),[142] or has otherwise expressed consent to receive such notices;[143] (3) if the

---

142. The salient provisions of this requirement include the following:
- The customer has consented to receive communication by email and not withdrawn the consent.
- The customer was provided a clear and conspicuous statement:
  - informing her of her right to have records made available in paper form and the right to withdraw consent;
  - informing her of what transactions the consent applies to;
  - describing the procedures required to withdraw consent;
  - describing how the customer may get a paper copy; and
  - describing the hardware and software requirements to access electronic records.

143. ALASKA STAT. § 45.48.030(2); ARK. CODE ANN. § 4-110-105(e)(2); CAL. CIV. CODE § 1798.82(j)(2); COLO. REV. STAT. § 6-1-716(1)(f)(III); CONN. GEN. STAT. § 36a-701b(e)(3); DEL. CODE ANN. tit. 6, § 12B-101(5)(c); D.C. CODE § 28-3851(2)(B); GA. CODE ANN. § 10-1-911(4)(C); HAW. REV. STAT. § 487N-2(e)(2); IDAHO CODE § 28-51-104(4)(c); 815 ILL. COMP. STAT. 530/10(c)(2); IOWA CODE § 715C.2(4)(b); KAN. STAT. ANN. § 50-7a01(c)(2); KY. REV. STAT. ANN. § 365.732(5)(b); LA. STAT. ANN. § 51:3074(G)(2); ME. REV. STAT. ANN. tit. 10, § 1347(4)(B); MD. CODE ANN., COM. LAW § 14-3504(e)(2); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(5)(b); MINN. STAT. § 325E.61(1)(g)(2); MISS. CODE ANN. § 75-24-29(6)(c); MO. ANN. STAT. § 407.1500(2)(6)(b); MONT. CODE ANN. § 30-14-1704(5)(a)(ii); NEB. REV. STAT. § 87-802(4)(c); NEV. REV. STAT. ANN. § 603A.220(4)(b); N.J. STAT. ANN. § 56:8-163(12)(d); N.M. STAT. ANN. § 57-12C-6(D)(2); N.Y. GEN. BUS. LAW § 899-aa(5)(b); N.C. GEN. STAT. § 75-65(e)(2); N.D. CENT. CODE § 51-30-05(2); OR. REV. STAT. § 646A.604(4)(b); P.R. LAWS ANN. tit. 10, § 4053(1); 11 R.I. GEN. LAWS § 11-49.3-3(c)(ii); S.C. CODE ANN. § 39-1-90(E)(2); TENN. CODE ANN. § 47-18-2107(e)(2); TEX. BUS. & COM. CODE ANN. § 521.053(e)(2); UTAH CODE

organization primarily conducts its business through internet account transactions or on the internet generally;[144] and/or (4) if the organization previously used email to communicate with the impacted individual(s) or if email was the primary method of communicating with the impacted individual(s).[145] To the extent the organization is contemplating notice via email, it should scrutinize the applicable law of the jurisdiction to ensure the facts satisfy the preconditions required to effect notice by email. By way of example, New York allows it if the customer has consented, but not if consent was required as a condition to doing business electronically.[146]

ANN. § 13-44-202(5)(a)(ii); VT. STAT. ANN. tit. 9, § 2435(b)(6)(A)(ii); WASH. REV. CODE § 19.255.010(2)(4)(b); W. VA. CODE § 46A-2A-101(7)(C).

144. MD. CODE ANN., COM. LAW § 14-3504(e)(2); MICH. COMP. LAWS § 445.72(5)(b).

145. ALA. CODE § 8-38-5(d); ALASKA STAT. § 45.48.030(2); ARIZ. REV. STAT. § 18-552(F)(2); COLO. REV. STAT. § 6-1-716(1)(f)(III); FLA. STAT. § 501.171(4)(d)(2); IND. CODE § 24-4.9-3-4(a)(4); IOWA CODE § 715C.2(4)(b); MINN. STAT. § 325E.61(1)(g)(2); MISS. CODE ANN. § 75-24-29(6)(c); N.H. REV. STAT. ANN. § 359-C:20(III)(b); OHIO REV. CODE ANN. § 1349.19(E)(2); OKLA. STAT. tit. 24, § 162(7)(c); OR. REV. STAT. § 646A.604(4)(b); S.C. CODE ANN. § 39-1-90(E)(2); S.D. CODIFIED LAWS § 22-40-22(2); UTAH CODE ANN. § 13-44-202(5)(a)(ii); VT. STAT. ANN. tit. 9, § 2435(b)(6)(A)(ii); VA. CODE ANN. § 18.2-186.6(A); WIS. STAT. § 134.98(3)(b); WYO. STAT. ANN. § 40-12-502(d).

146. N.Y. GEN. BUS. LAW § 899-aa(5)(b). The following states and DC require compliance with ESIGN to qualify for electronic-only notice: Arkansas; California; Connecticut; Delaware; Georgia; Hawaii; Idaho; Illinois; Kansas; Kentucky; Louisiana; Maine; Massachusetts; Missouri; Montana; Nevada; New Jersey; North Carolina; North Dakota; Rhode Island; Tennessee; Texas; Washington; West Virginia.

- Telephonic Notice

  Telephonic notice is also permissible, though not in every jurisdiction. To the extent the organization has neither a mailing address nor an email address for an impacted individual, but it does have a telephone number, the organization should carefully review the relevant data breach notification law to ensure telephonic notice is permissible; otherwise, the organization may have to make substitute notice (as discussed below). The following states permit telephonic notice generally: Arizona, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Indiana, Maryland, Michigan, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, Utah, Vermont, Virginia, West Virginia, and Wisconsin.[147] Depending on the state, however, certain criteria may have to be satisfied to permit telephonic

147. ARIZ. REV. STAT. § 18-552(F)(3); COLO. REV. STAT. § 6-1-716(1)(f)(II); CONN. GEN. STAT. § 36a-701b(e)(2); DEL. CODE ANN. tit. 6, § 12B-101(5)(b); GA. CODE ANN. § 10-1-911(4)(B); HAW. REV. STAT. § 487N-2(e)(3); IDAHO CODE § 28-51-104(4)(b); IND. CODE § 24-4.9-3-4(a)(2); MD. CODE ANN., COM. LAW § 14-3504(e)(3); MICH. COMP. LAWS ANN. § 445.72(5)(c); MISS. CODE ANN. § 75-24-29(6)(b); MO. ANN. STAT. § 407.1500(2)(6)(c); MONT. CODE ANN. § 30-14-1704(5)(a)(iii); NEB. REV. STAT. § 87-802(4)(b); N.H. REV. STAT. ANN. § 359-C:20(III)(c); N.Y. GEN. BUS. LAW § 899-aa(5)(c); N.C. GEN. STAT. § 75-65(e)(3); OHIO REV. CODE ANN. § 1349.19(E)(3); OKLA. STAT. tit. 24, § 162(7)(b); OR. REV. STAT. § 646A.604(4)(c); 73 PA. CONS. STAT. § 2302; S.C. CODE ANN. § 39-1-90(E)(3); UTAH CODE ANN. § 13-44-202(5)(a)(iii); VT. STAT. ANN. tit. 9, § 2435(b)(6)(A)(iii); VA. CODE ANN. § 18.2-186.6(A); W. VA. CODE § 46A-2A-101(7)(B); WIS. STAT. §134.98(3)(c).

notice, such as keeping a log of the call,[148] speaking directly with the impacted individual (i.e., not simply leaving a voicemail),[149] or notifying by telephone only if the organization has previously communicated with the impacted individual by telephone.[150]

- Substitute Notice

  Substitute notice is a legal construct devised by regulators to assist organizations in notifying impacted individuals of a data breach when the organization does not have sufficient contact information for the impacted individuals or the population of impacted individuals exceeds a certain threshold, such that direct notice would be inefficient and/or cost prohibitive. Substitute notice generally consists of two to three forms of communication: (1) a "conspicuous" publication of the notice to the organization's website; (2) publication of the notice in "major statewide media;" and/or (3) general email notice where email addresses for impacted individuals are available.[151] The

148. N.H. REV. STAT. ANN. § 359-C:20(III)(c); N.Y. GEN. BUS. LAW § 899-aa(5)(c).

149. ARIZ. REV. STAT. § 18-552(F)(3); HAW. REV. STAT. § 487N-2(e)(3); MICH. COMP. LAWS § 445.72(5)(c); MO. ANN. STAT. § 407.1500(2)(6)(c); N.C. GEN. STAT. § 75-65(e)(3); OR. REV. STAT. § 646A.604(4)(c); VT. STAT. ANN. tit. 9, § 2435(b)(6)(A)(iii).

150. WIS. STAT. § 134.98(3)(b).

151. ALA. CODE § 8-38-5(e)(2); ALASKA STAT. § 45.48.030(3); ARIZ. REV. STAT. § 18-552(F)(4); ARK. CODE ANN. § 4-110-105(e)(3)(B); CAL. CIV. CODE § 1798.82(j)(3); COLO. REV. STAT. § 6-1-716(1)(f)(IV); CONN. GEN. STAT. § 36a-701b(e)(4); DEL. CODE ANN. tit. 6, § 12B-101(3)(d); D.C. CODE § 28-3851(2)(C)(ii); FLA. STAT. § 501.171(4)(f); GA. CODE ANN. § 10-1-911(4)(D); HAW. REV. STAT. § 487N-2(e)(4); IDAHO CODE § 28-51-104(4)(d); 815 ILL. COMP.

requirements for substitute notice (e.g., how long the website notice must be maintained, or the media that are acceptable for publication) will vary by jurisdiction; and, therefore, to the extent the organization is contemplating substitute notice, it should consult each applicable law for guidance. Although substitute notice is generally permissible in all jurisdictions with data breach notification laws, certain prerequisites must be met before utilizing the substitute notice mechanism. These criteria, which vary by jurisdiction, could include: (1) the impacted class of individuals exceeds a certain threshold (ranging from in excess of 1,000 to 500,000 persons); (2) the cost of providing direct notice to the class of impacted individuals exceeds a certain minimum amount (ranging from in excess of $5,000 to $250,000); and/or (3) the

---

STAT. 530/10(c)(3); IND. CODE § 24-4.9-3-4(b); IOWA CODE § 715C.2(4)(c); KAN. STAT. ANN. § 50-7a01(c)(3); KY. REV. STAT. ANN. § 365.732(5)(c); LA. STAT. ANN. § 51:3074(G)(3); ME. REV. STAT. ANN. tit. 10, § 1347(4)(C); MD. CODE ANN., COM. LAW § 14-3504(f); MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(5)(d); MINN. STAT. § 325E.61(1)(g)(3); MISS. CODE ANN. § 75-24-29(6)(d); MO. ANN. STAT. § 407.1500(2)(6)(d); MONT. CODE ANN. § 30-14-1704(5)(a)(iv); NEB. REV. STAT. § 87-802(4)(d); NEV. REV. STAT. ANN. § 603A.220(4)(c); N.H. REV. STAT. ANN. § 359-C:20(III)(d); N.J. STAT. ANN. § 56:8-163(12)(d)(3); N.M. STAT. ANN. § 57-12C-6(D)(3); N.Y. GEN. BUS. LAW § 899-aa(5)(d); N.C. GEN. STAT. § 75-65(e)(4); N.D. CENT. CODE § 51-30-05(3); OHIO REV. CODE ANN. § 1349.19(E)(4); OKLA. STAT. tit. 24, § 162(7)(d); OR. REV. STAT. § 646A.604(4)(d); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4053(2); 11 R.I. GEN. LAWS § 11-49.3-3(c)(iii); S.C. CODE ANN. § 39-1-90(E)(4); S.D. CODIFIED LAWS § 22-40-22(3); TENN. CODE ANN. § 47-18-2107(e)(3); TEX. BUS. & COM. CODE ANN. § 521.053(f); UTAH CODE ANN. § 13-44-202(5)(a)(iv); VT. STAT. ANN. tit. 9, § 2435(b)(6)(B); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(2)(4)(c); W. VA. CODE § 46A-2A-101(7)(D); WYO. STAT. ANN. § 40-12-502(d)(iii).

organization does not have sufficient contact information for impacted individuals to notify them directly.[152]

Once the appropriate method of notification has been determined, the organization must next determine the content required for the notice.

- Contents of Notice to Impacted Individuals

  Though the content of the notice is arguably one of the most important aspects of the notice process, well over half of the states, territories, and D.C. do *not* have any specific content requirements written into their statutes, including: Alaska, Arkansas,

152. ALA. CODE § 8-38-5(e)(1); ALASKA STAT. § 45.48.030(3); ARIZ. REV. STAT. § 18-552(F)(4); ARK. CODE ANN. § 4-110-105(e)(3)(A); CAL. CIV. CODE § 1798.82(j)(3); COLO. REV. STAT. § 6-1-716(1)(f)(IV); CONN. GEN. STAT. § 36a-701b(e)(4); DEL. CODE ANN. tit. 6, § 12B-101(5)(d); D.C. CODE § 28-3851(2)(C)(i); FLA. STAT. § 501.171(4)(f); GA. CODE ANN. § 10-1-911(4)(D); HAW. REV. STAT. § 487N-2(e)(4); IDAHO CODE § 28-51-104(4)(d); 815 ILL. COMP. STAT. 530/10(c)(3); IND. CODE § 24-4.9-3-4(b); IOWA CODE § 715C.2(4)(c); KAN. STAT. ANN. § 50-7a01(c)(3); KY. REV. STAT. ANN. § 365.732(5)(c); LA. STAT. ANN. § 51:3074(G)(3); ME. REV. STAT. ANN. tit. 10, § 1347(4)(C); MD. CODE ANN., COM. LAW § 14-3504(f; MASS. GEN. LAWS ch. 93H, § 1(a); MICH. COMP. LAWS § 445.72(5)(d); MINN. STAT. § 325E.61(1)(g)(3); MISS. CODE ANN. § 75-24-29(6)(d); MO. ANN. STAT. § 407.1500(2)(7); MONT. CODE ANN. § 30-14-1704(5)(a)(iv); NEB. REV. STAT. § 87-802(4)(d); NEV. REV. STAT. ANN. § 603A.220(4)(c); N.H. REV. STAT. ANN. § 359-C:20(III)(d); N.J. STAT. ANN. § 56:8-163(12)(d)(3); N.M. STAT. ANN. § 57-12C-6(D)(3); N.Y. GEN. BUS. LAW § 899-aa(5)(d); N.C. GEN. STAT. § 75-65(e)(4); N.D. CENT. CODE § 51-30-05(3); OHIO REV. CODE ANN. § 1349.19(E)(4); OKLA. STAT. tit. 24, § 162(7)(d); OR. REV. STAT. § 646A.604(4)(d); 73 PA. CONS. STAT. § 2302; P.R. LAWS ANN. tit. 10, § 4053(2); 11 R.I. GEN. LAWS § 11-49.3-3(c)(iii); S.C. CODE ANN. § 39-1-90(E)(4); S.D. CODIFIED LAWS § 22-40-22(3); TENN. CODE ANN. § 47-18-2107(e)(3); TEX. BUS. & COM. CODE ANN. § 521.053(f); UTAH CODE ANN. § 13-44-202(5)(a)(iv); VT. STAT. ANN. tit. 9, § 2435(b)(6)(B); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(2)(4)(c); W. VA. CODE § 46A-2A-101(7)(D); WYO. STAT. ANN. § 40-12-502(d)(iii).

> Connecticut, Delaware, D.C., Georgia, Idaho, Indiana, Kansas, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, and Utah. While not required, however, it is advisable to consider including the general content components identified below to avoid claims from consumers and/or regulators alleging the insufficiency of notice.

In contrast with the above states and D.C., the following jurisdictions have breach notice content requirements to varying degrees: Alabama, Arizona, California, Colorado, Florida, Hawaii, Illinois, Iowa, Maryland, Massachusetts, Michigan, Missouri, New Hampshire, New Mexico, New York, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.[153]

Importantly, although these jurisdictions set forth specific content requirements, many exempt organizations from compliance with the specific notification obligations if the organization already has its own breach notice plan in place and notifies impacted individuals according to that plan. For example, in California, if the organization maintains its own notification

153. ALA. CODE § 8-38-5(d); ARIZ. REV. STAT. § 18-552(E); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2); FLA. STAT. § 501.171(4)(e); HAW. REV. STAT. § 487N-2(d); 815 ILL. COMP. STAT. 530/10(a); IOWA CODE § 715C.2(5); MD. CODE ANN., COM. LAW § 14-3504(g); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS ANN. § 445.72(6); MO. ANN. STAT. § 407.1500(2)(4); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; N.Y. GEN. BUS. LAW § 899-aa(7); N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(6) [effective Mar. 1, 2020]; W. VA. CODE § 46A-2A-102(d); WIS. STAT. § 134.98(2)(a); WYO. STAT. ANN. § 40-12-502(e).

procedures as part of a data breach response or information security policy, and the organization notifies impacted individuals in accordance with those policies and procedures, and the timing of notice pursuant to that policy is otherwise consistent with California's timing requirements, then the organization is deemed to be in compliance with California's statutory notification requirements, even if the organization's policies and procedures are different from California's statutory notice requirements.[154]

Organizations may also be exempt from compliance with the statutory notice obligations if the breach is otherwise regulated by or subject to HIPAA, GLBA's Security Standards, or another federal statute. In these instances, if the organization makes notice to impacted individuals pursuant to those federal notice requirements, then the organization is deemed to have automatically complied with the notice statute of the relevant U.S. jurisdiction, even if the federal notice requirements differ from that jurisdiction's requirements. These federal statutes, however, may have specific content requirements to which the organization must adhere. Thus, the organization must scrutinize the statutes in the relevant states, territories, and D.C., as well as federal statutes.

Further, if a data breach impacts residents in more than one jurisdiction, and each of those jurisdictions has content requirements, the organization will need to comply with the content requirements for each of the relevant jurisdictions. Apart from Massachusetts, compliance with each of those notice requirements, however, does not necessarily mean the organization must draft and disseminate several different breach notices. Instead, with careful crafting and scrutiny of the requirements in each relevant statute, in most instances, a single notice can be

154. CAL. CIV. CODE § 1798.82(l).

drafted that includes and complies with statutory content requirements in all of the relevant jurisdictions.

Finally, California, Hawaii, Michigan, North Carolina, Puerto Rico, Vermont, and Washington require that the notice be clear and conspicuous and crafted using plain language.[155] Though not a requirement across all jurisdictions, it is advisable that all notices be drafted using plain and concise language.

Table VI.C.3(A):
General Content Requirements for Notice to Individuals

Depending on the applicable statute, the following categories of information may be required in a notice to impacted individuals:	
Content Required	**U.S. Jurisdiction**
No specific content requirements	Alaska, Arkansas, Connecticut, Delaware, D.C., Georgia, Idaho, Indiana, Kansas, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah

155. CAL. CIV. CODE § 1798.82(d); HAW. REV. STAT. § 487N-2(d); MICH. COMP. LAWS § 445.72(6); N.C. GEN. STAT. § 75-65(d); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); WASH. REV. CODE § 19.255.010(2)(6).

Content Required	**U.S. Jurisdiction**
A general description of the incident	California, Hawaii, Iowa, Michigan, Missouri, New Hampshire, New Mexico, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Wyoming[156]
Date of the breach (or estimated date or date range within which the breach occurred)	Alabama, Arizona, California, Colorado, Florida, Iowa, New Hampshire, New Mexico, Oregon, Vermont, Washington, Wyoming[157]

156. CAL. CIV. CODE § 1798.82(d); HAW. REV. STAT. § 487N-2(d)(1); IOWA CODE § 715C.2(5); MICH. COMP. LAWS § 445.72(6); MO. ANN. STAT. § 407.1500(2)(4); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(a); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WYO. STAT. ANN. § 40-12-502(e).

157. ALA. CODE § 8-38-5(d)(1); ARIZ. REV. STAT. § 18-552(E)(1); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2)(I); FLA. STAT. § 501.171(4)(e)(1); IOWA CODE § 715C.2(5); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; OR. REV. STAT. § 646A.604(5)(b); VT. STAT. ANN. tit. 9, § 2435(b)(5); WASH. REV. CODE § 19.255.010(2)(6)(b)(iii); WYO. STAT. ANN. § 40-12-502(e).

Content Required	U.S. Jurisdiction
Categories of personal information reasonably believed to have been breached (e.g., username, password, date of birth, social security number)	Alabama, Arizona, California, Colorado, Florida, Hawaii, Iowa, Maryland, Michigan, Missouri, New Hampshire, New Mexico, New York, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Washington, West Virginia, Wyoming[158]
Whether notice was delayed as a result of a law enforcement investigation	California, Wyoming[159]
The steps the organization has taken to protect impacted individuals and their personal information from further unauthorized access or acquisition	Alabama, California, Hawaii, Michigan, North Carolina, Vermont, Virginia, Wyoming[160]

158. ALA. CODE § 8-38-5(d)(2); ARIZ. REV. STAT. § 18-552(E)(2); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2)(II); FLA. STAT. § 501.171(4)(e)(2); HAW. REV. STAT. § 487N-2(d)(2); IOWA CODE § 715C.2(5); MD. CODE ANN., COM. LAW § 14-3504(g)(1); MICH. COMP. LAWS § 445.72(6); MO. ANN. STAT. § 407.1500(2)(4); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; N.Y. GEN. BUS. LAW § 899-aa(7); N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(c); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WASH. REV. CODE § 19.255.010(2)(6)(b)(ii); W. VA. CODE § 46A-2A-102(d); WYO. STAT. ANN. § 40-12-502(e).

159. CAL. CIV. CODE § 1798.82(d); WYO. STAT. ANN. § 40-12-502(e).

160. ALA. CODE § 8-38-5(d)(3); CAL. CIV. CODE § 1798.82(d); HAW. REV. STAT. § 487N-2(d)(3); MICH. COMP. LAWS § 445.72(6); N.C. GEN. STAT. § 75-65(d); VT.

Content Required	**U.S. Jurisdiction**
Advice regarding additional steps the impacted individuals can take to further protect themselves and their personal information	Alabama, California, Colorado, Hawaii, Illinois, Iowa, Maryland, Massachusetts, Michigan, Missouri, New Mexico, North Carolina, Oregon, Vermont, Virginia, Wyoming[161]
Contact information for the organization reporting the breach	Alabama, California, Colorado, Florida, Hawaii, Maryland, Michigan, Missouri, New Hampshire, New Mexico, New York, North Carolina, Oregon, Puerto Rico, Vermont, Virginia, Washington, West Virginia, Wyoming[162]

STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WYO. STAT. ANN. § 40-12-502(e).

161. ALA. CODE § 8-38-5(d)(4); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2)(VI); HAW. REV. STAT. § 487N-2(d)(5); 815 ILL. COMP. STAT. 530/10(a)(iii); IOWA CODE § 715C.2(5); MD. CODE ANN., COM. LAW § 14-3504(g)(4); MASS. GEN. LAWS ch. 93H, § 3(b); MICH. COMP. LAWS § 445.72(6); MO. ANN. STAT. § 407.1500.2(4); N.M. STAT. ANN. § 57-12C-7; N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(f); VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A); WYO. STAT. ANN. § 40-12-502(e).

162. ALA. CODE § 8-38-5(d)(5); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a)(a.2)(III); FLA. STAT. § 501.171(4)(e)(3); HAW. REV. STAT. § 487N-2(d)(4); MD. CODE ANN., COM. LAW § 14-3504(g)(2); MICH. COMP. LAWS § 445.72(6); MO. ANN. STAT. § 407.1500(2)(4); N.H. REV. STAT. ANN. § 359-C:20(IV); N.M. STAT. ANN. § 57-12C-7; N.Y. GEN. BUS. LAW § 899-aa(7); N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(d); P.R. LAWS ANN. tit. 10, § 4053; VT. STAT. ANN. tit. 9, § 2435(b)(5); VA. CODE ANN. § 18.2-186.6(A);

Content Required	U.S. Jurisdiction
Toll-free numbers and addresses of the three major credit reporting agencies and/or FTC	Arizona, California, Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, Washington, West Virginia, Wyoming[163]

As with most aspects of notice, content requirements vary by jurisdiction, with some, like North Carolina and California, requiring very specific language to be included, and others, like Massachusetts, identifying information that should *not* be included. For example, California requires the notice to be titled "Notice of Data Breach" and to include very specific headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."[164] Similarly, North Carolina sets forth specific language to be used in explaining to impacted individuals what additional steps they may take to protect themselves (e.g., the use of a security freeze).[165] Massachusetts, on the other hand, actually prohibits the notice to include a description of the nature of the breach; therefore, in the event a data breach impacts residents in Massachusetts as well as other jurisdictions, like California,

WASH. REV. CODE § 19.255.010(2)(6)(i); W. VA. CODE § 46A-2A-102(d); WYO. STAT. ANN. § 40-12-502(e).

163. ARIZ. REV. STAT. § 18-552(E)(3)—(4); CAL. CIV. CODE § 1798.82(d); COLO. REV. STAT. § 6-1-716(2)(a.2)(IV)—(V); 815 ILL. COMP. STAT. 530/10(a)(i)—(ii); IOWA CODE § 715C.2(5); MD. CODE ANN., COM. LAW § 14-3504(g)(3)—(4); MO. ANN. STAT. § 407.1500(2)(4); N.M. STAT. ANN. § 57-12C-7; N.C. GEN. STAT. § 75-65(d); OR. REV. STAT. § 646A.604(5)(e); WASH. REV. CODE § 19.255.010(2)(6)(b)(iv); W. VA. CODE § 46A-2A-102(d); WYO. STAT. ANN. § 40-12-502(e).

164. CAL. CIV. CODE § 1798.82(d).

165. N.C. GEN. STAT. § 75-63(p).

notice to Massachusetts residents will need to be made separately (since all other jurisdictions require notice to contain a brief description of the breach).[166] To that end, the Massachusetts Attorney General has created a sample data breach notification letter and posted it on the Massachusetts Attorney General's website. Though the Massachusetts data breach notification law does not require the use of this sample notice, based on the experience of the drafting team, the Massachusetts Attorney General's office has *strongly* encouraged the use of such sample notice in notifying impacted Massachusetts residents. As a result, scrutiny and consultation of the specific statutory language is advisable to ensure all specific content requirements are satisfied in any crafted notice.

In addition to the above general categories of content, many jurisdictions now require organizations to provide identity theft prevention and mitigation services (a.k.a. "credit monitoring") to impacted individuals *for free* for at least twelve months.[167] Connecticut now requires organizations to provide twenty-four months of free credit monitoring.[168]

166. MASS. GEN. LAWS ch. 93H, § 3(b).

167. *See, e.g.*, CAL. CIV. CODE § 1798.82(d). Connecticut's Attorney General has adopted this approach as a matter of policy, even though it is not required under that state's statute.

168. CONN. GEN. STAT. § 36a-701b(2)(B). A more detailed discussion of credit monitoring can be found in Section V.F, *supra*.

VII. AFTER-ACTION REVIEWS

A major theme of incident response guidance is that data breaches and security incidents are a recurring threat, and the threat landscape constantly changes. IRPs should be comprehensive, adaptive, and regularly updated to work effectively in this dynamic environment. After-action review is critical to the continuous improvement process. It also provides an opportunity to identify which areas of the IRP worked or failed, to update the IRP and internal practices and policies with a view towards preventing the same type of incident from occurring again, and to address blind spots that the IRP did not account for.

Data breaches and security incidents are a cycle, not discrete stages. There might not be a bright line that separates the "during" phase of incident response from the "after." Depending on the size and nature of the incident, the affected organization needs to continue monitoring for anomalies and repeated attempts to gain access to its systems, even as it compiles data for after-action reports. If an unauthorized access reoccurs, the organization may need to evaluate what phase of the IRP it truly is in, especially if the new attack is from the same source.

As the organization moves into the "after" phase, it should continue to use its IRP as a checklist. Depending on its level of detail, the IRP may call for an overall report to the management group that is responsible for the governance of the IRP, as well as reports for specific audiences. The nature and scope of the incident will also determine how broad or narrow the after-action report needs to be. Incidents that are localized may only require a review of practices within that group, while major incidents may necessitate an organization-wide review. The need and scope depend on the organization's size, the extent and sophistication of the incident, and how well existing policies and procedures enabled identification and remediation of the incident.

Post-incident assessments should focus on how well the IRP worked as a guide to decision-making and action-planning before and during the incident. The roles and performance of internal functions and individuals, and of outside resources, should also be assessed. As a reflection on a crisis that has passed, the assessment should be constructive. The following should be considered:

- Did members of the IRT know answers to the questions that arose?
- If not, did they know how to find answers quickly?
- Were they able to improvise effectively if a novel situation presented itself?
- Was the IRP activated in a timely fashion?
- Were outside resources (e.g., outside counsel, forensic and security consultants, breach communications specialists, insurers) notified and engaged at the right times?
- Were necessary contracts in place, and did third parties perform to agreed-upon service levels?
- Were outside resources effective?
- Did members of the IRT (including outside resources) communicate effectively, timely, and efficiently?
- Was the incident due to a gap in the written information security plan or was it beyond the organization's control?

If the evaluation of either the IRP or the performance of the people who executed it reveals areas for improvement, a plan should be made to close the gaps. Even if the after-action report concludes that the incident was not reasonably avoidable, why that conclusion was reached should be documented to

demonstrate the organization's active adherence to the IRP, and the reasonableness of its practices.

In addition to evaluating the plan and the performance of the individuals who executed it, the organization should reexamine the policies, processes, and procedures that support data security and data incident preparedness in the period immediately following an incident. If inconsistencies or gaps in supporting documents come to light, they should be addressed. Gaps might also signal the need for additional training and table-top exercises. Particular attention should be paid to the incident's cause—some incidents are not reasonably avoidable because they result from pervasive, newly discovered flaws in technology systems. Other incidents may be caused because particular Vendors, technologies, or practices are not sufficiently robust. Technologies or practices that cause recurring issues, or that are implicated repeatedly in the organization's incidents, should be evaluated to see if they are reasonable and appropriate for the organization from a security perspective.

Given the criticality of communications to effective incident response, all aspects of communications strategy and tactics should be reviewed. Questions include:

- Were internal lines of communication sufficient and effective?
- Were communications with third-party service providers sufficient and effective?
- Were communications with law enforcement, regulatory bodies, insurers, and the public managed smoothly?

Reports that call for change or gap closure should include details that support the proposed change, the projected cost to implement it, a timeline, and a follow-up plan.

Beyond the tactical evaluations already suggested, post-incident reviews should examine more strategic issues, such as the adequacy of the organizational structure to support a robust incident response. The review should place particular emphasis on whether IRP responsibilities are mismatched, as in cases where responsibility is assigned to a person, department, or division that is unsuitable or lacks the appropriate competencies to carry out the assigned role. Based on the experience of the drafting team, the organization should give serious consideration to separating the security and incident response function from the IT function, because robust security and incident response functions do not always align well with the traditional IT role, which focuses on usability and efficiency of the organization's information technology systems.

The organization should tailor after-action reports to the specific recipient, to fit that person's or group's need to know. The organization should also take care to preserve confidentiality and all applicable privileges it has decided not to waive. Counsel to the IRT should maintain records and reports in accordance with the organization's records retention policy, with counsel being mindful of any additional steps that may be necessary to maintain any privileges that may apply. The after-action review should also examine whether the IRP and internal policies are still in compliance with the organization's legal obligations, especially where those obligations have changed since any previous after-action report.

Finally, in addition to identifying gaps and failures, the parts of the IRP that worked well should be singled out and applied to other parts of the IRP specifically, or the organization more generally. Areas of success may inform the organization how to correct areas that failed or underperformed. The primary objective of the after-action review is to become more prepared for the next incident.

VIII. **CONCLUSION**

The collection, analysis, and maintenance of information are increasingly essential elements to commerce. The custodian of the information collected is responsible for protecting it and, if it is compromised, taking actions necessary to comply with applicable notification requirements. We hope that organizations and practitioners will find the *Incident Response Guide* a useful tool to assist in preparing for and executing proper responses to incidents of data compromise.

APPENDIX A:
MODEL INCIDENT RESPONSE PLAN

I. Objective and Scope

This document defines the procedures for responding to information security incidents. It discusses how information is communicated to necessary personnel and how an incident's impact is evaluated. It further outlines guidelines for incident documentation and rules for evidence preservation.

Some examples of potential security incidents include:

- theft, damage, or unauthorized access (e.g., unauthorized logins, broken locks, missing log files, or unscheduled/unauthorized physical entry);
- inaccurate information within databases, logs, files, or other records;
- abnormal system behavior (e.g., unscheduled system reboots, unexpected messages, or abnormal errors in logs); and
- security event notifications (e.g., file integrity alerts, intrusion detection alarms, or physical security alarms).

It is the responsibility of all members of the Incident Response Team ("IRT") to read, understand, and adhere to the procedures described in this Incident Response Plan ("IRP").

II. Responsible Party

The IRT, with the assistance of designated outside resources as appropriate, is tasked with providing a fast, effective, and orderly response to security incidents. The team is authorized to take any appropriate steps deemed necessary to mitigate or resolve a security incident. It is responsible for investigating suspected security incidents in a timely manner and reporting any findings as set forth in this document.

III. Incident Response Team Identification

[The composition of your IRT should reflect the needs of your organization; Section IV of the Incident Response Guide provides guidance on the composition of the IRT.]

[*LIST HERE – Include 24x7 Contact Information*]

IV. Reporting Procedures

The IRT should be notified immediately of any suspected or actual security incidents involving data systems, particularly any critical system, or systems that handle Personally Identifiable Information (PII). If it is unclear as to whether a situation should be considered a security incident, the IRT should be contacted to evaluate the situation.

Except for the steps outlined below, it is imperative that any investigative or corrective action be undertaken by trained personnel or under the oversight of trained personnel, to ensure the integrity of the incident investigation and recovery process.

When faced with a potential situation, the Information Technology (IT) team, in consultation with the IRT to the most reasonable degree possible, will take the following actions:

- A compromised computer system should be examined immediately.
  - The system should remain powered on and all currently running computer programs left as is.
  - Do not shutdown or restart the computer.
  - Immediately disconnect the computer from the network by removing the network cable from the back of the computer.[169]

169. If the computer is a virtual machine, it should be snapshotted and archived. Then the running version should have virtual Network Interface Controllers disabled but be left in running condition.

- Information about a security incident can come to light anywhere in the organization.
  - Information about any suspected or actual incidents are reported to the Chair of the IRT.
  - All communications with law enforcement or the public will be coordinated by the Legal Representative(s) of the IRT.
  - Document immediately all key information known about the incident, including:
    - date and time of discovery, and the nature of the incident;
    - immediate action taken in response to the incident; and
    - date and time the IRT was notified of the incident.

V. Severity Classification

The IRT will determine if the security incident justifies activating the IRP. If the IRT decides it does not, the incident will be delegated to one of the members of the IRT for resolution.

The following classifications will be used to help guide the response that the IRT should take:

- **Level One**—Potentially unfriendly activity, e.g.:
  - Unauthorized port scans
  - Virus detection with automated correction
  - Unexpected performance peak
  - Other routine minor events
- **Level Two**—Clear attempts to obtain unauthorized information or access, e.g.:
  - Unauthorized vulnerability scans
  - Attempt to access restricted areas

- Virus infection on a noncritical system
- Level One incidents occurring against systems storing sensitive data, including PII or Non-Public Information
- Level One incidents originating from unauthorized internal systems
- Repeated Level One incidents from a single source
- Other similar incidents

- **Level Three**—Serious attempt or actual breach of security, e.g.:
  - Multi-pronged attack
  - Denial-of-service attempt
  - Virus infection on a critical system or the network
  - Successful unauthorized access to sensitive data or systems
  - Repeated Level Two incidents from a single source
  - Other similar incidents

VI. Response Procedures

A. Response Process

Any given response to an incident can include—or proceed through—each of the following stages: identification, classification, containment, eradication, recovery, and root cause analysis. When possible, these steps will be taken in parallel.

At a minimum, the following actions should be taken once an incident has been identified and classified:

- If **Level One**—Contain and Monitor

  - Record source of the incident (e.g., user, internet protocol (IP) address, etc.).
  - Use technology controls to temporarily or permanently block the source.
  - Monitor the source for future incidents.
- If **Level Two**—Contain, Monitor, and Warn
  - Perform all actions in Level One.
  - Collect and protect information associated with the incident.
  - Determine the origin of the incident.
  - Eliminate the intruder's means of access and related vulnerabilities.
  - Provide breach notifications to applicable federal and state authorities, and to affected individuals as appropriate.
  - Notify insurance carrier and broker.
  - Review incident to determine if it should be reclassified to Level Three.
- If **Level Three**—Contain, Eradicate, Recover, and Analyze the Root Cause
  - Perform all actions in Level One and Level Two.
  - Contain the incident and determine further action. Consider limiting or eliminating network access and applying more restrictive access controls, deactivating switch ports, etc.
  - Collect and protect information associated with the incident, which may include offline methods. In the event that a forensic investigation is required, the IRT will identify appropriate

internal and external resources to perform that investigation.

- Notify Chief Executive Officer of the situation and provide progress updates as necessary.
- Research potential risks or damage caused by the identified method of intrusion.

B. Root Cause Analysis

Not more than one week after completing the response for any incident and the required activation of the IRP, members of the IRT and the affected parties as identified by the IRT will meet to review the results of the investigation conducted to determine the root cause of the compromise and evaluate the effectiveness of the IRP. Other security controls will also be reviewed to determine their appropriateness for the current risks. Any identified areas in which the plan, policy, or security control can be made more effective or efficient, including training and education, must be updated accordingly. Upon conclusion of an investigation, compromised systems will be reimaged to a clean and uncompromised state.

VII. Reporting

All employees have an obligation to report any known or suspected violation of this policy to the IRT.

VIII. Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

IX. Exceptions

Exceptions to this policy may exist where the exception has been:

- documented for its legitimate business purpose;

- approved by a Director or above; and
- recorded for audit purposes.

APPENDIX B:
MODEL NOTIFICATION LETTER

Subject: IMPORTANT DATA SECURITY INCIDENT INFORMATION

[Date]

We greatly value your business and respect the privacy of your information, which is why we are writing to inform you that we recently learned of a serious data security incident, which took place [on [date] or from [date] to [date]], in which personal, private, and unencrypted credit and debit card information was accessed by an outside party and compromised.

The compromised information included your name, shipping address, billing address, credit card security code, and credit and/or debit card number. We are working around the clock, with the aid of outside resources, to help you avoid—or at least minimize—any negative consequences.

We are in the process of reporting the incident to the appropriate state agencies and federal authorities to initiate an investigation. Our notification has not been delayed as a result of any law enforcement investigation.

We are notifying you so you can take additional actions to minimize or eliminate potential personal harm. Because this is a serious incident, **we strongly encourage you to take the following preventive measures to help detect and mitigate any misuse of your information**:

1. [Client] is providing each impacted customer with free credit monitoring services through [details of credit monitoring services]. In the meantime, we encourage you to consider the other action items listed in this communication.
2. Closely monitor your financial accounts and promptly contact your financial institution if you

notice any unusual activity. You may also wish to contact your credit or debit card issuer to determine whether a new card should be issued and whether additional levels of security or protective measures should be placed on your account(s).

3. We strongly encourage you to report incidents of suspected identity theft to your local law enforcement, the Federal Trade Commission, and your state attorney general.
4. We also recommend that you monitor your free credit reports. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, by calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.
5. You also may want to place a security freeze on your credit files by calling each of the three credit reporting agencies. Freezing credit files will prevent someone from using your personal information to open new accounts or borrow money in your name. Please understand that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card unless you temporarily or permanently remove the freeze.

While we have already notified the three major credit reporting agencies, we strongly encourage you to contact the credit reporting agencies directly to notify them, receive credit alerts, or freeze your credit files. Contact for the three agencies is provided below:

Equifax	Experian	TransUnion
P.O. Box 740241 Atlanta, GA 30374 General: 1-888-685-1111 Fraud alert: 1-888-766-0008 Security freeze: 1-800-685-1111 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 2104 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze	P.O. Box 2000 Chester, PA 19022 General: 1-800-888-4213 Identity theft and fraud: 1-800-680-7289 www.transunion.com/credit-freeze/place-credit-freeze

You may also contact the Federal Trade Commission to receive information about fraud alerts, security freezes, and preventing identity theft:

> 1-877-ID-THEFT (877-438-4338)
> Federal Trade Commission
> 600 Pennsylvania Avenue, NW
> Washington, DC 20580
> https://www.consumer.ftc.gov/features/feature-0014-identity-theft

Maryland residents may wish to review information provided by the Maryland Attorney General at https://www.oag.state.md.us/idtheft/businessGL.htm, by calling 888-743-0023, or writing to the Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202. Maryland residents may contact the attorney general for information about preventing identity theft.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling 877-566-7226, or by writing to the Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699. North Carolina residents may contact the attorney general for information about preventing identity theft.

We sincerely regret this incident and any inconvenience it may cause. We will do everything we can to mitigate any negative consequences of this unfortunate incident. We also want you to know that we have determined the cause of the incident and have taken action to prevent future incidents of this nature.

[Details about efforts to prevent future breaches].

Thanks for your ongoing patience and understanding as we work through this process. Please call [toll-free number] with any questions or to receive further assistance.

Sincerely,

[Signature and Contact Information]

APPENDIX C:
MODEL NOTIFICATION LETTER—MASSACHUSETTS

Subject: IMPORTANT DATA SECURITY INCIDENT INFORMATION

[Date]

We recently learned of a serious data security incident, which took place [on [date] or from [date] to [date]], in which personal, private, and unencrypted information was likely compromised.

We believe the compromised information could reasonably be used to make fraudulent credit or debit card purchases. We are working around the clock, with the aid of outside resources, to help you avoid or at least minimize any negative consequences.

We are in the process of reporting the incident to the appropriate state agencies and federal authorities to initiate an investigation. Our notification has not been delayed as a result of any law enforcement investigation.

We are notifying you so you can take additional actions to minimize or eliminate potential personal harm. Because this is a serious incident, **we strongly encourage you to take the following preventive measures to help detect and mitigate any misuse of your information:**

1. [Client] is providing each impacted customer with free credit monitoring services [describe services].
2. Closely monitor your financial accounts and promptly contact your financial institution if you notice any unusual activity. You may also wish to contact your credit or debit card issuer to determine whether a new card should be issued and whether additional levels of security or protective measures should be placed on your account(s).

3. We strongly encourage you to report incidents of suspected identity theft to your local law enforcement and state attorney general.
4. We also recommend that you monitor your free credit reports. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every twelve months by visiting www.annualcreditreport.com, by calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.
5. You also may want to place a security freeze on your credit files by calling each of the three credit reporting agencies. Freezing credit files will prevent someone from using your personal information to open new accounts or borrow money in your name. Please understand that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card unless you temporarily or permanently remove the freeze. Note that, in Massachusetts, placing or lifting a security freeze is free for victims of identity theft, but in other cases, credit reporting agencies may charge up to $5 each to place, lift, or remove a security freeze. If you choose to obtain a security freeze by directly contacting the credit reporting agencies, you must send a letter by regular certified mail to each of the credit reporting agencies listed below. The letter should include your name, address, date of birth, social security number, and credit card number and expiration date for payment, if applicable. Each of the credit

> reporting agencies has specific requirements to place a security freeze. Review these requirements on the website for each prior to sending your written request. For more information see http://www.mass.gov/ago/consumer-resources/consumer-information/scams-and-identity-theft/identity-theft/fraud-alerts.html.

While we have already notified the three major credit reporting agencies, we strongly encourage you to contact the credit reporting agencies directly to notify them, receive credit alerts, or freeze your credit files. Contact for the three agencies is provided below:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241 Atlanta, GA 30374 General: 1-888-685-1111 Fraud alert: 1-888-766-0008 Security freeze: 1-800-685-1111 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 2104 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze	P.O. Box 2000 Chester, PA 19022 General: 1-800-888-4213 Identity theft and fraud: 1-800-680-7289 www.transunion.com/credit-freeze/place-credit-freeze

You may also contact the Federal Trade Commission to receive information about fraud alerts, security freezes, and preventing identity theft:

> 1-877-ID-THEFT (877-438-4338)
> Federal Trade Commission
> 600 Pennsylvania Avenue, NW

Washington, DC 20580
https://www.consumer.ftc.gov/features/feature-0014-identity-theft

In addition, as a Massachusetts resident, you have the right to obtain a police report if you are the victim of identity theft.

We sincerely regret this incident and any inconvenience it may cause. We will do everything we can to mitigate any negative consequences of this unfortunate incident. We also want you to know that we have determined the cause of the incident and have taken action to prevent future incidents of this nature.

Thanks for your ongoing patience and understanding as we work through this process.

Sincerely,

[Name and Contact Information]

APPENDIX D:
MODEL ATTORNEY GENERAL BREACH NOTIFICATION—MARYLAND

[typically communicated by counsel]

[Date]

VIA EMAIL

Office of the Attorney General of the State of Maryland

E-mail: Idtheft@oag.state.md.us

Re: Data Security Breach Notification

To Whom It May Concern:

[Client], a client of [name of law firm], is notifying the Office of the Attorney General of the State of Maryland that [client] intends to notify [number] residents of Maryland about the data security incident described below.

[On [date] or from [date] to [date]], a third party obtained customer data from [client] by hacking into [client]'s internal computer network. The data stolen included names, shipping and billing addresses, credit/debit card numbers, and credit security codes.

[Client] has reported the incident to appropriate law enforcement authorities to initiate an investigation and is in the process of notifying the three major U.S. credit reporting agencies. It also plans to offer free credit monitoring services to the affected residents. [Information about steps [client] is taking to restore the integrity of the system.]

[Client] now intends to notify affected Maryland residents of the data security incident. A sample of the notification to the Maryland residents is enclosed.

If you would like any additional information concerning the above event, please feel free to contact us at your convenience.

Sincerely,

[Counsel]
Enclosure

APPENDIX E:
MODEL ATTORNEY GENERAL BREACH NOTIFICATION—CONNECTICUT

[typically communicated by counsel]

[Date]

VIA EMAIL

Office of the Attorney General of the State of Connecticut

Email: ag.breach@ct.gov

Re: Data Security Breach Notification

To Whom It May Concern:

[Client], a client of [name of law firm], is notifying the Office of the Attorney General of the State of Connecticut that [client] intends to notify [number] residents of Connecticut about the data security incident described below.

[On [date] or from [date] to [date]], a third party obtained customer data from [client] by improperly accessing [client]'s internal computer network. The data accessed included names, shipping and billing addresses, credit/debit card numbers, and credit security codes.

[Client] has reported the incident to appropriate law enforcement authorities to initiate an investigation and is in the process of notifying the three major U.S. credit reporting agencies. It also plans to offer free credit monitoring services to the affected residents. [Information about steps [client] is taking to restore the integrity of the system.]

[Client] now intends to notify affected Connecticut residents of the data security incident. A sample of the notification to the Connecticut residents is enclosed.

Notification was not delayed because of a law enforcement investigation.

If you would like any additional information concerning the above event, please feel free to contact us at your convenience.

Sincerely,

[Counsel]

Enclosure

APPENDIX F:
GLBA AND HIPAA

I. Special Requirements in the United States:

A. Gramm-Leach-Bliley Act (GLBA)[170]

1. Governs data security for financial institutions and any other business engaged in financial activities, such as:
   - lending, investing, or safeguarding money or securities for others;
   - insuring, indemnifying, or guaranteeing against loss, harm, damage, illness, or death;
   - providing or issuing annuities or acting as a broker for such;
   - providing financial, investment, or economic advisory services; or
   - underwriting or dealing in securities.
2. Obligations are triggered where there is:
   - unauthorized access to, or use of, customer information maintained by a financial institution or its service provider;
   - misuse of customer information or it is reasonably possible that customer information will be misused; or
   - misuse of customer information that could result in substantial harm or inconvenience to customers.

170. Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et. seq.*

3. Response should include:
    - assessing nature and scope of incident;
    - identifying what customer information has been accessed or misused;
    - notifying primary federal regulator of unauthorized access or use;
    - providing Suspicious Activity Report ("SAR") to the Financial Crimes Enforcement Network (FinCEN);
    - notifying law enforcement;
    - containing and controlling the incident to prevent further unauthorized access or use;
    - notifying customers, when warranted (if misuse has occurred or is reasonably possible, notify affected customers as soon as possible); and
    - if the institution cannot determine which specific customers are affected, notifying the entire group of customers whose files have been accessed.
4. Notice should include the following:
    - Description of the data breach
    - Description of the customers' information subject to unauthorized access or use
    - Telephone number customers can call for further information and assistance
    - Reminder to customers to monitor accounts for twelve to twenty-four months
    - Recommendation that customers promptly report incidents of suspected identity theft

- Description of what the institution has done to protect customers' information from further unauthorized access
- For large breaches, publication of notice on the organization's website and in major local media
- Information about what happened, how consumers can protect themselves from potential future harm, and contact information for the notifying party

B. Health Insurance Portability and Accountability Act of 1996 (HIPAA)[171]/Health Information Technology for Economic and Clinical Health (HITECH) Act[172]

1. Notification obligations triggered following breach
   - Breach presumed when there is an impermissible use or disclosure of Personal Health Information (PHI), unless risk assessment demonstrates low probability that PHI has been compromised
2. When to notify
   - Following the unauthorized acquisition, access, use, or disclosure of unsecured (i.e., unencrypted) information relating to individuals' past, present, or future physical or mental health and the provision of health care

171. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d *et. seq.*

172. Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. § 17931 *et. seq.*

- Without unreasonable delay, not later than sixty days following the discovery of a breach

3. Who to notify
   - Affected individuals
   - Media, if over 500 individuals in a single state or jurisdiction
   - Secretary of Health and Human Services
   - Notice shall include:
     - a brief description of the breach;
     - a description of the types of information that were involved;
     - the steps affected individuals should take to protect themselves from potential harm;
     - what the provider is doing to investigate the breach, mitigate the harm, and prevent further breaches; and
     - contact information for the provider.

THE SEDONA CONFERENCE GLOSSARY: EDISCOVERY & DIGITAL INFORMATION MANAGEMENT, FIFTH EDITION

A Project of The Sedona Conference Technology Resource Panel

Editor:

Paul H. McVoy, Meta-e Discovery LLC

Technology Resource Panel:

(See thesedonaconference.org for a listing of the Technology Resource Panel members)

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Technology Resource Panel. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263 (2020).

PREFACE

Welcome to the Fifth Edition of *The Sedona Conference Glossary*, a project of The Sedona Conference Technology Resource Panel. The Sedona Conference is a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The Technology Resource Panel consists of two halves: a "User Group," whose members regularly negotiate and work with service providers; and a panel of service provider members, who have agreed to work with the User Group's output, and who provide input along the way. The mission of the Technology Resource Panel is to provide input to Sedona's multiple Working Groups when they are working on an issue involving the use of technology or services provided by electronic discovery or electronic information governance service providers, and to help create tools and solutions like the *Glossary* that will benefit the entire marketplace.

The Sedona Conference Glossary, first published in 2005, is not intended to be an all-encompassing replacement of existing technical glossaries published by other organizations. Rather, the *Glossary* is published as a tool to assist in the understanding and discussion of electronic discovery and electronic information management issues, allowing for more effective communication between user and provider, enhanced by the ability to compare "apples to apples" when selecting a provider. The Technology Resource Panel was formed in the belief that a well-informed marketplace, speaking in the same language, will ultimately lead to reduced transaction costs for all parties, higher quality, and greater predictability.

The Sedona Conference acknowledges the contributions of Paul H. McVoy, who served as Editor of this Fifth Edition and

who was invaluable in driving this project forward. We also thank all of the Technology Resource Panel members who reviewed and commented on drafts of this edition. For a current listing of the Technology Resource Panel service provider and user group members, see https://thesedonaconference.org/trp.

As with all of our publications, your comments are welcome. Please forward them by email to comments@sedonaconference.org.

Craig Weinlein
Executive Director
The Sedona Conference
February 2020

30(b)(6): A shorthand reference to Rule 30(b)(6) of the Federal Rules of Civil Procedure, under which a corporation, partnership, association, or governmental agency is subject to the deposition process, and required to provide one or more witnesses to testify as to matters "known or reasonably available to the organization" on the topics requested by the deposition notice. Sometimes the 30(b)(6) topics concern the discovery process itself, including procedures for preservation, collection, chain of custody, processing, review, and production.

Ablate: To burn laser-readable "pits" into the recorded layer of optical disks, DVD-ROMs and CD-ROMs.

Ablative: Unalterable data. See Ablate.

Access Control List (ACL): A security group comprised of individual users or user groups that is used to grant similar permissions to a program, database, or other security-controlled environment.

ACL: See Access Control List.

ACM: See Association for Computing Machinery.

Active Data: Information residing on the direct-access storage media (disk drives or servers) that is readily visible to the operating system and/or application software with which it was created. It is immediately accessible to users without restoration or reconstruction.

Active Machine Learning: Technology-assisted-review algorithm for the selection of training documents, in which the machine selects sets of additional documents that should best improve results beyond the training that has already been done. Compare to Passive Learning.

Active Records: Records related to current, ongoing, or in-process activities referred to on a regular basis to respond to day-to-day operational requirements. See Inactive Record.

Address: A structured format for identifying the specific location or routing detail for information on a network or the internet. These include simple mail transfer protocol (SMTP) email addresses, internet protocol (IP) addresses, and uniform resource locators (URLs) (commonly known as web addresses).

Adware: See Spyware.

Agent: A program running on a computer that performs as instructed by a central control point to track file and operating system events and takes directed actions, such as transferring a file or deleting a local copy of a file, in response to such events.

AI: See Artificial Intelligence.

AIIM: See Association for Intelligent Information Management.

Air Gap: A network security measure that uses a physical separation of computer hardware to isolate a secure computer network from other, unsecured networks.

Algorithm: With regard to electronic discovery, a computer script that is designed to analyze data patterns using mathematical formulas and is commonly used to group or find similar documents based on common mathematical scores.

Alphanumeric: Characters composed of letters, numbers, and sometimes noncontrol characters (such as @, #, $). Excludes control characters.

Ambient Data: See Latent Data; Residual Data.

American National Standards Institute (ANSI): A private, nonprofit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. See https://www.ansi.org/.

American Standard Code for Information Interchange (ASCII, pronounced "ass-kee"): A nonproprietary text format built on a set of 128 (or 255 for extended ASCII) alphanumeric and

control characters. Documents in ASCII format consist of only text with no formatting and can be read by most computer systems.

Analog: Data in an analog format is represented by continuously variable, measurable, physical quantities such as voltage, amplitude, or frequency.

Analytics: See Conceptual Analytics.

Annotation: The changes, additions, or editorial comments made or applicable to a document—usually an electronic image file—using electronic sticky notes, highlighter, or other electronic tools. Annotations should be overlaid and not change the original document.

Anonymization (as used in the GDPR): The stripping of any identifiable information relating to a natural person from personal data in a manner such that it is impossible to derive insights on the data subject (discreet individual) and the individual is no longer identifiable.

ANSI: See American National Standards Institute.

Aperture Card: An IBM punch card with a window that holds a 35mm frame of microfilm. Indexing information is punched in the card.

API: See Application Programming Interface.

Applet: A program designed as an add-on to another program, allowing greater functionality for a specific purpose other than for what the original program was designed.

Appliance: A prepackaged piece of hardware and software designed to perform a specific function on a computer network, for example, a firewall.

Application: Software that is programmed for one or more specific uses or purposes. The term is commonly used in place of

"program" or "software." Applications, often referred to as apps, may be designed for individual users, for example, a word processing program, or for multiple users, as in an accounting application used by many users at the same time.

Application Programming Interface (API): The specifications designed into a program that allows interaction with other programs. See Mail Application Programming Interface (MAPI).

Application Service Provider (ASP): An internet-based organization that hosts applications on its own servers within its own facilities. Customers license the application and access it through a browser over the internet or via some other network. See Software as a Service (SaaS).

Architecture: Refers to the hardware, software, or combination of hardware and software comprising a computer system or network. "Open architecture" describes computer and network components that are more readily interconnected and interoperable. "Closed architecture" describes components that are less readily interconnected and interoperable.

Archival Data: Information an organization maintains for long-term storage and record-keeping purposes, but which may not be immediately accessible to the user of a computer system. Archival data may be written to removable media or may be maintained on system hard drives. Some systems allow users to retrieve archival data directly, while other systems require the intervention of an IT professional.

Archive, Electronic: Long-term repositories for the storage of records. Electronic archives preserve the content, prevent or track alterations, and control access to electronic records.

ARMA International: A nonprofit association and recognized authority on managing records and information, both paper and electronic. See https://www.arma.org/.

Artificial Intelligence (AI): A subfield of computer science focused on the development of intelligence in machines so that the machines can react and adapt to their environment and the unknown. AI is the capability of a device to perform functions that are normally associated with human intelligence, such as reasoning and optimization through experience. It attempts to approximate the results of human reasoning by organizing and manipulating factual and heuristic knowledge. Areas of AI activity include expert systems, natural language understanding, speech recognition, vision, and robotics. See Machine Learning.

ASCII: See American Standard Code for Information Interchange.

ASP: See Application Service Provider.

Aspect Ratio: The relationship of the height to the width of any image. The aspect ratio of an image must be maintained to prevent distortion.

Association for Computing Machinery (ACM): An association for computer professionals with a number of resources, including a special interest group on search and retrieval. See https://www.acm.org/.

Association for Intelligent Information Management (AIIM): An organization that focuses on Enterprise Content Management (ECM). See https://www.aiim.org/.

Asymmetrical Encryption: Public-key encryption utilized in blockchain transactions that require the user to procure both a public and private key to decipher the transaction—thereby allowing anyone to view the existence of the transaction, but the details of the transaction are only accessible to the participants of the transaction.

Attachment: A record or file associated with another record for the purpose of retention, transfer, processing, review,

production, and routine records management. There may be multiple attachments associated with a single "parent" or "master" record. In many records and information management programs or in a litigation context, the attachments and associated record(s) may be managed and processed as a single unit. In common use, this term often refers to a file (or files) associated with an email for retention and storage as a single message unit. See Document (or Document Family); Message Unit; and Unitization.

Attribute: A specific property of a file such as location, size, or type. The term attribute is sometimes used synonymously with "data element" or "property."

Audio-Video Interleave (AVI): A Microsoft standard for Windows animation files that interleaves audio and video to provide medium quality multimedia.

Audit Log or Audit Trail: An automated or manual set of chronological records of system activities that may enable the reconstruction and examination of a sequence of events and/or changes in an event.

Authenticate (as a security term): To technically verify the identity of an entity or individual requesting access to or use of a system, data, or resource.

Author or Originator: The person, office, or designated position responsible for an item's creation or issuance. In the case of a document in the form of a letter, the author or originator is usually indicated on the letterhead or by signature. In some cases, a software application producing a document may capture the author's identity and associate it with the document. For records management purposes, the author or originator may be designated as a person, official title, office symbol, or code.

Auto-Delete: The use of technology to run predefined rules at scheduled intervals to delete or otherwise manage electronically

stored information. May also be referred to as a janitor program or system cleanup.

Availability: The probability that a computer system is operational during the period of need.

Avatar: A graphical representation of a user in a shared virtual reality, such as web forums or chat rooms.

AVI: See Audio-Video Interleave.

Backbone: The top level of a hierarchical network. It is the main channel along which data is transferred.

Backup: The process of creating a copy of active data as a precaution against the loss or damage of the original data. The process is usually automated on a regular schedule, which can include the automatic expiration of older versions. The term is also used to refer to the electronically stored information itself, as in, "a backup of the email server exists." Backups can be made to any type of storage, including portable media, CDs, DVDs, data tapes, or hard drives—also known as a full backup. See Differential Backup; Incremental Backup.

Backup Data: A copy of electronically stored information that serves as a source for recovery in the event of a system problem or disaster. See Backup.

Backup Tape: Magnetic tape used to store copies of electronically stored information, for use when restoration or recovery is required. The creation of backup tapes is made using any of a number of specific software programs and usually involves varying degrees of compression.

Backup Tape Rotation or Recycling: The process whereby an organization's backups are overwritten with new data, usually on an automated schedule that should be determined by IT in consultation with records management and legal personnel. For example, the use of nightly backup tapes for each day of the

week—with the daily backup tape for a particular day being overwritten on the same day the following week.

Bandwidth: The amount of data a network connection can accommodate in a given period of time. Bandwidth is usually stated in kilobits per second (kbps), megabits per second (mbps) or gigabits per second (gbps).

Bar Code: A small pattern of vertical lines or dots that can be read by a laser or an optical scanner. In records management and electronic discovery, bar codes may be affixed to specific records for indexing, tracking, and retrieval purposes.

Basic Input Output System (BIOS): The set of user-independent computer instructions stored in a computer's ROM, immediately available to the computer when the computer is turned on. BIOS information provides the code necessary to control the keyboard, display screen, disk drives, and communication ports in addition to handling certain miscellaneous functions.

Batch File: A set of commands written for a specific program to complete a discrete series of actions, for example, renaming a series of files en masse.

Batch Processing: The processing of multiple sets of electronically stored information at one time. See Processing Data.

Bates Number: Sequential numbering system used to identify individual pages of documents where each page or file is assigned a unique number. Often used in conjunction with a suffix or prefix to identify a producing party, the litigation, or other relevant information. See Beginning Document Number; Production Number.

Bayesian Search: An advanced search that utilizes the statistical approach developed by Thomas Bayes, an 18th century mathematician and clergyman. Bayes published a theorem that describes how to calculate conditional probabilities from the

combinations of observed events and prior probabilities. Many information retrieval systems implicitly or explicitly use Bayes's probability rules to compute the likelihood that a document is relevant to a query. For a more thorough discussion, see The Sedona Conference, *Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 15 SEDONA CONF. J. 217 (2014), *available at* https://thesedonaconference.org/publication/Commentary_on_Search_and_Retrieval_Methods.

BBS: See Bulletin Board System.

Beginning Document Number or BegDoc#: A unique number identifying the first page of a document or a number assigned to identify a native file.

Bibliographic Coding: Manually recording objective information from documents such as date, authors, recipients, carbon copies, and blind copies, and associating the information with a specific document. See Indexing; Coding.

Big Data: A catch phrase informally used to describe a large volume of information that is gathered or compiled over time, is often distributed across multiple storage locations, is not uniformly structured, and may be challenging to analyze with traditional technology solutions.

Binary: The base-2 numbering system used in digital computing that represents all numbers using combinations of zero and one.

Biometric Data (as used in the GDPR): Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data.

BIOS: See Basic Input Output System.

Bit: Binary digit—the smallest unit of computer data. A bit consists of either 0 or 1. There are eight bits in a byte. See Byte.

Bit Stream Backup: A sector-by-sector/bit-by-bit copy of a hard drive; an exact copy of a hard drive, preserving all latent data in addition to the files and directory structures. See Forensic Copy.

> *Glossary* definition cited: *Nucor Corp. v. Bell*, 2:06-CV-02972-DCN2008, WL 4442571, at *14 (D.S.C. Jan. 11, 2008). *United States v. Saboonchi*, 990 F. Supp. 2d 536, 540 (D. Md. 2014).

Bitmap (BMP): A file format that contains information on the placement and color of individual bits used to convey images composed of individual bits (pixels), for which the system file extension is .bmp.

Bitonal: A bitonal image uses only black and white.

Bits Per Inch (BPI): A unit of measure of data densities in disk and magnetic tape systems.

Bits Per Second (BPS): A measurement of the rate of data transfer. See Bandwidth.

Blockchain: A type of asymmetrically encrypted, distributed ledger technology dispersed across multiple locations, with the purpose of ensuring transparency and resistance to falsification. Either public, private, or a combination of both, blockchain is generally structured chronologically so that each subsequent transaction builds on the previous record. See Distributed Ledger Technology.

Blowback: The term for printing electronically stored information to hard copy.

BMP: See Bitmap.

Bookmark: A link to another location, either within the current file or location, or to an external location like a specific address on the internet.

Boolean Search: Boolean searches use keywords and logical operators such as "and," "or," and "not" to include or exclude terms from a search, and thus produce broader or narrower search results. See Natural Language Search.

Boot Sector/Record: See Master Boot Sector/Record; Volume Boot Sector/Record.

BPI: See Bits Per Inch.

BPS: See Bits Per Second.

Breach: An incident, or series of incidents, where an unauthorized person or entity accesses and/or removes secured data of an organization.

Bring Your Own Device Policy (BYOD): A policy whereby an organization specifies how personal computing devices, like smart phones, personal laptops, or portable tablets, can be used in the context of work for that organization, and may include provisions for the ownership and discoverability of the organization's data stored on the device. See The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495 (2018), *available at* https://thesedonaconference.org/publication/Commentary_on_BYOD.

Broadband: Commonly used in the context of high bandwidth internet access made available through a variety of quickly evolving technologies.

Brontobyte: 1,024 yottabytes. See Byte.

Browser: An application used to view and navigate the World Wide Web and other internet resources.

Bulletin Board System (BBS): A computer system or service that users access to participate in electronic discussion groups, post messages, and/or download files.

Burn: The process of moving or copying data to portable media such as a CD or DVD.

Bus: A parallel circuit that connects the major components of a computer, allowing the transfer of electric impulses from one connected component to any other.

BYOD: See Bring Your Own Device.

Byte (Binary Term): A basic measurement of most computer data consisting of 8 bits. Computer storage capacity is generally measured in bytes. Although characters are stored in bytes, a few bytes are of little use for storing a large amount of data. Therefore, storage is measured in larger increments of bytes. See Kilobyte; Megabyte; Gigabyte; Terabyte; Petabyte; Exabyte; Zettabyte; Yottabyte; Brontobyte; and Geopbyte (listed here in order of increasing volume).

Cache: A dedicated, temporary, high-speed storage location that can be used to store frequently used data for quick user access, allowing applications to run more quickly.

CAD: See Computer Aided Design.

CAL: See Continuous Active Learning.

Case De-Duplication: Eliminates duplicates to retain only one copy of each file per case. For example, if an identical file resides with three custodians, only the first custodian's copy will be saved. Also known as Cross Custodial De-Duplication, Global De-Duplication or Horizontal De-Duplication.

Catalog: See Index.

CCITT Group 4: A lossless compression technique/format that reduces the size of a file, generally about 5:1 over run-length

encoding (RLE) and 40:1 over bitmap. CCITT Group 4 compression may only be used for bitonal images.

CD: See Compact Disk.

CDPD: See Cellular Digital Packet Data.

Cellular Digital Packet Data (CDPD): A data communication standard utilizing the unused capacity of cellular voice providers to transfer data.

Central Processing Unit (CPU): The primary silicon chip that runs a computer's operating system and application software. It performs a computer's essential mathematical functions and controls essential operations.

Certificate: An electronic affidavit vouching for the identity of the transmitter. See Digital Certificate; Digital Signature; and Public Key Infrastructure (PKI) Digital Signature.

Chain of Custody: Documentation regarding the possession, movement, handling, and location of evidence from the time it is identified to the time it is presented in court or otherwise transferred or submitted; necessary to establish both admissibility and authenticity, and important to help mitigate risk of spoliation claims.

Characters Per Inch (CPI): A description of the number of characters that are contained in an inch of backup tape.

Checksum: A value calculated on a set of data as a means of verifying its authenticity to a copy of the same set of data, usually used to ensure data was not corrupted during storage or transmission.

Child: As related to Parent. See Document.

CIA Triad: The three basic security principles: confidentiality, integrity, and availability.

CJK: An abbreviation used in a discovery context to describe data that may contain one or more of Chinese, Japanese, and Korean languages.

Clawback Agreement: An agreement outlining procedures to be followed if documents or electronically stored information are inadvertently produced; typically used to protect against the waiver of privilege.

Client: (1) In a network, a computer that can obtain information and access applications on a server; (2) an application on a hard drive that relies on a server to perform some operations. See Thin Client.

Client Server: An architecture whereby a computer system consists of one or more server computers and numerous client computers (workstations). The system is functionally distributed across several nodes on a network and is typified by a high degree of parallel processing across distributed nodes. With client-server architecture, CPU intensive processes (such as searching and indexing) are completed on the server, while image viewing and Optical Character Recognition (OCR) occur on the client. This dramatically reduces network data traffic and insulates the database from workstation interruptions.

Clipboard: A holding area in a computer's memory that temporarily stores information copied or cut from a document or file.

Cloud Computing: "[A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (last visited February 10, 2020). For further discussion, see the cited NIST publication SP800-145.pdf.

Cluster (File): The smallest unit of storage space that can be allocated to store a file on operating systems. Windows and DOS organize hard disks based on clusters (also known as allocation units), which consist of one or more contiguous sectors. Disks using smaller cluster sizes waste less space and store information more efficiently.

Cluster (System): A collection of individual computers that appear as a single logical unit. Also referred to as matrix or grid systems.

Cluster Bitmap: Used in NTFS to keep track of the status (free or used) of clusters on the hard drive. See New Technology File System (NTFS).

Clustering: Unsupervised machine learning in which thematically similar files are grouped together based on the text of the individual files.

Coding: An automated or human process by which specific information is captured from documents. Coding may be structured (limited to the selection of one of a finite number of choices) or unstructured (a narrative comment about a document). See Indexing; Verbatim Coding; Bibliographic Coding; Level Coding; and Subjective Coding.

> *Glossary* definition cited: *Hinterberger v. Catholic Health System, Inc.*, 2013 WL 2250591 at *8 (W.D.N.Y. May 21, 2013). *Gordon vs. Kaleida Health*, 2013 WL 2250506 at *7 (W.D.N.Y. May 21, 2013).

Cold Storage: A description of data storage where the data is removed from a more expensive production server environment to a less expensive location that is not readily available to end users. See also Off-line Storage.

Co-Location: A company that provides a place where multiple unrelated companies can house their servers and other

computer equipment, offering advanced security, fire suppression, and redundant power, cooling and internet access. Also known as a Colo.

Comma Separated Value (CSV): A text file used for the transmission of data that separates data fields with a comma and typically encloses data in quotation marks.

Commercial Off-the-Shelf (COTS): Hardware or software products that are commercially manufactured, ready-made, and available for use by the general public without the need for customization.

Compact Disk (CD): A type of optical disk storage media; compact disks come in a variety of formats. These formats include CD-ROM (CD Read-Only Memory)—read-only; CD-R or CD+R (CD Recordable)—can be written to once and are then read-only; and CD-RW (CD Re-Writable)—can be written to multiple times.

Company Owned Personally Enabled (COPE): A personal computing device, such as a smart phone or laptop, that is owned by an organization but by policy of the organization is also used for personal business. See also BYOD.

Compound Document: A file that contains multiple files, often from different applications, by embedding objects or linked data; multiple elements may be included, such as images, text, animation, or hypertext. See Container File; Object Linking and Embedding (OLE).

Compression: The reduction in the size of a source file or files with the use of a variety of algorithms, depending on the software being used. Algorithms approach the task in a variety of ways, generally eliminating redundant information or by predicting where changes are likely to occur.

Compression Ratio: The ratio of the size of an uncompressed file to a compressed file; e.g., with a 10:1 compression ratio, a 10 KB file can be compressed to 1 KB.

Computer: Any one of a number of electronic devices that are used to process and analyze data using a variety of programs and programing languages as directed by a user or other system.

Computer Aided Design (CAD): The use of a wide range of computer-based tools that assist engineers, architects, and other design professionals in their design activities.

Computer Aided or Assisted Review: See Technology-Assisted Review.

Computer Client: A computer or program that requests a service of another computer system. A workstation requesting the contents of a file from a file server is a client of the file server. Also commonly used as synonymous with an email application, by reference to the Email Client. See Client; Thin Client.

Computer Forensics: The use of specialized techniques for recovery, authentication, and analysis of electronic data when an investigation or litigation involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis, or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end users or system-support personnel and generally requires strict adherence to chain-of-custody protocols. See Forensics; Forensic Copy.

Concatenate: Generally, to add by linking or joining to form a chain or series; the process of linking two or more databases of similar structure to enable the user to search, use, or reference them as if they were a single database.

Concept Search: The method of search that uses word meanings and ideas, without the presence of a particular word or phrase, to locate electronically stored information related to a desired concept. Word meanings can be derived from any of a number of sources, including dictionaries, thesauri, taxonomies, and ontologies, or computed mathematically from the context in which the words occur.

Conceptual Analytics: Using one or more of a number of mathematical algorithms or linguistic methodologies to analyze unstructured data by themes and ideas contained within the documents, enabling the grouping or searching of documents or other unstructured data by their common themes or ideas.

Confidence Interval: The range of values that is likely to contain the true parameter for a population to the specified confidence level (also called the Margin of Error). For example, sampling a set of documents at a 95 percent confidence level with an interval of plus-or-minus 2 percent means that 95 percent of samples will produce a result within 2 percent of the actual population.

Confidence Level: The percentage of samples for which the results are expected to correctly describe a population parameter within a provided confidence interval. For example, sampling a set of documents at a 95 percent confidence level means that 95 percent of samples taken from the population would contain the correct result within a specified interval. See Margin of Error.

Confidentiality (as a security term): A classification of data by use of a specific attribution of that data so that it is technically accessible only to authorized users or entities.

Consent (as used in the GDPR): Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear

affirmative action, signifies agreement to the processing of personal data relating to him or her.

Container File: A compressed file containing multiple files; used to minimize the size of the original files for storage and/or transporting. Examples include .zip, .pst, and .nsf files. The file must be ripped or decompressed to determine volume, size, record count, etc. and to be processed for litigation review and production. See also Decompression; Rip.

> *Glossary* definition cited: *Country Vintner of North Carolina, LLC v. E. & J. Gallo Winery, Inc.*, 718 F.3d 249, 252 (4th Cir. Apr. 29, 2013). *United States v. Life Care Centers Of America, Inc.*, 2015 WL 10987073, at *9 (E.D. Tenn. Aug. 31, 2015).

Content Comparison: A method of de-duplication that compares file content or output (to image or paper) and ignores metadata. See De-Duplication.

Contextual Search: Using one of a number of mathematical algorithms or linguistic methodologies to enlarge search results to include not only exact term matches but also matches where terms are considered in context of how and where they frequently occur in a specific document collection or more general taxonomy. For example, a search for the term "diamond" may bring back documents related to baseball but with no reference to the word diamond because the term frequently occurs within similar documents and therefore has a logical association.

Continuous Active Learning (CAL): A machine-learning algorithm that periodically analyzes users' decisions in order to rank unreviewed data, with the most likely desired data ranking first based on the users' previous decisions. See also Technology-Assisted Review.

Control Character: A character used by a computer program to perform a command rather than translate the character to written text.

Control Number: A unique record identifier within a database. Sometimes also referred to as Begdoc id.

Control Set: See Seed Set.

Conversation Index: A hexadecimal number string created by an email program on outgoing messages, indicating the relative position of a message within a specific email thread.

Cookie: A text file containing tracking information such as dates and times of website visits, deposited by a website onto a user's computer or mobile device. The text file is accessed each time the website is visited by a specific user and updated with browsing and other information. The main purpose of cookies is to identify users and possibly prepare customized web pages for them, including the personalization of advertising appearing on the websites.

Coordinated Universal Time (UTC): A high-precision atomic time standard with uniform seconds defined by International time and leap seconds announced at regular intervals to compensate for the earth's slowing rotation and other discrepancies. Leap seconds allow UTC to closely track Universal time, a time standard based not on the uniform passage of seconds but on the earth's angular rotation. Time zones around the world are expressed as positive or negative offsets from UTC. Local time is UTC plus or minus the time-zone offset for that location, plus an offset (typically +1) for daylight savings, if in effect. For example, 3:00 a.m. Mountain Standard Time = 10:00 UTC minus 7. As the zero point reference, UTC is also referred to as Zulu time (Z). See Normalization.

COPE: See Company Owned Personally Enabled.

Corrupted File: A file that has become damaged in some way, such as by a virus or by software or hardware failure, so that it is partially or completely unreadable by a computer.

COTS: See Commercial Off-the-Shelf.

CPI: See Characters Per Inch.

CPU: See Central Processing Unit.

CRC: See Cyclical Redundancy Checking.

CRM: See Customer Relationship Management Application.

Cross-Custodian De-Duplication: The suppression or removal of exact copies of files across multiple custodians for the purposes of minimizing the amount of data for review and/or production. Sometimes referred to as Case De-Duplication. See also De-Duplication.

Cryptocurrency: A digital-only form of currency, highlighted as having no central or regulating authority, which utilizes decentralized, distributed ledger technology called blockchain to record online transactions and issue new units of currency, denominated in terms of a virtual "token." See Blockchain; Distributed Ledger Technology.

Cryptography: A technique to scramble data to preserve confidentiality or authenticity.

CSV: See Comma Separated Value.

Cull (verb): To remove, or suppress from viewing, a document from a collection to be reviewed or produced. See Data Filtering; Harvesting.

Custodian: See Record Custodian; Record Owner.

Custodian De-Duplication: The removal or suppression of exact copies of a file found within a single custodian's data for the purposes of minimizing the amount of data for review and/or

production. Also known as Vertical De-duplication. See De-Duplication.

Customer Relationship Management (CRM) Application: A computer program that helps manage communications with client and contains contact information.

Cybersecurity: Measures undertaken to protect a network or system against unauthorized access or attack.

Cyclical Redundancy Checking (CRC): Used in data communications to create a checksum character at the end of a data block to ensure integrity and receipt of data transmission. See Checksum.

Cylinder: The set of tracks on both sides of each platter in a hard drive that is located at the same head position. See Platter.

DAC: See Digital to Analog Converter.

DAD: See Digital Audio Disk.

DAT: See Text Delimited File.

Data: Any information stored on a computer, whether created automatically by the computer, such as log files, or created by a user, such as the information entered on a spreadsheet. See Active Data; Latent Data.

Data Categorization: The process of classifying electronically stored information with supervised machine learning software, using categories created by either the user or automatically by the software based on the similar content of the individual files.

Data Cell: An individual field of an individual record. For example, in a table containing information about all of a company's employees, information about employee Joe Smith is stored in a single record, and information about his social security number is stored in an individual Data Cell. See Field.

Data Collection: See Harvesting.

Data Controller (as used in the GDPR): The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Element: A combination of characters or bytes referring to one separate piece of information, such as name, address, or age.

Data Exfiltration: Unauthorized transfer of data from a computer or other digital media device.

Data Extraction: The process of parsing data, including the text of the file, from any electronic documents into separate metadata fields such as date created and date last accessed.

> *Glossary* definition cited: *Race Tires America, Inc. v. Hoosier Racing Tire Corp.*, 674 F.3d 158, 161 (3d Cir. 2012).

Data Field: See Field.

Data File: See Text Delimited File.

Data Filtering: The process of identifying data based on specified parameters, such as date range, author, and/or keyword search terms, often used to segregate data for inclusion or exclusion in the document culling or review workflow.

Data Formats: The organization of information for display, storage, or printing. Data is sometimes maintained in certain common formats so that it can be used by various programs that may only work with a particular format, e.g. PDF or HTML. Also used by parties to refer to production specifications during the exchange of data during discovery.

Data Harvesting: See Harvesting.

Data Integrity: The process and procedure to ensuring that data is not improperly modified or deleted, whether through accident or malicious intent.

Data Lake: A repository of data from a variety of sources and in any of format, structured or unstructured. The collection of data is established to allow for the implementation of a variety of analytics. A data lake is distinguished from a data warehouse in that the data exists in its native, minimally processed (or "raw") form unless and until an analytical task or query is executed, generally requiring sophisticated data science methods. Data lakes are more comprehensive, as no data is denied from them and is typically stored indefinitely. See also Data Warehouse.

Data Map: A document or visual representation that records the physical or network location and format of an organization's data. Information about the data can include where the data is stored, physically and virtually, in what format it is stored, backup procedures in place, how the electronically stored information moves and is used throughout the organization, information about accessibility of the electronically stored information, retention and lifecycle management practices and policies, and identity of records custodians.

Data Mining: The process of knowledge discovery in databases (structured data); often techniques for extracting information, summaries, or reports from databases and data sets. In the context of electronic discovery, this term often refers to the processes used to analyze a collection of electronically stored information to extract evidence for production or presentation in an investigation or in litigation. See Text Mining.

Data Processor (as used in the GDRP): A natural or legal person (other than an employee of the data controller), public

authority, agency or other body which processes personal data on behalf of the data controller.

Data Set: A named or defined collection of data. See Production Data Set; Privilege Data Set.

Data Subject (as used in the GDRP): A natural person to whom personal data relates.

Data Subject Access Request (DSAR; as used in the GDPR): Also referred to as "the Right of Access," DSAR is one of eight rights in the GDPR and is defined as a request by an individual to a company or organization asking for access to the personal data the company holds upon the aforementioned individual, thus allowing the individual to be aware of and verify the lawfulness of any processing of his or her personal data. The individual is entitled to see information regarding why the individual's data was requested, how the data was processed, the timeframe of data processed, who the data has been disclosed to, if the disclosed data has been used to make an automated decision regarding the individual, and/or if the individual's data has been used by an organization to create a profile on that individual. May also be referred to as SAR.

Data Trust: An independent legal entity established to take custody, physically or virtually, of data from trustors, for the purpose of protecting data privacy and security while allowing the data to be accessed, on a limited basis under strict rules, for research or commercial purposes. Examples of data trusts include a consortium of medical institutions establishing a trust to hold patient records for medical research purposes, or a consortium of retailers establishing a trust to hold consumer data for market research purposes.

Data Verification: Assessment of data to ensure it has not been modified from a prior version. The most common method of verification is hash coding by using industry accepted

algorithms such as MD5, SHA1, or SHA2. See Digital Fingerprint; File-Level Binary Comparison; and Hash Coding.

Data Warehouse: A repository of mastered or enriched data from a variety of sources and in a more refined variety of formats. All collected data must be in structured form, either from ingestion of or manipulations to the raw data, for ease of identification and access. A data warehouse is distinguished from a data lake in that the data may be accessed from an index or with a simple query, analogous to obtaining records from an historical archive. See also Data Lake.

Database: A set of data elements consisting of at least one file or of a group of integrated files, usually stored in one location and made available to several users. The collection of information is organized into a predefined formatted structure and usually organized into fields of data that comprise individual records that are further grouped into data tables. Databases are sometimes classified according to their organizational approach, with the most prevalent approach being the relational database—a tabular database in which data is defined so that it can be reorganized and accessed in a number of different ways. Another popular organizational structure is the distributed database, which can be dispersed or replicated among different points in a network. Computer databases typically contain aggregations of data records or files, such as sales transactions, product catalogs and inventories, and customer profiles. For further discussion, see The Sedona Conference Database Principles, available for download at https://thesedonaconference.org/publication/Database_Principles.

Database Management System (DBMS): A software system used to access and retrieve data stored in a database.

Date Created: A common metadata field that contains the date a file was created or moved and the media where it currently resides.

Date Last Accessed: A common metadata field that contains the date a file was lasted accessed, meaning last opened or moved or even copied, depending on the technology used to copy.

Date Last Modified: A common metadata field that contains the date a file was last changed either by a modification to the content or format, printed, or changed by the automatic running of any macros that are executed upon the file being opened. The date-last-modified field does not normally reflect a change to a file's storage location or when the file was opened and read, and is thus often used as an electronic file date control field for discovery purposes.

Date Sent: A common metadata field that contains the date on which an email was sent.

Date Received: A common metadata field that contains the date on which an email was received.

Date/Time Normalization: See Normalization.

Daubert or Daubert Challenge: *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579, at 593–94 (1993), addresses the admission of scientific expert testimony to ensure that the testimony is reliable before considered for admission pursuant to Rule 702. The court assesses the testimony by analyzing the methodology and applicability of the expert's approach. Faced with a proffer of expert scientific testimony, the trial judge must determine first, pursuant to Rule 104(a), whether the expert is proposing to testify to (1) scientific knowledge that (2) will assist the trier of fact to understand or determine a fact at issue. This involves preliminary assessment of whether the reasoning or methodology is scientifically valid and whether it can be applied to the facts at issue. Daubert suggests an open approach and provides a list of

four potential factors: (1) whether the theory can be or has been tested; (2) whether the theory has been subjected to peer review or publication; (3) known or potential rate of error of that particular technique and the existence and maintenance of standards controlling the technique's operation; and (4) consideration of general acceptance within the scientific community.

DBMS: See Database Management System.

DDE: See Dynamic Data Exchange.

DEB: See Digital Evidence Bag.

Decompression: To expand or restore compressed data back to its original size and format. See Compression.

Decryption: Transformation of encrypted (or scrambled) data back to original form. See Encryption.

De-Duplication (de-dupe): The process of comparing electronic files or records based on their characteristics and removing, suppressing, or marking exact duplicate files or records within the data set for the purposes of minimizing the amount of data for review and production. De-duplication is typically achieved by calculating a file or record's hash value using a mathematical algorithm. De-duplication can be selective, depending on the agreed-upon criteria. See Case De-Duplication; Content Comparison; Cross-Custodian De-Duplication; Custodian De-Duplication; Data Verification; Digital Fingerprint; File-Level Binary Comparison; Hash Coding; Horizontal De-Duplication; Metadata Comparison; and Near Duplicates.

> *Glossary* definition cited: *CBT Flint Partners, LLC v. Return Path, Inc.*, 737 F.3d 1320, 1328 (Fed. Cir. Dec. 13, 2013).

Defensible Disposition: The effective disposal of physical and electronic information that does not need to be retained according to an organization's policies when the data is not or no longer subject to a legal requirement for retention, be it statutory

or as part of a litigation. See Disposition. For further discussion, see The Sedona Conference, *Commentary on Defensible Disposition*, 20 SEDONA CONF. J. 179 (2019), *available at* https://thesedonaconference.org/publication/Commentary_on_Defensible_Disposition.

Defragment (defrag): Use of a computer utility to reorganize files so they are more physically contiguous on a hard drive or other storage medium, when the files or parts thereof have become fragmented and scattered in various locations within the storage medium in the course of normal computer operations. Used to optimize the operation of the computer, it will overwrite information in unallocated space. See Fragmentation.

Deleted Data: Information that is no longer readily accessible to a computer user due to the intentional or automatic deletion of the data. Deleted data may remain on storage media in whole or in part until overwritten or wiped. Even after the data itself has been wiped, directory entries, pointers, or other information relating to the deleted data may remain on the computer. Soft deletions are data marked as deleted (and not generally available to the end user after such marking) but not yet physically removed or overwritten. Soft-deleted data can be restored with complete integrity.

Deletion: The process whereby data is removed from active files and other data storage structures on computers and rendered more inaccessible except through the use of special data recovery tools designed to recover deleted data. Deletion occurs on several levels in modern computer systems: (1) File-level deletion renders the file inaccessible to the operating system and normal application programs and marks the storage space occupied by the file's directory entry and contents as free and available to reuse for data storage; (2) Record-level deletion occurs when a record is rendered inaccessible to a database management system (DBMS) (usually marking the record storage

space as available for reuse by the DBMS, although in some cases the space is never reused until the database is compacted) and is also characteristic of many email systems; and (3) Byte-level deletion occurs when text or other information is deleted from the file content (such as the deletion of text from a word processing file); such deletion may render the deleted data inaccessible to the application intended to be used in processing the file, but may not actually remove the data from the file's content until a process such as compaction or rewriting of the file causes the deleted data to be overwritten.

De-NIST: The use of an automated filter program that screens files against the National Institute of Standards and Technology (NIST) list in order to remove files that are generally accepted to be system generated and have no substantive value in most instances. See NIST List.

De-skewing: The process of straightening skewed (tilted) images. De-skewing is one of the image enhancements that can improve OCR accuracy. Documents often become skewed when scanned or faxed.

Desktop: Generally refers to the working area of the display on an individual personal computer.

DFS: See Distributed File System.

Differential Backup: A method of backing up data that backs up data that is new or has been changed from that last full backup.

Digital: Information stored as a string of ones and zeros (numeric). Opposite of analog.

Digital Audio Disk (DAD): Another term for compact disk.

Digital Audio Tape: A magnetic tape generally used to record audio but can hold up to 40 gigabytes (or 60 CDs) of data if used

for data storage. Has the disadvantage of being a serial access device. Often used for backup.

Digital Certificate: Electronic records that contain unique secure values used to decrypt information, especially information sent over a public network like the internet. See Certificate; Digital Signature; and Public Key Infrastructure (PKI) Digital Signature.

Digital Evidence Bag (DEB): A container file format used for electronic evidence to preserve and transfer evidence in an encrypted or protected form that prevents deliberate or accidental alteration. The secure wrapper provides metadata concerning the collection process and context for the contained data.

Digital Fingerprint: A fixed-length hash code that uniquely represents the binary content of a file. See Data Verification, File-Level Binary Comparison, and Hash Coding.

Digital Linear Tape (DLT): A type of magnetic computer tape used to copy data from an active system for purposes of archiving or disaster recovery.

Digital Millennium Copyright Act (DMCA): United States copyright law enacted to protect against copyright infringement of data, address rights and obligations of owners of copyrighted material, and the rights and obligations of internet service providers on whose systems the infringing material may reside.

Digital Rights Management (DRM): A program that controls access to, movement, or duplication of protected data.

Digital Signature: A way to ensure the identity of the sender, utilizing public key cryptography and working in conjunction with certificates. See Certificate; Digital Certificate; and Public Key Infrastructure (PKI) Digital Signature.

Digital to Analog Converter (DAC): Converts digital data to analog data.

Digital Video Disk or Digital Versatile Disk (DVD): A plastic disk, like a CD, on which data can be optically written and read. DVDs can hold more information and can support more data formats than CDs. Formats include: DVD-R or DVD+R (DVD Recordable)—written to once and are then read-only; and DVD-RW (DVD Re-Writable)—can be written to multiple times.

Digital Visual Interface (DVI): A piece of hardware used to connect a video source to a video display device, like a computer monitor.

Digitize: The process of converting an analog value into a digital (numeric) representation. See Analog.

Directory: The organizational structure of a computer's file storage, usually arranged in a hierarchical series of folders and subfolders. Often simulated as a file folder tree.

Disaster Recovery Tapes: Portable magnetic storage media used to store data for backup purposes. See Backup Data; Backup Tape.

Discovery: The process of identifying, locating, preserving, securing, collecting, preparing, reviewing, and producing facts, information, and materials for the purpose of producing/obtaining evidence for use in the legal process. There are several ways to conduct discovery, the most common of which are interrogatories, requests for production of documents, and depositions. See Electronic Discovery.

Disk: Round, flat storage media with layers of material that enable the recording of data.

Disk Mirroring: The ongoing process of making an exact copy of information from one location to another in real time and often used to protect data from a catastrophic hard-disk failure or for long-term data storage. See Mirror Image; Mirroring.

Disk Partition: A discrete section of a computer's hard drive that has been virtually separated from one or more other partitions on the same drive.

Diskwipe: A utility that overwrites existing data. Various utilities exist with varying degrees of efficiency—some wipe only named files or unallocated space of residual data, thus unsophisticated users who try to wipe evidence may leave behind files of which they are unaware.

Disposition: The final business action carried out on a record. This action generally is to destroy or archive the record. Electronic record disposition can include "soft deletions," "hard deletions," "hard deletions with overwrites," "archive to long-term store," "forward to organization," and "copy to another media or format and delete (hard or soft)." See Deletion; Defensible Disposition.

Distributed Data: Information belonging to an organization that resides on portable media and nonlocal devices such as remote offices, home computers, laptop computers, personal digital assistants (PDAs), wireless communication devices (e.g., Blackberry), and internet repositories (including email hosted by internet service providers or portals and websites). Distributed data also includes data held by third parties such as application service providers and business partners. Note: Information Technology organizations may define distributed data differently (for example, in some organizations distributed data includes any non-server-based data, including workstation disk drives).

Distributed File System (DFS): The architecture of a system that is based upon the client/server schema, whereby one or more file servers store data that can be accessed by an unlimited number of remote clients, provided they have the authorization to do so**.**

Distributed Ledger Technology (DLT): A decentralized database technology existing across multiple locations or participants, eliminating the need for an intermediary or central authority to process, validate, or authenticate transactions and other types of data. DLT technology provides aforementioned validation and authentication. The records are only stored in the ledger once full consensus or acceptance is reached by all participants involved, at which point all files are timestamped and given a unique cryptographic signature, allowing all participants on the distributed ledger to view all transaction records.

DLT: See Digital Linear Tape; Digital Ledger Technology.

DMCA: See Digital Millennium Copyright Act.

Document (or Document Family): A collection of pages or files produced manually or by a software application, constituting a logical single communication of information, but consisting of more than a single stand-alone record. Examples include a fax cover, the faxed letter, and an attachment to the letter, the fax cover being the "Parent," and the letter and attachment being a "Child." See Attachment; Load File; Message Unit; and Unitization—Physical and Logical.

> *Glossary* definition cited: *Abu Dhabi Commercial Bank v. Morgan Stanley & Co. Inc.*, 2011 WL 3738979, at *2 (S.D.N.Y., Aug. 18, 2011). *United States v. Life Care Centers Of America, Inc.*, 2015 WL 10987073, at *8 (E.D. Tenn. Aug. 31, 2015).

Document Date: Generally, the term used to describe the date the document was last modified or put in final form; applies equally to paper and electronic files. See Date Last Modified; Date Created; Date Last Accessed; Date Sent; and Date Received.

Document Imaging Programs: Software used to scan paper documents and to store, manage, retrieve, and distribute documents quickly and easily.

Document Type or Doc Type: A bibliographic coding field that captures the general classification of a document, i.e., whether the document is correspondence, memo, report, article, and others.

DoD 5015: The Department of Defense standard addressing records management.

Domain: A group of servers and computers connected via a network and administered centrally with common rules and permissions.

DOS: See Microsoft-Disk Operating System (MS-DOS).

Dots Per Inch (DPI): Used as a measure of the resolution of an image, where more dots in the linear inch indicates a higher resolution.

Double-Byte Characters : See Unicode.

Double-Byte Language: See Unicode.

Download: To move data from a remote location to a local computer or network, usually over a network or the internet; also used to indicate that data is being transmitted from one location to another. See Upload.

DPI: See Dots Per Inch.

Draft Record: A preliminary version of a record before it has been completed, finalized, accepted, validated, or filed. Such records include working files and notes. Records and information management policies may provide for the destruction of draft records upon finalization, acceptance, validation, or filing of the final or official version of the record. However, draft records generally must be retained if: (1) they are deemed to be

subject to a legal hold; or (2) a specific law or regulation mandates their retention; and policies should recognize such exceptions.

Drag and Drop: The movement of files by dragging them with the mouse and dropping them in another place.

DRAM: See Dynamic Random Access Memory.

Drive Geometry: A computer hard drive is made up of a number of rapidly rotating platters that have a set of read/write heads on both sides of each platter. Each platter is divided into a series of concentric rings called tracks. Each track is further divided into sections called sectors, and each sector is subdivided into bytes. Drive geometry refers to the number and positions of each of these structures.

Driver: A computer program that controls various hardware devices such as the keyboard, mouse, or monitor and makes them operable with the computer.

DRM: See Digital Rights Management.

Drop-Down Menu: A menu window that opens on-screen to display context-related options. Also called pop-up menu or pull-down menu.

DSAR: See Data Subject Access Request.

DVD: See Digital Video Disk or Digital Versatile Disk.

DVI: See Digital Visual Interface.

Dynamic Data Exchange (DDE): A form of interprocess communications used by Microsoft Windows to support the exchange of commands and data between two simultaneously running applications.

Dynamic Random Access Memory (DRAM): A memory technology that is periodically refreshed or updated—as opposed to

static RAM chips that do not require refreshing. The term is often used to refer to the memory chips themselves.

Dynamic Search: A term used to describe a saved search that is updated each time the search is run to account for changes in the search corpus, such as added data or coding information. See also Static Search.

Early Case Assessment (ECA): The process of assessing the merits of a case early in the litigation lifecycle to determine its viability. The process may or may not include the collection, analysis, and review of data.

Early Data Assessment (EDA): The process of separating possibly relevant electronically stored information from nonrelevant electronically stored information using both computer techniques, such as date filtering or advanced analytics, and human-assisted logical determinations at the beginning of a case. This process may be used to reduce the volume of data collected for processing and review. See also Early Case Assessment.

ECA: See Early Case Assessment.

ECM: See Enterprise Content Management.

EDA: See Early Data Assessment.

EDI: See Electronic Data Interchange.

eDiscovery: See Electronic Discovery.

EDMS: See Electronic Document Management System.

e-doc: A colloquial term used to refer to an electronic document that is not an email.

e-file: A colloquial term used to refer to an electronic file or a colloquial term used to describe the process of submitting a file electronically.

Electronic Data Interchange (EDI): Eliminating forms altogether by encoding the data as close as possible to the point of the transaction; automated business information exchange.

Electronic Discovery (eDiscovery): The process of identifying, locating, preserving, collecting, preparing, reviewing, and producing electronically stored information (ESI) in the context of the legal process. See Discovery.

> *Glossary* definition cited: *Gordon v. Kaleida Health*, 2013 WL 2250579, at *2 (W.D.N.Y. May 21, 2013). *Hinterberger v. Catholic Health System Inc.*, 2013 WL 2250603, at *2 (W.D.N.Y. May 21, 2013). *Small v. University Medical Center of Southern Nevada*, 2014 WL 4079507, at *5 (D. Nev. Aug. 18, 2014).

Electronic Document Management: The process of using a computer program to manage individual unstructured files, either those created electronically or scanned to digital form from paper. See Information Lifecycle Management.

Electronic Document Management System (EDMS): A system to electronically manage documents during all life cycles. See Electronic Document Management.

Electronic File Processing: See Processing Data.

Electronic Image: An individual page or pages of an electronic document that has been converted into a static format, for example PDF or TIFF. See PDF and TIFF.

Electronic Record: Information recorded in a form that requires a computer or other machine to process it.

Electronically Stored Information (ESI): As referenced in the U.S. Federal Rules of Civil Procedure, information that is stored electronically, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard copy (i.e., on paper).

Glossary definition cited: *EEOC v. BOK Financial Corp.*, 2013 WL 12330078 at *1 (D.N.M. May 7, 2013).

Elusion: The percentage of documents of a search's null set that were missed by the search, usually determined with review of a random sample of the null set. The elusion rate can be multiplied by the number of documents in the null set to estimate how many documents were missed by the search.

Email (Electronic Mail): An electronic means for sending, receiving, and managing communications via a multitude of different structured data applications (email client software), such as Outlook or Lotus Notes or those often known as "webmail," such as Gmail or Yahoo Mail. See Email Message.

Glossary definition cited: *Rosehoff, Ltd. v. Truscott Terrace Holdings LLC*, 2016 WL 2640351, at *5 (W.D.N.Y. May 10, 2016).

Email Address: A unique value given to individual user accounts on a domain used to route email messages to the correct email recipient, most often formatted as follows: user-ID@ domain-name. See Email Message.

Email Archiving: A systematic approach to retaining and indexing email messages to provide centralized search and retrieval capabilities. See Journaling.

Email Client: See Email (Electronic Mail).

Email Message: A file created or received via an electronic mail system. Any attachments that may be transmitted with the email message are not part of the email message but are part of the Message Unit and Document Family.

Email Store: A file or database containing individual email messages. See Container File; Message Unit; OST; PST; and NSF.

Email String: An electronic conversation between two or more parties via email. Also referred to as an email thread. See Thread.

Email Threading: A technical process of regrouping emails that comprise an email discussion, including replies and forwards.

Embedded Object: A file or piece of a file that is copied into another file, often retaining the utility of the original file's application; for example, a part of a spreadsheet embedded into a word processing document that still allows for editing and calculations after being embedded. See Compound Document.

> *Glossary* definition cited: *United States v. Life Care Centers Of America, Inc.*, 2015 WL 10987073, at *9 (E.D. Tenn. Aug. 31, 2015).

EML: File extension of a generic email message file.

Emoji: An image utilized to express an emotion or thought in an electronic message.

Emoticon: An image or set of keyboard characters used to depict a facial expression and used to indicate the author's intended tone or feelings.

Encapsulated PostScript (EPS): Uncompressed files for images, text, and objects. Can only be printed on printers with PostScript drivers.

Encoding: To change or translate into code; to convert information into digital format. For software, encoding is used for video and audio references, such as encoding analog format into digital or raw digital data into compressed format.

Encryption: A procedure that renders the contents of a message or file unreadable to anyone not authorized to read it; used to protect electronically stored information being stored or transferred from one location to another.

Encryption Key: A data value that is used to encrypt and decrypt data. The number of bits in the encryption key is a rough measure of the encryption strength; generally, the more bits in the encryption key, the more difficult it is to break. See Decryption.

End Document Number or EndDoc#: A common metadata field that contains the Bates number of the last page of a document.

End of File (EOF): A distinctive code that uniquely marks the end of a data file.

Enhanced Parallel Port (EPP): See Port.

Enhanced Small Device Interface (ESDI): A defined, common electronic interface for transferring data between computers and peripherals, particularly disk drives.

Enhanced Titles: A bibliographic coding field that captures a meaningful/descriptive title for a document based on a reading of the document as opposed to a verbatim title lifted as it appears on the face of the document. See Verbatim Coding.

Enterprise Architecture: Framework of information systems and processes integrated across an organization. See Information Technology Infrastructure.

Enterprise Content Management (ECM): Management of an organization's unstructured electronically stored information, regardless of where it exists, throughout the entire lifecycle of the ESI.

EOF: See End of File.

Ephemeral Data: Data that exists for a very brief, temporary period and is transitory in nature, such as data stored in random access memory (RAM).

EPP: See Enhanced Parallel Port.

EPS: See Encapsulated PostScript.

Erasable Optical Disk: A type of optical disk that can be erased and new electronically stored information added; most optical disks are read only.

ESDI: See Enhanced Small Device Interface.

ESI: See Electronically Stored Information.

Ethernet: A common way of networking personal computers to create a Local Area Network (LAN).

Evidentiary Image or Copy: See Forensic Copy.

Exabyte: 1,024 petabytes (approximately one billion gigabytes). See Byte.

Exception Files: See Processing Exception.

Exchange Server: A server running Microsoft Exchange messaging and collaboration software. It is widely used by enterprises using Microsoft infrastructure solutions. Among other things, Microsoft Exchange manages email, shared calendars, and tasks.

Expanded Data: See Decompression.

Export: The process of saving data or a subset of data in a format that can be used or imported by another system.

Extended Partitions: If a computer hard drive has been divided into more than four partitions, extended partitions are created. Under such circumstances each extended partition contains a partition table in the first sector that describes how it is further subdivided. See Disk Partition.

Extensible Markup Language (XML): A software coding language specification developed by the W3C (World Wide Web Consortium—the web development standards board). XML is a pared-down version of Standard Generalized Markup

Language (SGML), designed especially for web documents. It allows designers to create their own customized tag, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

Extraction: The process of parsing a file into separate components for further analysis or to prepare for loading into a database. Text and metadata are commonly extracted from a file in order to prepare them for loading to a database.

Extranet: The portion of an intranet site that is accessible by users outside of a company or organization hosting the intranet. This type of access is often utilized in cases of joint defense, joint venture, and vendor-client relationships.

False Negative: A result from a search that is not correct because it fails to indicate a match or hit where one exists.

False Positive: A result from a search that is not correct because it indicates a match or hit where there is none.

Fast Mode Parallel Port: See Port.

FAT: See File Allocation Table.

Federal Information Processing Standards (FIPS): A set of standards issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949, as amended by the Computer Security Act of 1987, Public Law 100-235.

Fiber Optics: A method of transmitting information by sending light pulses over cables made from thin strands of glass.

Field (or Data Field): A defined area of a file or data table used to record an individual piece of standardized data, such as the author of a document, a recipient, or the date of a document.

Field Mapping: The process of normalizing data to the structure of an existing database for purposes of loading the data to the correct field, after validating the data type is the same. For example, mapping the data from a field called Date to an existing field in a database named DocDate.

Field Separator or Field Delimiter: A character in a text delimited file that separates the fields in an individual record. For example, the CSV format uses a comma as the field separator. See Text Delimited File.

File: A collection of related data or information stored as a unit under a specified name on storage medium.

File Allocation Table (FAT): An internal data table on hard drives that keeps track of where the files are stored. If a FAT is corrupt, a drive may be unusable, yet the data may be retrievable with forensics. See Cluster (File).

File Compression: See Compression.

File Extension: Many systems, including DOS and UNIX, allow a filename extension that consists of one or more characters following the proper filename. For example, image files are usually stored as .bmp, .gif, .jpg or .tiff. Audio files are often stored as .aud or .wav. There are a multitude of file extensions identifying file formats. The filename extension should indicate what type of file it is; however, users may change filename extensions to evade firewall restrictions or for other reasons. Therefore, file types should be identified at a binary level rather than relying on file extensions. To research file types, see http://www.filext.com. Different applications can often recognize only a predetermined selection of file types. See Format (noun).

File Format: The organization or characteristics of a file that determine with which software programs it can be used. See Format (noun).

File Header: See Header.

File-Level Binary Comparison: A method of de-duplication using the digital fingerprint (hash) of a file to compare the individual content and location of bytes in one file against those of another file. See Data Verification; De-Duplication; Digital Fingerprint; and Hash Coding.

File Plan: A document containing the identifying number, title, description, and disposition authority of files held or used in an office.

File Server: A computer that serves as a storage location for files on a network. File servers may be employed to store electronically stored information, such as email, financial data, or word processing information or to back up the network. See Server.

File Sharing: Providing access to files or programs to multiple users on a network.

File Signature: See Digital Signature.

File Slack: See Slack Space.

File System: The means by which an operating system or program organizes and keeps track of electronically stored information in terms of logical structures and software routines to control access to the ESI, including the structure in which the files are named, stored, and organized. The file system also tracks data when a user copies, moves, or deletes a file or subdirectory.

File Table: A specific table in a Structured Query Language (SQL) database that allows for the storage of files and information that can be directly accessible from the Windows interface, as opposed to only from within SQL itself. See Master File Table; SQL.

File Transfer: The process of moving or transmitting a copy of a file from one location to another, as between two programs or from one computer to another.

File Transfer Protocol (FTP): An internet protocol that governs the transfer of files between computers over a network or the internet. The terms FTP server or FTP site are commonly used to refer to a location to upload/download and exchange data, particularly in large volume.

> *Glossary* definition cited: *Balance Point Divorce Funding, LLC v. Scrantom*, 305 F.R.D. 67, 75 (S.D.N.Y. 2015).

File Type: The description of a file's contents based on the performance of a signature analysis, which analyzes the internal structure of the file, typically the header or footer, which contains information about the true program-related origin of the file, even where the file extension has been changed.

Filename: The name used to identify a specific file in order to differentiate it from other files, typically comprised of a series of characters, a dot, and a file extension (e.g., sample.doc). See File Extension and Full Path.

Filter (verb): See Data Filtering.

Filtering: See Data Filtering.

FIPS: See Federal Information Processing Standards.

Firewall: A set of related security programs and/or hardware that protects the resources of a private network from unauthorized access by users outside of an organization or user group. A firewall filters information to determine whether to forward the information toward its destination.

Flash Drive: A small, removable data storage device that uses flash memory and connects via a USB port. Also referred to as Jump Drive, Key Drive, and Thumb Drive.

Flash Memory: A type of computer memory used for storage of data to a physical disk by electrical impulses.

Flat File: A nonrelational, text-based file (i.e., a word processing document).

Floppy Disk: A thin magnetic film disk housed in a protective sleeve, used to copy and transport relatively small amounts of data.

F-Measure: Also known as the F1 Score or the F Score, a measure of a search's accuracy calculated by using precision and recall. (Precision x Recall) / (Precision + Recall).

Folder: See Directory.

Forensic Copy: An exact copy of an entire physical storage media (hard drive, CD-ROM, DVD-ROM, tape, etc.), including all active and residual data and unallocated or slack space on the media. Forensic copies are often called images or imaged copies. See Bit Stream Backup; Mirror Image.

> *Glossary* definition cited: *CBT Flint Partners, LLC v. Return Path, Inc.*, 737 F.3d 1320, 1328 (Fed. Cir. Dec. 13, 2013). *Javeler Marine Services LLC v. Cross*, 175 F. Supp. 3d 756, 762 (S.D. Tex. 2016).

Forensics: The scientific examination and analysis of data held on, or retrieved from, a computer in such a way that the information can be used as evidence in a court of law. It may include the secure collection of computer data; the examination of suspect data to determine details such as origin and content; the presentation of computer-based information to courts of law; and the application of a country's laws to computer practice. Forensics may involve recreating deleted or missing files from hard drives, validating dates and logged-in authors/editors of documents, and certifying key elements of documents and/or hardware for legal purposes.

Form of Production: The specifications for the exchange of documents and/or data between parties during a legal dispute. It is used to refer both to file format (e.g., native vs. imaged format, with agreed-upon metadata and extracted text in a load file) and the media on which the documents are produced (paper vs. electronic). See Load File; Native Format.

Format (noun): The internal structure of a file, which defines the way it is stored and used. Specific applications may define unique formats for their data (e.g., "MS Word document file format"). Many files may only be viewed or printed using their originating application or an application designed to work with compatible formats. There are several common email formats, such as Outlook and Lotus Notes. Computer storage systems commonly identify files by a naming convention that denotes the format (and therefore the probable originating application). For example, DOC for Microsoft Word document files; XLS for Microsoft Excel spreadsheet files; TXT for text files; HTM for HyperText Markup Language (HTML) files such as web pages; PPT for Microsoft PowerPoint files; TIF for tiff images; PDF for Adobe images; etc. Users may choose alternate naming conventions, but this will likely affect how the files are treated by applications.

> *Glossary* definition cited: *EEOC v. BOK Financial Corp.*, 2013 WL 12330078 at *1 (D.N.M. May 7, 2013).

Format (verb): To make a drive ready to store data within a particular operating system. Erroneously thought to "wipe" drive. Typically, formatting only overwrites the File Allocation Table, but not the actual files on the drive.

Forms Processing: A specialized imaging application designed for handling pre-printed forms. Forms processing systems often use high-end (or multiple) OCR engines and elaborate data

validation routines to extract handwritten or poor-quality print from forms that go into a database.

Fragmentation: The process by which parts of files are separately stored in different areas on a hard drive or removable disk in order to utilize available space. See Defragment.

FTP: See File Transfer Protocol.

Full Duplex: Data communications devices that allow full-speed transmission between computers in both directions at the same time.

Full Path: A file location description that includes the drive, starting or root directory, all attached subdirectories, and ending with the file or object name. Often referred to as the Path Name.

Full-Text Indexing: The extraction and compilation of text from a collection of ESI. Text is gathered both from the body of the data and selected metadata fields. See Index.

Full-Text Search: The ability to search an index of all the words in a collection of electronically stored information for specific characters, words, numbers, and/or combinations or patterns thereof in varying degrees of complexity.

Fuzzy Search: The method of searching an index that allows for one or more characters in the original search terms to be replaced by wild-card characters, so that a broader range of data hits will be returned. For example, a fuzzy search for "fell" could return "tell" "fall," or "felt."

GAL: See Global Address List.

GB: See Gigobyte.

GDPR: See General Data Protection Regulation.

General Data Protection Regulation (GDPR): The GDPR imposes a single set of data protection and privacy regulations and

rights for all data subjects of the European Union (EU) and European Economic Area (EEA), both residents and those performing regulated tasks within the EU or EEA. The Regulations consists of 99 Articles, grouped into 11 chapters, and 173 recitals with explanatory remarks.

Genetic data (as used in the GDPR): Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. Information about a natural person's physical or mental health, past, present and future, including the provision of health care services is included.

Geopbyte: 1,024 brontobytes. See Byte.

Ghost Imaging: A data copying methodology that uses software to copy the entire content of a hard drive to a single compressed file or set of files. The copy includes all programs and configuration settings and is often used to restore a template copy to new computers or servers.

GIF: See Graphics Interchange Format.

Gigabyte (GB): 1,024 megabytes. See Byte.

Global Address List (GAL): A Microsoft Outlook directory of all Microsoft Exchange users and distribution lists to which messages can be addressed. The global address list may also contain public folder names. Entries from this list can be added to a user's personal address book.

Global De-Deduplication: See Case De-Duplication.

Global Positioning System (GPS): A technology used to track the location of ground-based objects using three or more orbiting satellites.

GMT Timestamp: Identification of a file using Greenwich Mean Time as the central time authentication method. See Normalization.

GPS: See Global Positioning System.

GPS Generated Timestamp: Timestamp that identifies time as a function of its relationship to Greenwich Mean Time.

Graphical User Interface (GUI, pronounced "gooey"): An interface to a computer or device comprised of pictures and icons, rather than words and numbers, by which users can interact with the device.

Graphics Interchange Format (GIF): A common file format for storing images first originated by CompuServe, an internet service provider, in 1987. Limited to 256 colors.

Grayscale: See Scale-to-Gray.

Groupware: Software designed to operate on a network and allow several people to work together on the same documents and files.

GUI: See Graphical User Interface.

Half Duplex: Transmission systems that can send and receive data between computers, but not at the same time.

Handshake: A transmission that occurs at the beginning of a communication session between computers to establish the technical format of the communication.

Handwriting Recognition Software (HRS): Software that interprets handwriting into machine readable form.

Hard Drive: A storage device consisting of one or more magnetic media platters on which digital data can be written and erased. See Platter.

Harvesting: The process of retrieving or collecting electronically stored information from any media; an eDiscovery vendor or specialist "harvests" ESI from computer hard drives, file servers, CDs, backup tapes, portable devices, and other sources for processing and loading to storage media or a database management system.

Hash Coding (also Hash Value, Hash): A mathematical algorithm that calculates a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently ensuring that data has not been modified. Common hash algorithms include MD5 and SHA. See Data Verification; Digital Fingerprint; and File-Level Binary Comparison.

> *Glossary* definition cited: *United States v. Life Care Centers Of America, Inc.*, 2015 WL 10987073, at *18 (E.D. Tenn. Aug. 31, 2015). *United States v. Apple MacPro Computer*, 851 F.3d 238, 242 (3d Cir. 2017). *Digital Assurance Certification, LLC v. Pendolino*, 2017 WL 4342316, at *7 (M.D. Fla. Sept. 29, 2017).

HDMI: See High-Definition Multimedia Interface.

Head: Devices which ride very closely to the surface of the platter on a hard drive and allow information to be read from and written to the platter.

Header: Data placed at the beginning of a file or section of data that in part identifies the file and some of its attributes. A header can consist of multiple fields, each containing its own value. See Message Header.

Hexadecimal: A number system with a base of 16. The digits are 0-9 and A-F, where F equals the decimal value of 15.

Hidden Files or Data: Files or data not readily visible to the user of a computer. Some operating system files are hidden to

prevent inexperienced users from inadvertently deleting or changing these essential files. See Steganography.

Hierarchical Storage Management (HSM): Software that automatically migrates files from online to less expensive near-line storage, usually on the basis of the age or frequency of use of the files.

High-Definition Multimedia Interface (HDMI): An interface for the transmittal of audio and video signals from a source to a device, like a television or computer display.

High Technology Crime Investigation Association (HTCIA): A computer forensics nonprofit association; resources include educational programs and Listservs. See https://htcia.org/.

Hit Report or Hit List: A report containing search terms or search phrases used on a set of data, which details the results of each term or phrase as applied to that data set, typically specifying the number of search hits per term or phrase across the entire search corpus, and the number of files returned by each term or phrase.

Hold: See Legal Hold.

Honey Pot: A computer system that acts as a decoy to lure cyber attackers by appearing to contain something of value, enabling those attacks to be more readily detected and studied.

Horizontal De-Duplication: A way to identify electronically stored information duplicated across multiple custodians or other production data sets, normally by comparing hash algorithms to identify duplicates and then removing or suppressing those duplicates. See Case De-Duplication; De-Duplication.

Host: In a network, the central computer that controls the remote computers and holds the central databases.

Glossary definition cited: *Hinterberger v. Catholic Health System, Inc.*, 2013 WL 2250591 at *1 (W.D.N.Y. May 21, 2013).

HRS: See Handwriting Recognition Software.

HSM: See Hierarchical Storage Management.

HTCIA: See High Technology Crime Investigation Association.

HTML: See HyperText Markup Language.

HTTP: See HyperText Transfer Protocol.

Hub: A network device that connects multiple computers and peripherals together, allowing them to share network connectivity. A central unit that repeats and/or amplifies data signals being sent across a network.

Hyperlink: A pointer in a hypertext document—usually appearing as an underlined or highlighted word or picture—that, upon selection, sends a user to another location either within the current document or to another location accessible on the network or internet.

HyperText: Text that includes hyperlinks or shortcuts to other documents or views, allowing the reader to easily jump from one view to a related view in a nonlinear fashion.

HyperText Markup Language (HTML): Developed by CERN of Geneva, Switzerland; the most common programming language format used on the internet. HTML+ adds support for multimedia. The tag-based ASCII language used to create pages on the World Wide Web uses tags to tell a web browser to display text and images. HTML is a markup or "presentation" language, not a programming language. Programming code can be imbedded in an HTML page to make it interactive. See Java.

HyperText Transfer Protocol (HTTP): The underlying protocol used by the World Wide Web. HTTP defines how messages are

formatted and transmitted, and what actions servers and browsers should take in response to various commands. For example, when you enter a website URL in your browser, this sends an HTTP command to the web server directing it to fetch and transmit the requested site. HTTPS adds a layer of encryption to the protocol to protect the information that is being transmitted and is often used by application service providers to protect the data being viewed over the web.

IaaS: See Infrastructure as a Service.

Icon: In a graphical user interface (GUI), a picture or drawing that is activated by clicking a mouse to command the computer program to perform a predefined series of actions.

ICR: See Intelligent Character Recognition.

IDE: See Integrated Drive Electronics.

IDS: See Intrusion Detection System.

IEEE: See Institute of Electrical and Electronic Engineers.

ILM: See Information Lifecycle Management.

IM: See Instant Messaging.

Image (noun): An electronic or digital picture of a document (e.g., TIFF, PDF, etc.). See Image Processing; Processing Data; and Render Images.

Image (verb): To make an identical copy of a storage device, including empty sectors. Also known as creating a mirror image or mirroring the drive. See Bit Stream Backup; Forensic Copy; and Mirror Image.

> *Glossary* definition cited: *CBT Flint Partners, LLC v. Return Path, Inc.*, 737 F.3d 1320, 1328 (Fed. Cir. Dec. 13, 2013). *Colosi v. Jones Lang LaSalle Americas, Inc.*, 781 F.3d 293, 297 (6th Cir. 2015). *Javeler Marine Services LLC v. Cross*, 175 F. Supp. 3d 756, 762 (S.D. Tex. 2016).

Image Copy or Imaged Copy: See Forensic Copy.

Image Enabling: A software function that creates links between existing applications and stored images.

Image File Format: See File Format; Format (noun).

Image Key: The name of an image and cross reference to the image's file in a document load file, often the Bates number of the page. See Bates Number.

Image Processing: To convert data from its current/native format to a fixed image for the purposes of preserving the format of a document and facilitating the transfer between parties, typically with the addition of a Bates number to the face of each image. See Bates Number; Form of Production; Native Format; Processing Data; Render Images.

Image Processing Card (IPC): A board mounted in a computer, scanner or printer that facilitates the acquisition and display of images. The primary function of most IPCs is the rapid compression and decompression of image files.

Import: The process of bringing data into an environment or application that has been exported from another environment or application.

Inactive Record: Records related to closed, completed, or concluded activities. Inactive records are no longer routinely referenced but may be retained in order to fulfill reporting requirements or for purposes of audit or analysis. Inactive records generally reside in a long-term storage format, remaining accessible for purposes of business processing only with restrictions on alteration. In some business circumstances, inactive records may be reactivated.

Incident Response (IR): The workflow developed to address and manage the impact of a security breach or cyberattack.

Incremental Backup: A method of backing up data that is new or has been changed from that last backup of any kind, be it a full backup or the last incremental backup.

Index: A searchable catalog of information created to maximize storage efficiency and allow for improved search. Also called catalog. See Full-Text Indexing.

Index/Coding Fields: Database fields used to categorize and organize records. Often user-defined, these fields can be used for searching for and retrieving records. See Coding.

Indexing: (1) The process of organizing data in a database to maximize storage efficiency and optimize searching; (2) Objective coding of documents to create a list similar to a table of contents. See Coding.

Information: For the purposes of this document, information is used to mean hard-copy documents and electronically stored information.

Information Governance: The comprehensive, interdisciplinary framework of policies, procedures, and controls used by mature organizations to maximize the value of an organization's information while minimizing associated risks by incorporating the requirements of: (1) eDiscovery, (2) records and information management, and (3) privacy/security, into the process of making decisions about information. See The Sedona Conference, *Commentary on Information Governance, Second Edition*, 20 SEDONA CONF. J. 95 (2019), *available at* https://thesedonaconference.org/publication/Commentary_on_Information_Governance.

Information Lifecycle Management (ILM): A phrase used to discuss the policies and procedures governing the management of data within an organization, from creation through destruction. See Disposition; Electronic Document Management; Information Governance.

Information Retrieval: The process of searching for and finding relevant electronically stored information within an information system using a variety of methods, processes, and technologies, including keyword search, categorization, concept clustering, machine learning, and technology-assisted review.

Information Systems (IS) or Information Technology (IT): Usually refers to the department of an entity that designs, maintains, and assists users with regard to the computer infrastructure.

Information Technology (IT) Infrastructure: The overall makeup of business-wide technology operations, including mainframe operations, standalone systems, email, networks (WAN and LAN), internet access, customer databases, enterprise systems, and application support, regardless of whether managed, utilized, or provided locally, regionally, globally, etc., or whether performed or located internally or by outside providers (outsourced to vendors). The IT infrastructure also includes applicable standard practices and procedures, such as backup procedures, versioning, resource sharing, retention practices, system cleanup, and the like. See Enterprise Architecture.

Infrastructure as a Service (IaaS): A form of cloud computing whereby a third-party service provider offers, on demand, a part of its computer infrastructure remotely. Specific services may include servers, software, or network equipment resources that can be provided on an as-needed basis without the purchase of the devices or the resources needed to support them. See Cloud Computing.

Inline Image: Images that appear on a web page.

Input device: Any peripheral that allows a user to communicate with a computer by entering information or issuing commands (e.g., keyboard).

Instant Messaging (IM): A form of electronic communication involving immediate correspondence between two or more online users. Instant messages differ from email in their limited metadata and in that messages are not stored past the messaging session.

Institute of Electrical and Electronic Engineers (IEEE): An international association that advocates the advancement of technology as it relates to electricity. IEEE sponsors meetings, publishes a number of journals, and establishes standards. See https://www.ieee.org.

Integrated Drive Electronics (IDE): An engineering standard for interfacing computers and hard disks.

Integrated Services Digital Network (ISDN): An all-digital network that can carry data, video, and voice.

Intelligent Character Recognition (ICR): The conversion of scanned images (bar codes or patterns of bits) to computer recognizable codes (ASCII characters and files) by means of software/programs that define the rules of and algorithms for conversion; helpful for interpreting handwritten text. See Handwriting Recognition Software (HRS); Optical Character Recognition (OCR).

Interlaced: To refresh only every other line of a display once per refresh cycle. Since only half the information displayed is updated each cycle, interlaced displays are less expensive than noninterlaced. However, interlaced displays are subject to jitters. The human eye/brain can usually detect displayed images that are completely refreshed less than 30 times per second.

Interleave: To arrange data in a noncontiguous way to increase performance. When used to describe disk drives, it refers to the way sectors on a disk are organized. In one-to-one interleaving, the sectors are placed sequentially around each track. In two-to-one interleaving, sectors are staggered so that consecutively

numbered sectors are separated by an intervening sector. The purpose of interleaving is to make the disk drive more efficient. The disk drive can access only one sector at a time, and the disk is constantly spinning beneath.

International Organization for Standardization (ISO): A worldwide federation of national standards organizations, founded to promote industrial and commercial standards. See https://www.iso.org.

International Telecommunication Union (ITU): An international organization under the UN, headquartered in Geneva, Switzerland, concerned with developing international data communications standards for the telecommunications industry; known as CCITT prior to March 1, 1993. See http://www.itu.int.

Internet: A worldwide interconnected system of networks that all use the TCP/IP communications protocol and share a common address space. The internet supports services such as email, the World Wide Web, file transfer (FTP), and Internet Relay Chat (IRC). Also known as "the net," "the information superhighway," and "cyberspace." See Transmission Control Protocol/Internet Protocol (TCP/IP).

Internet of Things (IoT): A catchall term used to describe a broad array of electronic devices, such as computers or sensors in cars, refrigerators, lights, or security systems, that are connected to the internet and may collect, store, and/or share information.

Internet Protocol (IP): The principal communications protocol for data communications across the internet.

Internet Protocol (IP) Address: A unique name that identifies the physical location of a server on a network, expressed by a numerical value (e.g., 128.24.62.1). See Transmission Control Protocol/Internet Protocol (TCP/IP).

Internet Publishing Software: Specialized software that allows materials to be published to the internet. The term internet publishing is sometimes used to refer to the industry of online digital publication as a whole.

Internet Relay Chat (IRC): A system allowing internet users to chat in real time.

Internet Service Provider (ISP): A business that provides access to the internet, usually for a fee.

Inter-Partition Space: Unused sectors on a track located between the start of the partition and the partition boot record of a hard drive. This space is important because it is possible for a user to hide information here. See Partition; Track.

Intranet: A secure, private network that uses internet-related technologies to provide services within an organization or defined infrastructure.

> *Glossary* definition cited: *Small v. University Medical Center of Southern Nevada*, 2014 WL 4079507, at *21 (D. Nev. Aug. 18, 2014).

Intrusion Detection System (IDS): A platform, device, or software designed to monitor systems and detect unauthorized or malicious activity.

Intrusion Prevention System (IPS): A platform, device, or software designed to monitor systems and prevent malicious or other unauthorized activity.

IoT: See Internet of Things.

IP: See Internet Protocol.

IPC: See Image Processing Card.

IPS: See Intrusion Prevention System.

IR: See Incident Response.

IRC: See Internet Relay Chat.

IS: See Information Systems.

ISDN: See Integrated Services Digital Network.

ISO: See International Organization for Standardization.

ISO 8859-1: Also called Latin-1. A standard character encoding of the Latin alphabet used for most Western European languages. ISO 8859-1 is considered a legacy encoding in relation to Unicode, yet it is still in common use today. The ISO 8859-1 standard consists of 191 printable characters from the Latin script. It is essentially a superset of the ASCII character encoding and a subset of the Windows-1252 character encoding. See ASCII; Windows-1252.

ISO 9660 CD Format: The ISO format for creating CD-ROMs that can be read worldwide.

ISO 15489-1: The ISO standard addressing international best practices in records management.

ISO 27000: An ISO standard that describes the use and parameters of an Information Security Management System.

ISO 27001: AN ISO standard that formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which an organization identifies, analyzes, and addresses its information risks.

ISO 27050: An ISO standard to promote methods and processes for forensic capture and investigation of digital evidence/electronically stored information for eDiscovery.

ISP: See Internet Service Provider.

IT: See Information Technology.

ITU: See International Telecommunication Union.

Jailbreak: A process of bypassing security restrictions of an operating system to take full control of a device.

Janitor Program: A category of software designed to automate data organization or disposition tasks. See Auto-Delete.

Java: A platform-independent programming language for adding animation and other actions to websites.

Joint Photographic Experts Group (JPEG): A compression algorithm for still images that is commonly used on the web.

Journal: A chronological record of data processing operations that may be used to reconstruct a previous or an updated version of a file. In database management systems, it is the record of all stored data items that have values changed as a result of processing and manipulation of the data.

Journaling: A function of electronic communication systems (such as Microsoft Exchange and Lotus Notes) that copies items that are sent and received into a second information store for retention or preservation. Because journaling takes place at the information store (server) level when the items are sent or received, rather than at the mailbox (client) level, some message-related metadata, such as user foldering (what folder the item is stored in within the recipient's mailbox) and the status of the "read" flag, is not retained in the journaled copy. The journaling function stores items in the system's native format, unlike email archiving solutions, which use proprietary storage formats designed to reduce the amount of storage space required. Journaling systems may also lack the sophisticated search and retrieval capabilities available with many email archiving solutions. See Email Archiving.

JPEG: See Joint Photographic Experts Group.

Judgmental Sampling: The human selection of a subset of documents from a larger population based on some logical criteria, such as search-term hits or the searcher's own experience and knowledge.

Jukebox: A mass storage device that holds optical disks and automatically loads them into a drive.

Jump Drive: See Flash Drive.

KB: See Kilobyte.

Kerning: Adjusting the spacing between two letters.

Key Drive: See Flash Drive.

Key Field: See Primary Key.

Keyword: Any specified word, or combination of words, used in a search, with the intent of locating certain results.

Kilobyte (KB): A unit of 1,024 bytes. See Byte.

Kofax Board: The generic term for a series of image processing boards manufactured by Kofax Imaging Processing. These are used between the scanner and the computer and perform real-time image compression and decompression for faster image viewing, image enhancement, and corrections to the input to account for conditions such as document misalignment.

LAN: See Local Area Network.

Landscape Mode: A page orientation or display such that the width exceeds the height (horizontal).

Language Identification or Detection: A form of textual analytics that identifies the languages present in each record.

Laser Disk: Same as an optical CD, except 12 inches in diameter.

Laser Printing: A printing process by which a beam of light hits an electrically charged drum and causes a discharge at that point. Toner is then applied, which sticks to the non-charged

areas. Paper is pressed against the drum to form the image and is then heated to dry the toner.

Latency: The time it takes to read a disk (or jukebox), including the time to physically position the media under the read/write head, seek the correct address, and transfer it.

Latent Data: Deleted files and other electronically stored information that are inaccessible without specialized forensic tools and techniques. Until overwritten, these data reside on media such as a hard drive in unused space and other areas available for data storage. Also known as ambient data. See Residual Data.

Latent Semantic Indexing and Analysis: A method of processing data that identifies relationships between data sets by analyzing terms and term frequency. Common applications include grouping documents together based on the documents' concepts and meanings instead of by simple searching.

Latin-1: See ISO 8859-1.

LCD: See Liquid Crystal Display.

Leading: The amount of space between lines of printed text.

Least Privilege: A security principle requiring each entity to have only the most restrictive access to a system or network to perform its authorized work.

Legacy Data, Legacy System: Electronically stored information that can only be accessed via software and/or hardware that has become obsolete or replaced. Legacy data may be costly to restore or reconstruct when required for investigation or litigation analysis or discovery.

Legal Hold: A communication issued as a result of current or reasonably anticipated litigation, audit, government investigation, or other such matter that suspends the normal disposition or processing of records. Legal holds may encompass

procedures affecting data that is accessible as well as data that is not reasonably accessible. The specific communication to business or IT organizations may also be called a hold, preservation order, suspension order, freeze notice, hold order, litigation hold, or hold notice. See The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019), *available at* https://thesedonaconference. org/publication/Commentary_on_Legal_Holds.

Lempel-Ziv & Welch (LZW): A common, lossless compression standard for computer graphics, used for most TIFF files. Typical compression ratios are 4/1.

Level Coding: Used in bibliographical coding to facilitate different treatment, such as prioritization or more thorough extraction of data, for different categories of documents, such as by type or source. See Coding.

LFP: IPRO Tech Inc.'s image cross reference file; an ASCII delimited text file that cross references an image's Bates number to its location and file name. See Bates Number.

Lifecycle: A record's lifecycle is the life span of a record from its creation or receipt to its final disposition. Usually described in three stages: (1) creation, (2) maintenance and use, and (3) archive to final disposition. See Information Lifecycle Management.

Linear and Nonlinear Review: Performed by humans. Linear review workflow begins at the beginning of a collection and addresses information in order until a full review of all information is complete. Nonlinear review workflow is to prepare only certain portions for review, based either on the results of criteria, such as search terms, technology-assisted review results, or some other method, to isolate only information likely to be responsive. See Review.

Linear Tape-Open (LTO): A type of magnetic backup tape that can hold as much as 800 GB of data, or 1200 CDs, depending on the data file format.

Link: See Hyperlink.

Liquid Crystal Display (LCD): Two polarizing transparent panels with a liquid crystal surface between them; the application of voltage to certain areas causes the crystal to turn dark, and a light source behind the panel transmits though crystals not darkened.

Litigation Hold: See Legal Hold.

Load File: A file that relates to a set of scanned images or electronically processed files, and that indicates where individual pages or files belong together as documents, to include attachments, and where each document begins and ends. A load file may also contain data relevant to the individual documents, such as selected metadata, coded data, and extracted text. Load files should be obtained and provided in prearranged or standardized formats to ensure transfer of accurate and usable images and data.

> *Glossary* definition cited: *Aguilar v. Immigration and Customs Enforcement Division of the U.S. Dept. of Homeland Security*, 255 F.R.D. 350, 353 (S.D.N.Y. 2008). *National Day Laborer Organization Network v. U.S. Immigration & Customs Enforcement Agency*, 2011 U.S. Dist. LEXIS 11655 (S.D.N.Y. February 7, 2011). *CBT Flint Partners, LLC v. Return Path, Inc.,* 737 F.3d 1320, 1332 (Fed. Cir. Dec. 13, 2013). *EEOC v. SVT, LLC,* 2014 WL 1411775, at *3 (N.D. Ind. Apr. 10, 2014).

Local Area Network (LAN): A group of computers at a single location (usually an office or home) that are connected by phone lines, coaxial cable, or wireless transmission. See Network.

Location Services: A term used to describe a program or applications function of using the global positioning services (GPS) on a device to ascertain the location of a user at a given time.

Log File: A text file created by an electronic device or application to record activity of a server, website, computer, or software program.

Logical Entities: An abstraction of a real-world object or concept that is both independent and unique. Conceptually, a logical entity is a noun, and its relationships to other entities are verbs. In a relational database, a logical entity is represented as a table. Attributes of the entity are in columns of the table, and instances of the entity are in rows of the table. Examples of logical entities are employees of a company, products in a store's catalog, and patients' medical histories.

Logical File Space: The actual amount of space occupied by a file on a hard drive. The amount of logical file space differs from the physical file space because when a file is created on a computer, a sufficient number of clusters (physical file space) are assigned to contain the file. If the file (logical file space) is not large enough to completely fill the assigned clusters (physical file space), then some unused space will exist within the physical file space.

Logical Unitization: See Unitization—Physical and Logical.

Logical Volume: An area on the hard drive that has been formatted for file storage. A hard drive may contain single or multiple volumes.

Loose File: A file that is not attached to or embedded in another file or email.

Lossless Compression: A method of compressing an image file, bit by bit, that results in no loss of information either during compression or extraction.

Lossy Compression: A method of image compression whereby storage size of image is reduced by decreasing the resolution and color fidelity while maintaining minimum acceptable standard for general use. A lossy image is one where the image after compression is different from the original image due to lost information. The differences may or may not be noticeable, but a lossy conversion process does not retain all the original information. JPEG is an example of a lossy compression method.

Lotus Domino: An IBM server product providing enterprise-level email, collaboration capabilities, and custom application platform; it began as Lotus Notes Server, the server component of Lotus Development Corporation's client-server messaging technology. Can be used as an application server for Lotus Notes applications and/or as a web server. Has a built-in database system in the format of .nsf.

LTO: See Linear Tape-Open.

LZW: See Lempel-Ziv & Welch.

Machine Learning: A subset of artificial intelligence enabling a system to automatically improve at a task on its own based upon experience and data, without being explicitly programmed for that task. See Artificial Intelligence.

Magnetic/Optical Storage Media: The physical piece of material that receives data that has been recorded using a number of different magnetic recording processes. Examples include hard drives, backup tapes, CD-ROMs, DVD-ROMs, Jaz, and Zip drives.

Magneto-Optical Drive: A drive that combines laser and magnetic technology to create high-capacity erasable storage.

Mail Application Programming Interface (MAPI): A Windows-based software standard that enables a program to send

and receive email by connecting the program to selected email servers. See API.

Mailbox: A term used to describe all email associated with an individual email account, whether located physically together on one server, across a server array, or in cloud-based storage.

Make-Available Production: Process by which a generally large universe of potentially responsive documents is made available to a requestor; the requestor selects or tags desired documents, and the producing party produces only the selected documents. See Quick Peek.

Malware: Any type of malicious software program, typically installed illicitly, including viruses, Trojans, worms, key loggers, spyware, adware, and others.

Managed Services: A business relationship whereby a company signs a contract with a service provider for the provision of specific services at a set price for a period of time.

Management Information Systems (MIS): A phrase used to describe the resources, people, and technology used to manage the information of an organization.

Manual Review: See Linear and Nonlinear Review.

MAPI: See Mail Application Programming Interface.

MAPI Mail Near-Line: Documents stored on optical disks or compact disks that are housed in a jukebox or CD changer and can be retrieved without human intervention.

Margin of Error (MOE): The percentage points that the results of a sample may vary from the actual number in the real population. For example, if the actual recall of responsive documents is 75 percent, then sampling responsive documents to a 95 percent confidence with a 5 percent margin of error means there is a 95 percent chance the sample will show between 70 (75 minus 5) and 80 (75 plus 5) percent. See Confidence Level.

Marginalia: Handwritten notes on documents.

Master Boot Sector/Record: The sector on a hard drive that contains the computer code (boot strap loader) necessary for the computer to start up and the partition table describing the organization of the hard drive.

Master File Table (MFT): The primary record of file storage locations on a Microsoft Windows-based computer employing NTFS filing systems.

> *Glossary* definition cited: *Digital Assurance Certification, LLC v. Pendolino*, 2017 WL 4342316, at *3 (M.D. Fla. Sept. 29, 2017).

Mastering: Making many copies of a disk from a single master disk.

MB: See Megabyte.

MBOX: The format in which email is stored on traditional UNIX email systems.

MD5: See Message-Digest Algorithm 5.

Media: An object or device, such as a disk, tape, or other device, on which data is stored.

Megabyte (MB): 1,024 kilobytes. See Byte.

Meme: A popular-culture term used to refer to a graphic, audio file, video file, or text that is used to parody something else, which is then often parodied itself with slight variations.

Memory: Data storage in the form of chips, or the actual chips used to hold data; storage is used to describe memory that exists on tapes, disks, CDs, DVDs, flash drives, and hard drives. See Random Access Memory (RAM); Read-Only Memory (ROM).

Menu: A list of options, each of which performs a desired action such as choosing a command or applying a particular format to a part of a document.

Message-Digest Algorithm 5 (MD5): A hash algorithm used to give a numeric value to a digital file or piece of data. Commonly used in eDiscovery to find duplicates in a data collection. See Hash Coding.

Message Header: The text portion of an email that contains routing information of the email and may include author, recipient, and server information, which tracks the path of the email from its origin server to its destination mailbox.

Message Unit: An email and any attachments associated with it.

Metadata: The generic term used to describe the structural information of a file that contains data about the file, as opposed to describing the content of a file. See System-Generated Metadata and User-Created Metadata. For a more thorough discussion, see The Sedona Conference, *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, Second Edition* (November 2007), *available at* https://thesedonaconference.org/publication/Guidelines_for_Managing_Information_and_Electronic_Records, and The Sedona Conference, *Commentary on Ethics & Metadata*, 14 SEDONA CONF. J. 169, *available at* https://thesedonaconference.org/publication/Commentary_on_Ethics_and_Metadata.

> *Glossary* definition cited: *Race Tires America, Inc. v. Hoosier Racing Tire Corp.*, 674 F.3d 158, 161 (3d Cir. 2012). *EEOC v. BOK Financial Corp.*, 2013 WL 12330078, at *1 (D.N.M. May 7, 2013). *CBT Flint Partners, LLC v. Return Path, Inc.*, 737 F.3d 1320, 1328 (Fed. Cir. Dec. 13, 2013). *Selectica, Inc. v. Novatus, Inc.*, 2015 WL 1125051, at *3 (M.D. Fla. Mar. 12, 2015). *United States v. Life Care Centers Of America, Inc.*,

2015 WL 10987073, at *10 (E.D. Tenn. Aug. 31, 2015). *United States v. Brown*, 843 F.3d 74, 76 (2d Cir. 2016). *Javeler Marine Services LLC v. Cross,* 175 F. Supp. 3d 756, 762 (S.D. Tex. 2016). *Morgan Hill Concerned Parents Ass'n v. California Dept. of Education*, 2017 WL 445722 at *2 (E.D. Cal. Feb. 2, 2017).

Metadata Comparison: A comparison of specified metadata as the basis for de-duplication without regard to content. See De-Duplication.

MFT: See Master File Table.

Microfiche: Sheet microfilm (4 inches by 6 inches) containing reduced images of 270 pages or more in a grid pattern.

Microprocessor: See Central Processing Unit (CPU).

Microsoft-Disk Operating System (MS-DOS): Used in Windows-based personal computers as the control system prior to the introduction of 32-bit operating systems.

Microsoft Outlook: A personal information manager from Microsoft, part of the Microsoft Office suite. Although often used mainly as an email application, it also provides calendar, task, and contact management; note taking; a journal; and web browsing. Can be used as a stand-alone application or operate in conjunction with Microsoft Exchange Server to provide enhanced functions for multiple users in an organization, such as shared mailboxes and calendars, public folders, and meeting-time allocation.

MiFi: A portable wireless hub that allows users with the correct credentials to access the internet.

Migrated Data: Electronically stored information that has been moved from one database or format to another.

Migration: Moving electronically stored information from one computer application or platform to another; may require conversion to a different format.

Mirror Image: A bit-by-bit copy of any storage media. Often used to copy the configuration of one computer to anther computer or when creating a preservation copy. See Forensic Copy and Image.

> *Glossary* definition cited: *White v. Graceland College Center for Professional Development & Lifelong Learning, Inc.*, 2009 WL 722056 at *6 (D. Kan. March 18, 2009). *Crosmun v. Fayetteville Technical Community College*, 832 S.E.2d 223, 229 (N.C. Ct. App. 2019).

Mirroring: The duplication of electronically stored information for purposes of backup or to distribute internet or network traffic among several servers with identical ESI. See Bit Stream Backup, Disk Mirroring, Image.

MIS: See Management Information Systems.

MMS: See Multimedia Messaging Service.

Modem (Modulator-Demodulator): A device that can encode digital information into an analog signal (modulates) or decode the received analog signal to extract the digital information (demodulate).

MOE: See Margin of Error.

Mount or Mounting: The process of making off-line electronically stored information available for online processing. For example, placing a magnetic tape in a drive and setting up the software to recognize or read that tape. The terms load and loading are often used in conjunction with, or synonymously with, mount and mounting (as in "mount and load a tape"). Load may also refer to the process of transferring ESI from mounted media to another media or to an online system.

MPEG-1, -2, -3 and -4: Different standards for full motion video to digital compression/decompression techniques advanced by the Moving Pictures Experts Group.

MS-DOS: See Microsoft-Disk Operating System.

MSG: A common file format in which emails can be saved, often associated with a Microsoft Outlook email program, which preserves both the format and any associated attachment information.

Multimedia: The combined use of different media; integrated video, audio, text, and data graphics in digital form.

Multimedia Messaging Service (MMS): A protocol of messaging that allows for the transmission of multimedia content such as pictures, video, or sound over mobile networks. See Text Message.

National Institute of Standards and Technology (NIST): A federal technology agency that works with industry to develop and apply technology measurements and standards. See NIST List.

Native Format: Electronic documents have an associated file structure defined by the original creating application. This file structure is referred to as the native format of the document. Because viewing or searching documents in the native format may require the original application (for example, viewing a Microsoft Word document may require the Microsoft Word application), documents may be converted to a neutral format as part of the record acquisition or archive process. Static format (often called imaged format), such as TIFF or PDF, is designed to retain an image of the document as it would look viewed in the original creating application but does not allow metadata to be viewed or the document information to be manipulated unless agreed-upon metadata and extracted text are preserved. In the conversion to static format, some metadata can be processed,

preserved, and electronically associated with the static format file. However, with technology advancements, tools and applications are increasingly available to allow viewing and searching of documents in their native format while still preserving pertinent metadata. It should be noted that not all electronically stored information may be conducive to production in either the native format or static format, and some other form of production may be necessary. Databases, for example, often present such issues. See Form of Production; Load File.

> *Glossary* definition cited: *Covad Communications Co. v. Revonet, Inc.*, 254 F.R.D. 147, 148 (D.D.C. 2008). *Race Tires America, Inc. v. Hoosier Racing Tire Corp.*, 674 F.3d 158, 161 (3d Cir. 2012). *Palar v. Blackhawk Bancorporation Inc.*, 2013 WL 1704302, at *1 (C.D. Ill. Mar. 19, 2013). *EEOC v. BOK Financial Corp.*, 2013 WL 12330078 at *1 (D.N.M. May 7, 2013). *Akanthos Capital Mgmt., LLC v. CompuCredit Holdings Corp.*, 2 F. Supp. 3d 1306, 1315 (N.D. Ga. 2014). *Life Plans, Inc. vs. Security Life of Denver Insurance Co.*, 52 F. Supp. 3d 893, 903 (N.D. Ill. 2014). *Morgan Hill Concerned Parents Ass'n v. California Dept. of Education*, 2017 WL 445722 at *1 (E.D. Cal. Feb. 2, 2017). *Carter v. Franklin Fire District*, 2019 WL 1224623 at 2* (N.J. Super. Ct. App. Div. Mar. 15, 2019).

Native Format Review: Review of electronically stored information in its native format using either a third-party viewer application capable of rendering native files in close approximation to their original application or the actual original application in which the ESI was created. See Review.

Natural Language Search: A manner of searching that permits the use of plain language without special connectors or precise terminology, such as "Where can I find information on William Shakespeare?" as opposed to formulating a search statement,

such as "information" and "William Shakespeare." See Boolean Search.

Near Duplicates: (1) Two or more files that are similar to a certain percentage, for example, files that are 90 percent similar may be identified as near duplicates; used for review to locate similar documents and review all near duplicates at one time; (2) The longest email in an email conversation where the subparts are identified and suppressed in an email collection to reduce review volume.

Near-Line Data Storage: A term used to refer to a data storage system where data is not actively available to users, but is available through an automated system that enables the robotic retrieval of removable storage media or tapes. Data in near-line storage is often stored on servers that do not have as high performance as active servers. Making near-line data available will not require human intervention (as opposed to off-line data, which can only be made available through human actions).

Network: A group of two or more computers and other devices connected together ("networked") for the exchange and sharing of resources. See Local-Area Network (LAN) and Wide-Area Network (WAN).

Network Operating System (NOS): See Operating System.

Network Operations Center (NOC): The location where a network or computer array is monitored and maintained.

Network Segmentation: A security principle of splitting a network into smaller segments separated by devices as a method of improving security by limiting access to those segments.

Neural Network: Neural networks are made up of interconnected elements called neurons, which respond in parallel to a set of input signals given to each.

New Technology File System (NTFS): A high-performance and self-healing file system proprietary to Microsoft, used in Windows NT, Windows 2000, Windows XP, and Windows Vista Operating Systems, that supports file-level security, compression, and auditing. It also supports large volumes and powerful storage solutions such as Redundant Array of Inexpensive Disks (RAID). An important feature of NTFS is the ability to encrypt files and folders to protect sensitive data. See Redundant Array of Inexpensive Disks (RAID).

NIST: See National Institute of Standards and Technology.

NIST List: A hash database of computer files developed by the National Institute of Standards and Technology (NIST) to identify files that are system generated and generally accepted to have no substantive value in most instances. See De-NIST.

NOC: See Network Operations Center.

Node: Any device connected to a network. PCs, servers, and printers are all nodes on the network.

Noise Words: See Stop Words.

Noninclusive Emails: Emails that are subparts of larger emails chains and therefor redundant with regard to information that can be found in the larger email chain.

Noninterlace: When each line of a video image is scanned separately. Older cathode-ray tube (CRT) computer monitors use noninterlaced video.

Normalization: The process of reformatting data so that it is stored in a standardized form, such as setting the date and time stamp of a specific volume of electronically stored information to a specific zone, often GMT, to permit advanced processing of the ESI, such as de-duplication. See Coordinated Universal Time.

NOS: See Network Operating System.

NoSQL Database: A NoSQL database is a type of database management system using a form of unstructured storage that is optimized for handling big data. Unlike relational databases, NoSQL databases do not have a fixed table structure, allowing data to be distributed across many "nodes." Additional nodes can readily be created as data volume grows. Some examples of NoSQL databases include Cassandra, Redis, Elasticsearch, MongoDB, and Hadoop. See Big Data; Database.

Notes Server: See Lotus Domino.

NSF: A Lotus Notes container file (i.e., database.nsf); can be either an email database or the traditional type of fielded database. See Lotus Domino.

NTFS: See New Technology File System.

Null Set: A set of files that are not positive results of a search.

Null Set Testing: Sampling a null set to search for false negatives of the search that created the null set.

Object: In personal computing, an object is a representation of something that a user can work with to perform a task and can appear as text or an icon. In a high-level method of programming called object-oriented programming (OOP), an object is a freestanding block of code that defines the properties of something.

Object Linking and Embedding (OLE): A feature in Microsoft Windows that allows the linking of different files, or parts of files, together into one file without forfeiting any of the original file's attributes or functionality. See Compound Document.

Objective Coding: See Coding.

OCR: See Optical Character Recognition.

Official Record Owner: See Record Owner.

Off-line Data: Electronically stored information that is stored outside the network in daily use (e.g., on backup tapes) and is only accessible through the off-line storage system, not the network.

Off-line Storage: Electronically stored information stored on removable disk (optical, compact, etc.) or magnetic tape and not accessible by the active software or server. Often used for making disaster-recovery copies of records for which retrieval is unlikely. Accessibility to off-line media usually requires restoring the data back to the active server.

OLE: See Object Linking and Embedding.

Online: Connected to a network or the internet.

Online Review: The review of data on a computer, either locally on a network or via the internet. See Review.

Online Storage: The storage of electronically stored information as fully accessible information in daily use on the network or elsewhere.

Ontology: A collection of categories and their relationships to other categories and to words. An ontology is one of the methods used to find related documents when given a specific query.

Open Source: Refers to software that is distributed with access to the software's source code, so that it can be freely modified by users.

Operating System (OS): The operating system provides the software platform that directs the overall activity of a computer, network, or system and on which all other software programs and applications run. In many ways, choice of an operating system will affect which applications can be run. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral

devices such as disk drives and printers. For large systems, the operating system has even greater responsibilities and powers—becoming a traffic cop to make sure different programs and users running at the same time do not interfere with each other. The operating system is also responsible for security, ensuring that unauthorized users do not access the system. Examples of computer operating systems are UNIX, DOS, Microsoft Windows, LINUX, Mac OS, and IBM z/OS. Examples of portable device operating systems are iOS, Android, Microsoft Windows, and BlackBerry. Operating systems can be classified in a number of ways, including: multi-user (allows two or more users to run programs at the same time; some operating systems permit hundreds or even thousands of concurrent users); multiprocessing (supports running a program on more than one CPU); multitasking (allows more than one program to run concurrently); multithreading (allows different parts of a single program to run concurrently); and real time (instantly responds to input; general-purpose operating systems, such as DOS and UNIX, are not real time).

OPT File: A file format that associates a Bates number to the path of an image file and is used to load images to a document review database. See Bates Number.

Optical Character Recognition (OCR): A technology process that captures text from an image for the purpose of creating a parallel text file that can be associated with the image and searched in a database. OCR software evaluates scanned data for shapes it recognizes as letters or numerals. See Handwriting Recognition Software (HRS); Intelligent Character Recognition (ICR).

> *Glossary* definition cited: *Race Tires America, Inc. v. Hoosier Racing Tire Corp.*, 674 F.3d 158, 161 (3d Cir. 2012). *Hinterberger v. Catholic Health System, Inc.*, 2013 WL 2250591 at *9 (W.D.N.Y. May 21, 2013). *Gordon v. Kaleida Health*, 2013

WL 2250506 at *1 (W.D.N.Y. May 21, 2103). *Country Vintner of North Carolina, LLC v. E. & J. Gallo Winery, Inc.*, 718 F.3d 249, 252 (4th Cir. 2013). *Life Plans, Inc. vs. Security Life of Denver Insurance Co.*, 52 F. Supp. 3d 893, 903 (N.D. Ill. 2014). *Balance Point Divorce Funding, LLC v. Scrantom*, 305 F.R.D. 67, 74 (S.D.N.Y. 2015).

Optical Disks: Computer media similar to a compact disk that cannot be rewritten. An optical drive uses a laser to read the electronically stored information.

Originator: See Author.

OS: See Operating System.

OST: A Microsoft Outlook information store used to save folder information that can be accessed off-line.

Glossary definition cited: *White v. Graceland College Center for Professional Development & Lifelong Learning, Inc.*, 2009 WL 722056 at *5 (D. Kan. March 18, 2009).

Outlook: See Microsoft Outlook.

Overinclusive: When referring to data sets returned by some method of query, search, filter, or cull, results that are overly broad.

Overlay File: A type of text-delimited load file used to add, modify, or remove information from existing records in a database.

Overwrite: To record or copy new data over existing data, as in when a file or directory is updated.

PaaS: See Platform as a Service.

PAB: See Personal Address Book.

Packet: A unit of data sent across a network that may contain identity and routing information. When a large block of data is

to be sent over a network, it is broken up into several packets, sent, and then reassembled at the other end. The exact layout of an individual packet is determined by the protocol being used.

Page File/Paging File: Also referred to as a swap file, a method to temporarily store data outside of the main memory but quickly retrievable. This data is left in the swap file after the programs are terminated and may be retrieved using forensic techniques. See Swap File.

Parallel Port: See Port.

Parent: See Document.

Parsing: In eDiscovery, the process by which a file is broken apart into its individual components for indexing, processing, or to prepare for loading into a review database.

Partition: An individual section of computer storage media such as a hard drive. For example, a single hard drive may be divided into several partitions in order that each partition can be managed separately for security or maintenance purposes. When a hard drive is divided into partitions, each partition is designated by a separate drive letter, i.e., C, D, etc.

Partition Table: Indicates each logical volume contained on a disk and its location.

Partition Waste Space: After the boot sector of each volume or partition is written to a track, it is customary for the system to skip from the rest of that track to the actual useable area of the volume on the next track. This results in unused or wasted space on the initial track where information can be hidden. This wasted space can only be viewed with a low-level disk viewer. However, forensic techniques can be used to search these wasted space areas for hidden information.

Passive Learning. A technology-assisted review workflow in which documents are randomly selected for training by human review. See also Active Learning.

Password: A text or alphanumeric string that is used to authenticate a specific user's access to a secure program, network, or part of a network.

Patching: The practice of updating software (or firmware) to a more recent version that updates, fixes, or improves the software, often to repair security vulnerabilities.

Path: (1) The hierarchical description of where a directory, folder, or file is located on a computer or network; (2) A transmission channel, the path between two nodes of a network that a data communication follows, and the physical cabling that connects the nodes on a network.

Pattern Matching: A generic term that describes any process that compares one file's content with another file's content.

Pattern Recognition: Technology that searches electronically stored information for like patterns and flags and extracts the pertinent data, usually utilizing an algorithm. For instance, in looking for addresses, alpha characters followed by a comma and a space, followed by two capital alpha characters, followed by a space, followed by five or more digits, are usually the city, state, and zip code. By programming the application to look for a pattern, the information can be electronically identified, extracted, or otherwise utilized or manipulated.

PB: See Petabyte.

PC: See Personal Computer.

PC Card: Plug-in cards for computers (usually portables) that extend the storage and/or functionality. Originally introduced as the PCMCIA, the PC Card standard was developed by the Personal Computer Memory Card International Association.

PDA: See Personal Digital Assistant.

PDF: See Portable Document Format.

PDF/A: An electronic document file format for long-term archival preservation. ISO 19005 defined the file format PDF/A, which preserves electronic documents visual appearance over time, independent of the tools and systems used for creating, storing, or rendering the files.

Peer-to-Peer or P2P: A form of network organization that uses portions of each user's resources, like storage space or processing power, for use by others on the network. Notorious examples include the storage sharing of Napster or BitTorrent.

Penetration Test: Testing that attempts to find security weaknesses and vulnerabilities in a network or system so that they can be remedied before they are used and located by a malicious party. Often referred to as "Pen Test."

Peripheral: Any accessory device attached to a computer, such as a disk drive, printer, modem, or joystick.

Peripheral Component Interconnect or Interface (PCI): A high-speed interconnect local bus used to support multimedia devices.

Personal Address Book (PAB): A file type to describe a Microsoft Outlook list of contacts created and maintained by an individual user for personal use.

Personal Computer (PC): A computer based on a microprocessor and designed to be used by one person at a time.

Personal Data (as used in the GDRP): Any information relating to a natural person who can be identified from the data, directly or indirectly, in particular by reference to an identification number, location data, online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental,

economic, cultural or social identity. Also referred to as PII (Personally Identifiable Information).

Personal Digital Assistant (PDA): A portable device used to perform communication and organizational tasks.

Personal Filing Cabinet (PFC): The AOL proprietary email storage container file used for the local storage of emails, contacts, calendar events, and other personal information.

Personally Identifiable Information (PII): Information, such as social security number, physical characteristics, address, or date of birth, from which an individual's identity can be determined.

Petabyte (PB): 1,024 terabytes (approximately one million gigabytes). See Byte.

PFC: See Personal Filing Cabinet.

PHI: See Protected Health Information.

Phishing: The practice of sending email messages to targeted users in an effort to extract private information, often security related, such as passwords, to assist in circumventing network security.

Physical Disk: An actual piece of computer media, such as the hard disk or drive, floppy disks, CD-ROM disks, zip drive, etc.

Physical File Storage: When a file is created on a computer, a sufficient number of clusters are assigned to contain the file. If the file is not large enough to completely fill the assigned clusters, then some unused space will exist within the physical file space. This is referred to as file slack and can contain unused space, previously deleted/overwritten files, or fragments thereof. See Slack Space.

Physical Unitization: See Unitization—Physical and Logical.

Picture Element: The smallest addressable unit on a display screen. The higher the resolution (the more rows and columns), the more information that can be displayed.

PII: See Personally Identifiable Information.

Ping: Executable command, used as a test for checking network connectivity.

Pitch: Characters (or dots) per inch, measured horizontally.

Pixel: A single unit of a raster image that allows a picture to be displayed on an electronic screen or computer monitor.

PKI: See Public Key Infrastructure Digital Signature.

Plaintext or Plain Text: The least formatted and therefore most portable form of text for computerized documents.

Plasma Display: A type of flat-panel display commonly used for large televisions in which many tiny cells are located between two panels of glass holding an inert mixture of gases, which are then electronically charged to produce light.

Platform as a Service (PaaS): A form of cloud computing that describes the outsourcing of the computer platform upon which development and other workflows can be performed without the costs of hardware, software, and personnel. See Cloud Computing.

Platter: One of several components that make up a computer hard drive. Platters are thin, rapidly rotating disks that have a set of read/write heads on both sides. Each platter is divided into a series of concentric rings called tracks. Each track is further divided into sections called sectors, and each sector is subdivided into bytes.

Plug and Play (PNP): A method by which new hardware may be detected, configured, and used by existing systems upon connection with little or no user intervention.

Plug-In: An application developed to be used as an add-on to another program and cannot usually be used without the program it was designed to augment.

PNP: See Plug and Play.

POD: See Print On Demand.

Point Estimate: The result of a sample that estimates prevalence in the specific population being sampled.

Pointer: An index entry in the directory of a disk (or other storage medium) that identifies the space on the disk in which an electronic document or piece of electronic data resides, thereby preventing that space from being overwritten by other data. In most cases, when an electronic document is deleted, the pointer is deleted, allowing the document to be overwritten, but the document is not actually erased until overwritten.

Port: An interface between a computer and other computers or devices. Ports can be divided into two primary groups based on signal transfer. Serial ports send and receive one bit at a time via a single pair of wires, while parallel ports send multiple bits at the same time over several sets of wires. See Universal Serial Bus (USB) Port. Software ports are virtual data connections used by programs to exchange data directly instead of going through a file or other temporary storage locations; the most common types are Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol (UDP).

Portable Document Format (PDF): A file format technology developed by Adobe Systems to facilitate the exchange of documents between platforms regardless of originating application by preserving the format and content.

> *Glossary* definition cited: *EEOC v. BOK Financial Corp.*, 2013 WL 12330078 at *1 (D.N.M. May 7, 2013). *Country Vintner of North Carolina, LLC v. E. & J. Gallo Winery, Inc.*,

718 F.3d 249, 253 (4th Cir. 2013). *Saliga v. Chemtura Corp.*, 2013 WL 6182227, at *2 (D. Conn. Nov. 25, 2013). *Balance Point Divorce Funding, LLC v. Scrantom*, 305 F.R.D. 67, 74 (S.D.N.Y. 2015). *Carter v. Franklin Fire District*, 2019 WL 1224623 at 2* (N.J. Super. Ct. App. Div. Mar. 15, 2019).

Portable Volumes: A feature that facilitates the moving of large volumes of documents without requiring copying multiple files. Portable volumes enable individual CDs to be easily regrouped, detached, and reattached to different databases for a broader information exchange.

Portrait Mode: A page orientation or display such that the height exceeds the width (vertical).

Precision: When describing search results, precision is the number of true positives retrieved from a search divided by the total number of results returned. For example, in a search for documents relevant to a document request, it is the percentage of documents returned that are actually relevant to the request. See The Sedona Conference, *Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 15 SEDONA CONF. J. 217 (2014), *available at* https://thesedonaconference.org/publication/Commentary_on_Search_and_Retrieval_Methods.

Predictive Coding/Ranking: See Technology-Assisted Review.

Preservation: The process of retaining documents and electronically stored information, including document metadata, for legal purposes and includes suspension of normal document destruction policies and procedures. See Spoliation.

Preservation Notice, Preservation Order: See Legal Hold.

Prevalence: The percent of a population that has a specific characteristic, such as responsiveness.

Primary Key: A unique value stored in a field or fields of a database record that is used to identify the record and, in a relational database, to link multiple tables together.

Print On Demand (POD): A term referring to document images stored in electronic format and available to be quickly printed.

Printout: Printed data, also known as hard copy.

Private Key Encryption: A method of securing data whereby data is made unreadable using an algorithm and can only be unscrambled using a key that is held only by the originator and those he or she chooses to share it with.

Private Network: A network that is connected to the internet but is isolated from the internet with security measures, allowing use of the network only by persons within the private network.

Privilege Data Set: The universe of documents identified as responsive and/or relevant but withheld from production on the grounds of legal privilege, a log of which is usually required to notify of withheld documents and the grounds on which they were withheld (e.g., work product, attorney-client privilege).

Process/processing (as used in the GDRP): Any controller delegated operation or set of operations at the instruction of and on behalf of the controller which is performed on personal data, or on sets of personal data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processing Data: The automated ingestion of electronically stored information into a program for the purpose of extracting metadata and text; and in some cases, the creation of a static image of the source ESI files according to a predetermined set of

specifications, in anticipation of loading to a database. Specifications can include the de-duplication of ESI, or filtering based on metadata contents such as date or email domain and specific metadata fields to be included in the final product.

> *Glossary* definition cited: *Balance Point Divorce Funding, LLC v. Scrantom*, 305 F.R.D. 67, 74 (S.D.N.Y. 2015).

Processing Exception: Files that a given processing software is not able to access in order to extract metadata and text or to convert to a static form. Processing exceptions may occur due to file corruption, password protection, or a file format that the processing software does not recognize.

Processor (as used in the GDPR): A natural or legal person, public authority, agency or other body which processes personal data on behalf and at the direction of the controller. The person is a separate legal entity with respect to the controller, and the person processes personal data on behalf of the controller. Processors have direct obligations with regard to "the how": security, record keeping, notifying controllers of data breach, and ensuring compliance of restrictions on data transfers. Obligations relating to "purpose" are only imposed on the controller. See Controller.

Production: The process of delivering to another party, or making available for that party's review, documents and/or electronically stored information deemed responsive to a discovery request.

Production Data Set: The universe of documents and/or electronically stored information identified as responsive to document requests and not withheld on the grounds of privilege.

Production Number: See Bates Number and Beginning Document Number.

Program: See Application and Software.

Properties: File-level metadata describing attributes of the physical file, i.e., size, creation date, and author. See Metadata.

Protected Health Information (PHI): Information concerning personal mental or physical health protected under U.S. and/or foreign laws.

Protocol: A common series of rules, signals, and conventions that allow different kinds of computers and applications to communicate over a network. One of the most common protocols for networks is called Transmission Control Protocol/Internet Protocol (TCP/IP).

Protodigital: Primitive or first-generation digital. Applied as an adjective to systems, software, documents, or ways of thinking. The term was first used in music to refer to early computer synthesizers that attempted to mimic the sound of traditional musical instruments and to early jazz compositions written on computers with that instrumentation in mind. In eDiscovery, this term is most often applied to systems or ways of thinking that—on the surface—appear to embrace digital technology, but attempt to equate electronically stored information to paper records, ignoring the unique attributes of ESI. When someone says, "What's the big deal with eDiscovery? Sure we have a lot of email. You just print it all out and produce it like you used to," that is an example of protodigital thinking. Likewise, when someone says, "We embrace electronic discovery. We scan everything to PDF before we produce it," that person is engaged in protodigital thinking—attempting to fit electronically stored information into the paper discovery paradigm.

Proximity Search: A search syntax written to find two or more words within a specified distance from each other.

PST: A Microsoft Outlook email storage file containing archived email messages in a compressed format.

Glossary definition cited: *White v. Graceland College Center for Professional Development & Lifelong Learning, Inc.*, 2009 WL 722056 at *5 (D. Kan. March 18, 2009).

Pseudonymization (as used in the GDPR): The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Public Key Infrastructure (PKI) Digital Signature: A system, including hardware, software, and policies, designed to manage digital certificates and match those certificates to specific users so that data can be validated as authentic. See Certificate; Digital Certificate; and Digital Signature.

Public Network: A network that is part of the public internet.

Purge: A process of permanently deleting data that does not allow for recovery.

QBIC: See Query By Image Content.

QC: See Quality Control.

QIC: See Quarter Inch Cartridge.

QR: See Quick Response Code.

Quality Control (QC): Steps taken to ensure that results of a given task, product, or service are of sufficiently high quality; the operational techniques and activities that are used to fulfill requirements for quality. In document handling and management processes, this includes image quality (resolution, skew, speckle, legibility, etc.), and data quality (correct information in appropriate fields, validated data for dates, addresses, names/issues lists, etc.).

Quarter Inch Cartridge (QIC): Digital recording tape, 2000 feet long, with an uncompressed capacity of 5 GB.

Query: An electronic search request for specific information from a database or other electronically stored information.

Query By Image Content (QBIC): An IBM search system for stored images that allows the user to sketch an image and then search the image files to find those which most closely match. The user can specify color and texture—such as sandy beaches or black clouds.

Queue: A sequence of items such as packets or print jobs waiting to be processed. For example, a print queue holds files that are waiting to be printed.

Quick Peek: An initial production whereby documents and/or electronically stored information are made available for review or inspection before being reviewed for responsiveness, relevance, privilege, confidentiality, or privacy. See Make-Available Production.

Quick Response (QR) Code: A small, square matrix pattern that can be read by an optical scanner or mobile phone camera; it can store thousands of alphanumeric characters and may be affixed to business cards, advertising, product parts, or other objects in order to convey information, commonly an internet URL.

RAID: See Redundant Array of Independent Disks.

RAM: See Random Access Memory.

Random Access Memory (RAM): Hardware inside a computer that retains memory on a short-term basis and stores information while the computer is in use. It is the working memory of the computer into which the operating system, startup applications, and drivers are loaded when a computer is turned on, or where a program subsequently started up is loaded, and

where thereafter, these applications are executed. RAM can be read or written in any section with one instruction sequence. When running advanced operating systems and applications, it helps increase operating efficiency to have more of this working space installed. RAM content is erased each time a computer is turned off. See Dynamic Random Access Memory (DRAM).

Random Sampling: The process of selecting data from a population with no bias or input from the person performing the sampling, in which each item has an equal chance of being selected as any other item. See also Sampling.

Ransomware: A form of malware that seeks to encrypt data without the knowledge of the user or administrator, providing keys for decryption only upon payment of a ransom. See Malware.

RAR: A proprietary compressed archive container file.

Raster/Rasterized (Raster or Bitmap Drawing): A method of representing an image with a grid (or map) of dots. Common raster file formats are GIF, JPEG, TIFF, PCX, BMP, etc., and they typically have jagged edges.

RBAC: See Role-based Access Controls.

Read-Only Memory (ROM): Random memory that can be read but not written or changed. Also, hardware, usually a chip, within a computer containing programming necessary for starting the computer and essential system programs that neither the user nor the computer can alter or erase. Information in the computer's ROM is permanently maintained even when the computer is turned off.

Recall: When describing search results, recall is the number of documents retrieved from a search divided by all of the responsive documents in a collection. For example, in a search for documents relevant to a document request, it is the percentage of

documents returned compared against all documents that should have been returned and exist in the data set. See The Sedona Conference, *Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 15 SEDONA CONF. J. 217 (2014), *available at* https://thesedonaconference.org/publication/Commentary_on_Search_and_Retrieval_Methods.

Record: (1) Information, regardless of medium or format, that has value to an organization. (2) A single row of information or subset of data elements in a database.

Record Custodian: An individual responsible for the physical storage of records throughout their retention period. In the context of electronic records, custodianship may not be a direct part of the records management function in all organizations. For example, some organizations may place this responsibility within their information technology department, or they may assign responsibility for retaining and preserving records with individual employees. See Record Owner.

> *Glossary* definition cited: *National Jewish Health v. WebMD Health Services Group, Inc.*, 305 F.R.D. 247, 255 (D. Colo 2014).

Record Lifecycle: The time period from which a record is created until it is disposed. See Information Lifecycle Management.

Record Owner: The physical custodian or subject-matter expert on the contents of the record who is responsible for the lifecycle management of the record. This may be, but is not necessarily, the author of the record. See Record Custodian.

Record Series: A description of a particular set of records within a file plan. Each category has retention and disposition data associated with it, applied to all record folders and records within the category. See DoD 5015.

Record Submitter: The person who enters a record in an application or system. This may be, but is not necessarily, the author or the record owner.

Records Archive: See Repository for Electronic Records.

Records Hold: See Legal Hold.

Records Management: The planning, controlling, directing, organizing, training, promoting and other managerial activities involving the lifecycle of information, including creation, maintenance (use, storage, retrieval) and disposition, regardless of media. See Disposition; Information Governance; Information Lifecycle Management.

Records Manager: The person responsible for the implementation of a records management program in keeping with the policies and procedures that govern that program, including the identification, classification, handling and disposition of the organization's records throughout their retention lifecycle. The physical storage and protection of records may be a component of this individual's functions, but it may also be delegated to someone else. See Record Custodian.

Records Retention Period: The length of time a given record series should be kept, expressed as either a time period (e.g., four years), an event or action (e.g., audit), or a combination (e.g., six months after audit).

Records Retention Schedule: A plan for the management of records, listing types of records and how long they should be kept; the purpose is to provide continuing authority to dispose of or transfer records to historical archives. See Information Lifecycle Management.

Records Store: See Repository for Electronic Records.

Recover, Recovery: See Restore.

Redaction: A portion of an image or document is intentionally obscured or removed to prevent disclosure of the specific portion. Done to protect privileged or irrelevant portions, including highly confidential, sensitive, or proprietary information.

Redundant Array of Independent Disks (RAID): A method of storing data on servers that usually combines multiple hard drives into one logical unit, thereby increasing capacity, reliability, and backup capability. RAID systems may vary in levels of redundancy, with no redundancy being a single, non-mirrored disk as level 0, two disks that mirror each other as level 1, on up, with level 5 being one of the most common. RAID systems are more complicated to restore and copy.

Refresh Rate: The number of times per second a computer display is updated.

Region (of an image): An area of an image file that is selected for specialized processing. Also called a zone.

Registration: (1) In document coding, the process of lining up an image of a form to determine the location of specific fields. See Coding; (2) entering pages into a scanner such that they are correctly read.

Relational Database: A model of databases where data is stored in two or more tables and the tables are linked to each other by a field common to the tables, sometimes referred to as a primary key.

Relative Path: The electronic path on a network or computer to an individual file from a common point on the network.

Remote Access: The ability to access and use digital information from a location off-site from where the information is physically located; e.g., to use a computer, modem, and some remote access software to connect to a network from a distant location.

Render Images: To take a native-format electronic file and convert it to an image that appears as if the original format file were printed to paper. See Image Processing.

Replication: See Disk Mirroring.

Report: Formatted output of a system providing specific information.

Repository for Electronic Records: A direct access device on which the electronic records and associated metadata are stored. Sometimes called a records store or records archive.

Residual Data: Sometimes referred to as ambient data; data that is not active on a computer system as the result of being deleted or moved to another location and is unintentionally left behind. Residual data includes: (1) data found on media free space; (2) data found in file slack space; and (3) data within files that has functionally been deleted in that it is not visible using the application with which the file was created, without use of undelete or special data-recovery techniques. May contain copies of deleted files, internet files, and file fragments. See Latent Data.

Resolution: Refers to the sharpness and clarity of an image. The term is most often used to describe monitors, printers, and graphic images.

Restore: To transfer data from a backup medium (such as tapes) to an active system, often for the purpose of recovery from a problem, failure, or disaster. Restoration of archival media is the transfer of data from an archival store to an active system for the purposes of processing (such as query, analysis, extraction, or disposition of that data). Archival restoration of systems may require not only data restoration but also replication of the original hardware and software operating environment. Restoration of systems is often called recovery.

Retention Schedule: See Records Retention Schedule.

Reverse Engineering: The process of analyzing a system or piece of software to identify how it was created in order to recreate it in a new or different form. Reverse engineering is usually undertaken in order to redesign the system for better maintainability or to produce a copy of a system without utilizing the design from which it was originally produced. For example, one might take the executable code of a computer program, run it to study how it behaved with different input, and then attempt to write a program that behaved the same or better.

Review: The process of reading or otherwise analyzing documents to determine the document's applicability to some objective or subjective standard. Often used to describe the examination of documents in a legal context for their responsiveness or relevance to specific issues in a matter. See Native Format Review; Online Review.

Review Batch: See Linear and Nonlinear Review.

Rewriteable Technology: Storage devices where the data may be written more than once—typically hard drives, floppy disks, and optical disks.

RFC822: A standard that specifies a syntax for text messages sent between one or more computer users, within the framework of email.

Rich Text Format (RTF): A standard text file format that preserves minimal stylistic formatting of document files for ease in exchange between various parties with different software.

Richness: See Prevalence.

RIM: Records and information management. (RIM is also used as the acronym of the company that developed and sells BlackBerry devices, Research In Motion.)

Rip: To extract electronically stored information from container files, e.g., to unbundle email collections into individual emails,

during the eDiscovery process while preserving metadata, authenticity, and ownership. Also used to describe the extraction or copying of data to or from an external storage device.

RLE: See Run Length Encoded.

Role-based Access Controls (RBAC): The capability of a program or platform to limit access to certain functions based upon user roles.

ROM: See Read-Only Memory.

Root Directory: The top level in a hierarchical file system. For example, on a personal computer, the root directory of the hard drive (usually C:) contains all the second-level subdirectories on that drive.

Root Expander: A search tool that identifies words with multiple endings of the term searches. For example, applying a root expander to "appl" would identify documents hitting the terms apply, applied, application, and applies. However, unlike stemming, if a root expander was added to "apply," documents with applied, application, and applies would not be identified. See Stemming.

Router: A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs, or a LAN and its ISP network. Routers are located at gateways, the places where two or more networks connect. See Wireless Router.

RTF: See Rich Text Format.

Run Length Encoded (RLE): A compressed image format that supports only 256 colors; most effective on images with large areas of black or white.

SaaS: See Software as a Service.

Sampling: The process of taking a subset of data from a larger set of data to test for the existence or frequency of a specific target or set of information that may be contained in the larger set of data. It can be a useful technique in addressing a number of issues relating to litigation, including decisions about what repositories of data are appropriate to search in a particular litigation, and determinations of the validity and effectiveness of searches or other data extraction procedures. See also Random Sampling, Stratified Sampling, and Statistical Sampling.

SAN: See Storage Area Network.

SAR: See Subject Access Request.

SAS-70 (Statement on Auditing Standards No. 70, Service Organizations): An auditing standard developed by the American Institute of Certified Public Accountants that includes an examination of an entity's controls over information technology, security, and related processes. There are two types of examinations: Type I examines the policies and procedures in place for their effectiveness to the stated objective; Type II reports on how the systems were actually used during the period of review. The SAS-70 Type II assessment is often used by hosting vendors and storage co-locations as a testament to their internal controls.

Scalability: The capacity of a system to expand without requiring major reconfiguration or reentry of data. For example, multiple servers or additional storage can be easily added.

Scale-to-Gray: An option to display a black-and-white image file in an enhanced mode, making it easier to view. A scale-to-gray display uses gray shading to fill in gaps or jumps (known as aliasing) that occur when displaying an image file on a computer screen. Also known as grayscale.

Schema: A set of rules or a conceptual model for data structure and content, such as a description of the data content and relationships in a database.

Script. A series of commands written to instruct a computer or other electronic computing device to perform an action or series of actions.

Scroll Bar: The bar on the side or bottom of a window that allows the user to scroll up and down through the window's contents. Scroll bars have scroll arrows at both ends and a scroll box, all of which can be used to scroll around the window.

SCSI: See Small Computer System Interface.

SDLT: See Super DLT.

Search: See Bayesian Search; Boolean Search; Concept Search; Contextual Search; Full-Text Search; Fuzzy Search; Index; Keyword; Pattern Recognition; Proximity Search; Query By Image Content (QBIC); Sampling; Search Engine; and Search Syntax.

Search Engine: A program that enables a search for keywords or phrases, such as on web pages throughout the World Wide Web, e.g., Google, Bing, etc.

Search Syntax: The grammatical formatting of a search string, which is particular to the search program. Includes formatting for proximity searches, phrase searches, or any other options that are supported by the search program.

Sector: A sector is normally the smallest individually addressable unit of information stored on a hard-drive platter and usually holds 512 bytes of information. Sectors are numbered sequentially starting with 1 on each individual track. Thus, Track 0, Sector 1 and Track 5, Sector 1 refer to different sectors on the same hard drive. The first PC hard disks typically held 17 sectors per track.

Secure Hash Algorithm (SHA-1 and SHA-2): A family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). Similar to MD5, SHA hash

algorithms are used to give a numeric value to a digital file or piece of data. In the context of eDiscovery, they are used to find duplicates in a data collection. See Hash Coding.

Security Information and Event Management (SIEM): Products and services designed to provide real-time information about security threats based upon analyzing data and logs from various sources in an enterprise.

Seed Set: A manually compiled set of documents used to train an analytic index for the purposes of performing some form of technology-assisted review. The set of documents can be gathered using various forms of sampling.

Sentiment Analysis: Sometimes referred to as opinion mining or emotion AI, sentiment analysis uses natural language processing to determine the emotional tenor of each component (phrase, sentences, segments). Basic examples would be positive or negative sentiment.

Serial Line Internet Protocol (SLIP): A connection to the internet in which the interface software runs in the local computer, rather than the internet's.

Serial Port: See Port.

Server: Any central computer on a network that contains electronically stored information or applications shared by multiple users of the network on their client computers; servers provide information to client machines. For example, there are web servers that send out web pages, mail servers that deliver email, list servers that administer mailing lists, FTP servers that hold FTP sites and deliver ESI to requesting users, and name servers that provide information about internet host names. See File Server.

> *Glossary* definition cited: *Rosehoff, Ltd. v. Truscott Terrace Holdings LLC*, 2016 WL 2640351, at *5 (W.D.N.Y. May 10, 2016).

Server Farm: A cluster of servers.

Service-Level Agreement: A contract that defines the technical support or business parameters that a service provider or outsourcing firm will provide its clients. The agreement typically spells out measures for performance and consequences for failure.

Session: A lasting connection, usually involving the exchange of many packets between a user or host and a server, typically implemented as a layer in a network protocol, such as Telnet or File Transfer Protocol (FTP).

SGML/HyTime: A multimedia extension to Standard Generalized Markup Language, sponsored by the Department of Defense.

SHA: See Secure Hash Algorithm.

Short Message Service (SMS): The most common data application for text messaging communication, SMS allows users to send text messages to phones and other mobile communication devices. See Text Message.

SIEM: See Security Information and Event Management.

Signature: See Certificate.

SIMM: See Single, In-Line Memory Module.

Simple Mail Transfer Protocol (SMTP): The protocol widely implemented on the internet for exchanging email messages.

Simple Network Management Protocol (SNMP): A standard, application-level protocol used to manage and monitor devices on an internet protocol network.

Simplex: One-sided page(s).

Single, In-Line Memory Module (SIMM): A mechanical package (with "legs") used to attach memory chips to printed circuit boards.

Single Instance Storage: The method of de-duplication that is undertaken on a storage device to maximize space by eliminating multiple copies of a single file by retaining only one copy. This system of storage can occur either on a file level or on a field level, where individual components of files are disassembled so that only unique parts are retained across an entire population and the reassembly of the original files is managed upon demand.

Slack Space: The unused space that exists on a hard drive when the logical file space is less than the physical file space. Also known as file slack. A form of residual data, the amount of on-disk file space from the end of the logical record information to the end of the physical disk record. Slack space can contain information soft-deleted from the record, information from prior records stored at the same physical location as current records, metadata fragments, and other information useful for forensic analysis of computer systems. See Cluster Bitmap; Cluster (File); Physical File Storage.

> *Glossary* definition cited: *Javeler Marine Services LLC v. Cross,* 175 F. Supp. 3d 756, 762 (S.D. Tex. 2016).

SLIP: See Serial Line Internet Protocol.

Small Computer System Interface (SCSI, pronounced "skuzzy"): A common, industry standard connection type between computers and peripherals, such as hard disks, CD-ROM drives, and scanners. SCSI allows for up to seven devices to be attached in a chain via cables.

Smart Card: A credit-card-size device that contains a microprocessor, memory, and a battery.

SMS: See Short Message Service.

SMTP: See Simple Mail Transfer Protocol.

Snapshot: See Bit Stream Backup.

SNMP: See Simple Network Management Protocol.

SOC1 and SOC2 Reports. Reports on an organization's compliance regarding their control of data security and management as detailed in the organization's SSAE16 standards. SOC1 reports on controls at a point in time, while SOC2 details compliance with controls over time, usually six months. See also SSAE16.

Social Media: Internet applications that permit individuals or organizations to interactively share content and communicate.

Social Network: A group of people that use the internet to share and communicate, either professionally or personally, in a public setting typically based on a specific theme or interest. For example, Facebook is a popular social network that allows people to connect to friends and acquaintances anywhere in the world in order to share personal updates, pictures and experiences, and is used by entities as a public-facing presence.

Software: Any set of coded instructions (programs) stored on computer-readable media that control what a computer does or can do. Includes operating systems and software applications.

Software Application: See Application; Software.

Software as a Service (SaaS): Software application delivery model where a software vendor develops a web-native software application and hosts and operates (either independently or through a third-party) the application for use by its customers over the internet. Customers pay not for owning the software itself, but for using it. See Application Service Provider (ASP); Cloud Computing.

Speckle: Imperfections in an image, as a result of scanning paper documents, that do not appear on the original.

Spoliation: The destruction of records or properties, such as metadata, that may be relevant to ongoing or anticipated litigation, government investigation, or audit. Courts differ in their interpretation of the level of intent required before sanctions may be warranted.

> *Glossary* definition cited: *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 516 (D. Md., 2010). *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598, 612 (S.D. Tex., 2010). *Quantlab Technologies Ltd. (BGI) v. Godlevsky*, 2014 WL 651944, at *8 (S.D. Tex. Feb. 19, 2014). *Castano v. Wal-Mart Stores Texas, LLC*, 2015 WL 2180573, at *2 (S.D. Tex. May 7, 2015).

SPP: See Standard Parallel Port.

Spyware: A data collection program that secretly gathers information about the user and relays it to advertisers or other interested parties. Adware usually displays banners or unwanted pop-up windows but often includes spyware as well. See Malware.

SQL: See Structured Query Language.

SQL Injection: A database attack process hackers implement to execute SQL commands against a database server through fields presented by a web browser application. See also Structured Query Language.

SSAE16: The successor to the Statement on Auditing Standards No. 70 (SAS 70) auditing standard, which details the parameters and policies of data security and handling for an organization. The reports regarding performance to the SSAE16 standards are identified as SOC1 and SOC 2 reports. See also SOC 1 and SOC 2 Reports.

Stand-Alone Computer: A personal computer that is not connected to any other computer or network.

Standard Generalized Markup Language (SGML): An informal industry standard for open systems document management that specifies the data encoding of a document's format and content. Has been virtually replaced by Extensible Markup Language (XML).

Standard Parallel Port (SPP): See Port.

Static Search: A search that is constructed to return the same records regardless of ongoing activity in the database, such as newly added documents or updated tagging. See Dynamic Search.

Statistical Sampling: A process used while sampling data to ensure that a sample is accurately representative of the entire population and is not affected by any kind of bias toward a specific attribute of the underlying data. See also Sampling.

Steganography: The hiding of information within a more obvious kind of communication. Although not widely used, digital steganography involves the hiding of data inside a sound or image file. Steganalysis is the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes.

Stemming: A search logic whereby the search engine identifies other terms based on the natural language root of the term being search. For example, stemming "apply" would identify documents hitting the terms apply, applied, application, and applies. See Root Expander.

Stop Words: Common words (e.g., all, the, of, but, not) that are purposefully excluded from a search index when it is created in order to make the index more efficient. Also knows as Noise Words.

Storage Area Network (SAN): A high-speed subnetwork of shared storage devices. A storage device is a machine that contains nothing but a disk or disks for storing data. A SAN's architecture works in a way that makes all storage devices available to all servers on a local-area network (LAN) or wide-area network (WAN). As more storage devices are added to a SAN, they too will be accessible from any server in the larger network. The server merely acts as a pathway between the end user and the stored data. Because stored data does not reside directly on any of a network's servers, server power is utilized for business applications, and network capacity is released to the end user. See Network.

Storage Device: A device capable of storing ESI.

Storage Media: See Magnetic/Optical Storage Media.

Stratified Sampling: A method of data sampling where data is initially divided into subgroups (e.g., by age range or a geographic criteria) or strata, and then each group is sampled in order to ensure that each subgroup is properly represented. See also Sampling.

Streaming Indexing: Real-time or near-real-time indexing of data as it being moved from one storage medium to another.

Structured Data: Data stored in a structured format, such as databases or data sets according to specific form and content rules as defined by each field of the database. Contrast to Unstructured Data.

Structured Query Language (SQL): A database computer language used to manage the data in relational databases. A standard fourth generation programming language (4GL—a programming language that is closer to natural language and easier to work with than a high-level language).

Subject Access Request (SAR): See DSAR.

Subjective Coding: Recording the judgments of a reviewer as to a document's relevancy, privilege, or importance with regard to factual or legal issues in a legal matter. See Coding.

Super DLT (SDLT): A type of backup tape that can hold up to 300 GB or 450 CDs, depending on the data file format. See Digital Linear Tape (DLT).

Supervised Learning: Use of machine learning to analyze data, using training examples that have been coded by humans, such as categorization. See also Unsupervised Learning.

Support Vector Machine (SVM): A machine-learning algorithm used to classify sets of data, distinguished from other machine-learning algorithms by its need for less exemplar input for its calculations and its use of less computing power.

Suspension Notice or Suspension Order: See Legal Hold.

SVM: See Support Vector Machine.

Swap File: A file used to temporarily store code and data for programs that are currently running. This information is left in the swap file after the programs are terminated and may be retrieved using forensic techniques. See also Page File/Paging File.

> *Glossary* definition cited: *Javeler Marine Services LLC v. Cross,* 175 F. Supp. 3d 756, 762 (S.D. Tex. 2016).

Switch (Network Switch): A network device that accepts incoming data packets and distributes them to their destination on a Local Area Network (LAN).

Symmetric Key Encryption: The same key both encrypts and decrypts messages, often used in email encryption.

System: (1) A collection of people, machines, and methods organized to perform specific functions; (2) An integrated whole composed of diverse, interacting, specialized structures, and subfunctions; and/or (3) A group of subsystems united by some

interaction or interdependence, performing many duties but functioning as a single unit.

System Administrator (sysadmin or sysop): The person responsible for and/or in charge of keeping a network or enterprise resource, such as a large database, operational.

System Files: Files allowing computer systems to run; non-user-created files.

System-Generated Metadata: Information about a file that is created and applied to a file by a computer process or application. Information could include the data a file was saved, printed or edited, and can include where a file was stored and how many times it has been edited. See Metadata.

> *Glossary* definition cited: *CBT Flint Partners, LLC v. Return Path, Inc.*, 737 F.3d 1320, 1328 (Fed. Cir. 2013).

T1: A high-speed, high-bandwidth leased line connection to the internet. T1 connections deliver information at 1.544 megabits per second.

T3: A high-speed, high-bandwidth leased line connection to the internet. T3 connections deliver information at 44.746 megabits per second.

Tabletop Exercise: In an information security data breach context, a tabletop exercise is a meeting to discuss the incident response policy, plan, and procedures. Attendees are typically key personnel, each of whom is responsible for specific tasks before, during, and after a data breach incident.

Tagged Image File Format (TIFF): A widely used and supported graphic file format for storing bit-mapped images, with many different compression formats and resolutions. File name has .TIF extension. Can be black and white, gray-scaled or color. Images are stored in tagged fields, and programs use the tags to

accept or ignore fields, depending on the application. The format originated in the early 1980s.

> *Glossary* definition cited: *Williams v. Sprint/United Management Co.*, 230 F.R.D. 640, 643 (D. Kan. 2005). *In re Seroquel Products Liability Litigation*, 244 F.R.D. 650, 652 (M.D. Fla., Aug. 21, 2007). *Race Tires America, Inc. v. Hoosier Racing Tire Corp.*, 674 F.3d 158, 161 (3d Cir. 2012). *Country Vintner of North Carolina, LLC v. E. & J. Gallo Winery, Inc.*, 718 F.3d 249, 253 (4th Cir. 2013). *Saliga v. Chemtura Corp.*, 2013 WL 6182227, at *2 (D. Conn. Nov. 25, 2013). *Akanthos Capital Mgmt., LLC v. CompuCredit Holdings Corp.*, 2 F. Supp. 3d 1306, 1315 (N.D. Ga. 2014). *E.E.O.C. v. SVT, LLC*, 2014 WL 1411775 (N.D. Ind. Apr. 10, 2014). *Balance Point Divorce Funding, LLC v. Scrantom*, 305 F.R.D. 67, 74 (S.D.N.Y. 2015).

Tape Drive: A hardware device used to store or back up electronically stored information on a magnetic tape. Tape drives are sometimes used to back up large quantities of ESI due to their large capacity and cheap cost relative to other storage options.

TAR: See Technology-Assisted Review.

Taxonomy: The science of categorization, or classification, of things based on a predetermined system. In reference to websites and portals, a site's taxonomy is the way it organizes its electronically stored information into categories and subcategories, sometimes displayed in a site map. Used in information retrieval to find documents related to a query by identifying other documents in the same category.

TCP/IP: See Transmission Control Protocol/Internet Protocol.

Technology-Assisted Review (TAR)[1]: A process for prioritizing or coding a collection of electronically stored information using a computerized system that harnesses human judgments of subject-matter experts on a smaller set of documents and then extrapolates those judgments to the remaining documents in the collection. Some TAR methods use algorithms that determine how similar (or dissimilar) each of the remaining documents is to those coded as relevant (or nonrelevant) by the subject-matter experts, while other TAR methods derive systematic rules that emulate the experts' decision-making processes. TAR systems generally incorporate statistical models and/or sampling techniques to guide the process and to measure overall system effectiveness.

Telnet (Telecommunications Network): A protocol for logging onto remote computers from anywhere on the internet.

Template: Sets of index fields for documents, providing a framework for preparation.

Temporary (Temp) File: Contemporaneous files created by applications and stored on a computer for temporary use only; created to enable the processor of the computer to quickly pull back and assemble data for currently active files.

Terabyte: 1,024 gigabytes (approximately one trillion bytes). See Byte.

Text Delimited File: A common format for structured data exchange whereby a text file contains fielded data, separated by a specific ASCII character and also usually containing a header

[1] Maura R. Grossman & Gordon V. Cormack, *The Grossman-Cormack Glossary of Technology-Assisted Review with Forward by John M. Facciola, U.S. magistrate Judge*, 2013 FED. CTS. L. REV. 7 (January 2013), *available at* https://www.fclr.org/fclr/articles/html/2010/grossman.pdf.

line that defines the fields contained in the file. See Field Separator or Field Delimiter.

Text Message: An electronic message, historically restricted to 160 characters in length, that is sent among users with mobile devices. The messages can be sent via the Short Messaging Service (SMS), as well as images, video, and other multimedia using the Multimedia Messaging Service (MMS).

Text Mining: The application of data mining (knowledge discovery in databases) to unstructured textual data. Text mining usually involves structuring the input text (often parsing, along with application of some derived linguistic features and removal of others, and ultimate insertion into a database), deriving patterns within the data, and evaluating and interpreting the output, providing such ranking results as relevance, novelty, and interestingness. Also referred to as Text Data Mining. See Data Mining.

Text Retrieval Conference (TREC): An ongoing series of workshops co-sponsored by the National Institute of Standards and Technology (NIST) and the U.S. Department of Defense.

TGA: Targa format file. A scanned format that is widely used for color-scanned materials (24-bit) as well as by various paint and desktop publishing packages.

Thin Client: A computer or software program that relies on a central server for processing and application resources, and electronically stored information storage in a central area instead of locally; used mainly for output and input of user information or commands. See Client.

Thread: A series of technologically related communications, usually on a particular topic. Threads can be a series of bulletin board messages (for example, when someone posts a question and others reply with answers or additional queries on the same topic). A thread can also apply to emails or chats, where

multiple conversation threads may exist simultaneously. See Email String.

Thread Suppression: A process whereby noninclusive emails and redundant attachments within email threads are removed (suppressed) from a review set to reduce the overall review population.

Threading: A process of recombining email or other electronic message conversations into a single comprehensive, chronologically correct chain.

Threat Vector: A computer network infrastructure path that is used by hackers to penetrate security defenses. For example, phishing attacks leverage an email threat vector.

Thumb Drive: See Flash Drive.

Thumbnail: A miniature representation of a page or item for quick overviews to provide a general idea of the structure, content, and appearance of a document. A thumbnail program may be a standalone or part of a desktop publishing or graphics program. Thumbnails provide a convenient way to browse through multiple images before retrieving the one needed. Programs often allow clicking on the thumbnail to retrieve it.

TIFF: See Tagged Image File Format.

TIFF Group III: A one-dimensional compression format for storing black-and-white images that is utilized by many fax machines. See TIFF.

TIFF Group IV: A two-dimensional compression format for storing black-and-white images. Typically compresses at a 20-to-1 ratio for standard business documents. See TIFF.

Time Zone Normalization: See Normalization.

Toggle: A switch (which may be physical or virtualized on a screen) that is either on or off and reverses to the opposite when selected.

Tone Arm: A device in a computer that reads to/from a hard drive.

Tool Kit Without An Interesting Name (TWAIN): A universal toolkit with standard hardware/software drivers for multimedia peripheral devices. Often used as a protocol between a computer and scanners or image-capture equipment.

Toolbar: The row of graphical or text buttons that perform special functions quickly and easily.

Topology: The geometric arrangement of a computer system. Common topologies include a bus (nodes are connected to a single cable, with terminators at each end); Star LAN (designed in the shape of a star, where all end points are connected to one central switching device, or hub); and ring (nodes are connected in a closed loop; no terminators are required because there are no unconnected ends). Star networks are easier to manage than ring topology.

Track: Each of the series of concentric rings contained on a hard-drive platter.

Transmission Control Protocol/Internet Protocol (TCP/IP): The first two defined networking protocols; enable the transfer of data upon which the basic workings of the features of the internet operate. See Internet Protocol; Port.

TREC: See Text Retrieval Conference.

Trojan: A malware program that contains another hidden program embedded inside it for the purpose of discretely delivering the second program to a computer or network without the knowledge of the user or administrator. See Malware.

True Resolution: The true optical resolution of a scanner is the number of pixels per inch (without any software enhancements).

TWAIN: See Tool Kit Without An Interesting Name.

TWiki: Enables simple, form-based web applications without programming, and granular access control (though it can also operate in the classic "no authentication" mode). Other enhancements include configuration variables, embedded searches, Server Side Includes (scripting language), file attachments, and a plug-in application programming interface (API) that has spawned over 150 plug-ins to link into databases, create charts, sort tables, write spreadsheets, make drawings, and so on. See Wiki.

Typeface: A specific size and style of type within a family. There are many thousands of typefaces available for computers, ranging from modern to decorative.

UDP: See User Datagram Protocol.

Ultrafiche: Microfiche that can hold 1,000 documents/sheet as opposed to the normal 270.

Unallocated Space: The area of computer media, such as a hard drive, that does not contain readily accessible data. Unallocated space is usually the result of a file being deleted. When a file is deleted, it is not actually erased but is simply no longer accessible through normal means. The space that it occupied becomes unallocated space, i.e., space on the drive that can be reused to store new information. Until portions of the unallocated space are used for new data storage, in most instances, the old data remains and can be retrieved using forensic techniques.

Underinclusive: When referring to data sets returned by some method of query, search, filter, or cull, results that are returned incomplete or too narrow. See False Negative.

Unicode: A 16-bit ISO 10646 character set accommodating many more characters than the ASCII character set. Created as a standard for the uniform representation of character sets from all languages. Unicode supports characters 2 bytes wide. Sometimes referred to as "double-byte language." See https://www.unicode.org for more information.

Uniform Resource Indicator (URIs): A uniform set of characters that specifies the location of resources on a network, commonly the world wide web. See World Wide Web.

Uniform Resource Locator (URL): The addressing system used in the World Wide Web and other internet resources. The URL contains information about the method of access, the server to be accessed, and the path of any file to be accessed. Although there are many different formats, a URL might look like this: http://thesedonaconference.org/publications. See Address.

Unitization—Physical and Logical: The assembly of individually scanned pages into documents. Physical unitization uses actual objects such as staples, paper clips, and folders to determine pages that belong together as documents for archival and retrieval purposes. Logical unitization is the process of human review of each individual page in an image collection, using logical cues to determine pages that belong together as documents. Such cues can be consecutive page numbering, report titles, similar headers and footers, and other logical indicators. This process should also capture document relationships, such as parent and child attachments. See Attachment; Document or Document Family; Load File; and Message Unit.

> *Glossary* definition cited: *Race Tires America, Inc. v. Hoosier Racing Tire Corp.*, 674 F.3d 158, 161 (3d Cir. 2012). *Balance Point Divorce Funding, LLC v. Scrantom*, 305 F.R.D. 67, 74 (S.D.N.Y. 2015).

Universal Serial Bus (USB) Port: A port on a computer or peripheral device into which a USB cable or device can be inserted—quickly replacing the use or need for serial and parallel ports by providing a single, standardized way to easily connect many different devices. See Flash Drive and Port.

UNIX: A software operating system designed to be used by many people at the same time (multiuser) and capable of performing multiple tasks or operations at the same time (multitasking); common operating system for internet servers.

Unstructured Data: Free-form data that either does not have a data structure or has a data structure not easily readable by a computer without the use of a specific program designed to interpret the data; created without limitations on formatting or content by the program with which it is being created. Examples include word-processing documents or slide presentations.

Unsupervised Learning: Use of machine learning to analyze data without training examples, such as clustering.

Upgrade: A newer version of hardware, software or application.

Upload: To move data from one location to another in any manner, such as via modem, network, serial cable, internet connection, or wireless signals; indicates that data is being transmitted to a location from a location. See Download.

> *Glossary* definition cited: *In re Online DVD-Rental Antitrust Litigation*, 779 F.3d 914, 929 (9th Cir. 2015).

URL: See Uniform Resource Locators.

USB: See Universal Serial Bus Port.

User-Created Metadata: Information about a file that is created and applied to a file by a user. Information includes the addressees of an email, annotations to a document, and objective coding information. See Metadata.

Glossary definition cited: *CBT Flint Partners, LLC v. Return Path, Inc.*, 737 F.3d 1320, 1328 (Fed. Cir. Dec. 13, 2013).

User Datagram Protocol (UDP): A protocol allowing computers to send short messages to one another. See Port.

UTC: See Coordinated Universal Time.

UTF-8: A character-encoding form of Unicode that represents Unicode code points with sequences of one, two, three, or four bytes. UTF-8 can encode any Unicode character. It is the most common Unicode encoding on the web and the default encoding of XML. An important advantage of UTF-8 is that it is backward compatible with ASCII encoding, which includes the basic Latin characters. Consequently, all electronic text in ASCII encoding is conveniently also Unicode. This backward compatibility was a primary reason for the invention of UTF-8. See ASCII; Unicode; UTF-16.

UTF-16: A character-encoding form of Unicode that represents Unicode code points with sequences of one or two 16-bit code units. UTF-16 can encode any Unicode character. It is used much less often for data interchange than the UTF-8 encoding form. UTF-16 is commonly used in computer programming languages and application programming interfaces (APIs) and is the encoding used internally for file names by Microsoft Windows and NTFS. See Unicode; UTF-8.

Validate: In the context of this document, to confirm or ensure well-grounded logic, and true and accurate determinations.

Validation: The process by which the effectiveness of a workflow is checked for accuracy.

VDT: See Video Display Terminal.

Vector: Representation of graphic images by mathematical formulas. For instance, a circle is defined by a specific position and radius. Vector images are typically smoother than raster images.

Verbatim Coding: Manually extracting information from documents in a way that matches exactly as the information appears in the documents. See Coding.

Version, Record Version: A particular form or variation of an earlier or original record. For electronic records the variations may include changes to file format, metadata, or content.

Vertical De-Duplication: A process through which duplicate electronically stored information, as determined by matching hash values, are eliminated within a single custodian's data set. See Content Comparison; File-Level Binary Comparison; Horizontal De-Duplication; Metadata Comparison; Near Duplicates.

VESA: See Video Electronics Standards Association.

Video Display Terminal (VDT): Generic name for all display terminals.

Video Electronics Standards Association (VESA): Sets industry-wide computer video standards. See https://vesa.org.

Video Scanner Interface: A type of device used to connect scanners with computers. Scanners with this interface require a scanner control board designed by Kofax, Xionics, or Dunord.

Virtual Backup: A data backup that is stored on a virtual server.

Virtual Private Network (VPN): A secure network that is constructed by using public wires to secure connect nodes. For example, there are a number of systems that enable creation of networks using the internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Virtualization: Partitioning a server into multiple virtual servers, each capable of running an independent operating system and associated software applications as though it were a separate computer. Virtualization is particularly useful for

centralized IT infrastructures to manage multiple computing environments with the same set of hardware, and for cloud computing providers to provide customized interfaces to clients without investing in separate machines, each with its own operating system.

Virus: A self-replicating program that spreads on a computer or network by inserting copies of itself into other executable code or documents. A program into which a virus has inserted itself is said to be infected, and the infected file (or executable code that is not part of a file) is a host. Viruses are a kind of malware that range from harmless to destructive and damage computers by either destroying data or overwhelming the computer's resources. See Malware.

Visualization: The process of graphically representing data.

Vital Record: A record that is essential to the organization's operation or to the reestablishment of the organization after a disaster.

Voice over Internet Protocol (VoIP): Telephonic capability across an internet connection.

VoIP: See Voice over Internet Protocol.

Volume: A specific amount of storage space on computer storage media such as hard drives, floppy disks, CD-ROM disks, etc. In some instances, computer media may contain more than one volume, while in others a single volume may be contained on more than one disk.

Volume Boot Sector/Record: When a partition is formatted to create a volume of data, a volume boot sector is created to store information about the volume. One volume contains the operating system, and its volume boot sector contains code used to load the operating system when the computer is booted up. See Partition.

VPN: See Virtual Private Network.

WAN: See Wide Area Network.

Warm Storage: See Near-Line Storage.

WAV: File extension name for Windows sound files.

Wearable: A term used to describe an electronic device or piece of clothing worn by an individual that can track and record specific information, such as exercise, health information, or sleep patterns.

Web Services Description Language (WSDL): A WSDL (pronounced "wiz del") file provides information on the available functionality of web-based applications that allows interaction with other web-based applications. WSDL files can be used by hackers to identify access points into a web-based application.

Webmail: Email service that is provided through a website. See Email.

Website: A collection of Uniform Resource Indicators (URIs), including Uniform Resource Locators (URLs), in the control of one administrative entity. May include different types of URIs (e.g., FTP, telnet, or internet sites). See URI; URL.

What You See Is What You Get (WYSIWYG): Display and software technology that shows on the computer screen exactly what will print.

Wide Area Network (WAN): Refers generally to a network of PCs or other devices, remote to each other, connected by electronic means, such as transmission lines. See Network.

WiFi (Wireless Fidelity): Wireless networking technology that allows electronic devices to connect to one another and the internet from a shared network access point.

Wiki: A collaborative website that allows visitors to add, remove, and edit content.

Wildcard Operator: A character used in text-based searching that assumes the value of any alphanumeric character, characters, or in some cases, words. Used to expand search terms and enable the retrieval of a wider range of hits.

Windows-1252: Also called ANSI, Western European, and CP1252 (Microsoft code page 1252). A character encoding of the Latin alphabet used for most Western European languages. Windows-1252 is a superset of ASCII and ISO 8859-1 standard character encodings. The characters that are included in Windows-1252, but that are not included in ISO 8859-1, are often the source of character interpretation and display problems in text on the web and in electronic mail. Similar problems sometimes occur when text in the Windows-1252 encoding is converted to the UTF-8 encoding form of Unicode, because UTF-8 is not wholly backward compatible with Windows-1252. The name ANSI is a misnomer resulting from historical happenstance, but it is not incorrect to use it in contexts where its meaning is readily understood. See ASCII; ISO 8859-1.

Wireless Router: A hardware device that opens access to a secured or unsecured internet connection or network via a receiver on a computer or other piece of hardware, such as a printer permitting wireless transmission. See WiFi.

WISP: See Written Information Security Program.

Workflow: The automation of a business process, in whole or part, during which electronically stored information or tasks are passed from one participant to another for action according to a set of procedural rules.

Workflow, Ad Hoc: A simple manual process by which documents can be moved around a multiuser review system on an as-needed basis.

Workflow, Rule-Based: A programmed series of automated steps that route documents to various users on a multiuser review system.

Workgroup: A group of computer users connected to share individual talents and resources as well as computer hardware and software—often to accomplish a team goal.

World Wide Web (WWW): A massive collection of hypertext documents accessed via the internet using a browser. The documents, also known as web pages, can contain formatted text, audio and video files, and multimedia programs.

Worm: A self-replicating computer program, sending copies of itself, possibly without any user intervention. See Malware.

WORM Disks: See Write Once Read Many Disks.

Write Once Read Many Disks (WORM Disks): A popular archival storage media during the 1980s. Acknowledged as the first optical disks, they are primarily used to store archives of data that cannot be altered. WORM disks are created by standalone PCs and cannot be used on the network, unlike CD-ROM disks.

Written Information Security Program (WISP): Administrative, technical, and physical safeguards appropriate to an entity's size and complexity, the nature and scope of activities, and the sensitivity of information at issue. A requirement that an information security program be in writing.

WSDL: See Web Services Description Language.

WWW: See World Wide Web.

WYSIWYG: See What You See Is What You Get.

X.25: A standard protocol for data communications that has largely been replaced by less complex protocols, including the internet protocol (IP).

XML, XRML: See Extensible Markup Language.

Yottabyte: 1,024 zettabytes. See Byte.

Zettabyte: 1,024 exabytes. See Byte.

ZIP: A common file compression format that allows quick and easy storage for transmission or archiving one or several files.

Zip Drive: A removable disk storage device developed by Iomega with disk capacities of 100, 250, and 750 megabytes.

Zombie Cookies: An illicit http cookie that will recreate itself after deletion and is typically stored outside of a web browser's normal cookie storage area in order to get around a user's preference.

Zone OCR: An add-on feature of imaging software that populates data fields by reading certain regions or zones of a document and then placing the recognized text into the specified field.

THE SEDONA CONFERENCE COMMENTARY AND PRINCIPLES ON JURISDICTIONAL CONFLICTS OVER TRANSFERS OF PERSONAL DATA ACROSS BORDERS

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

Author:
The Sedona Conference

Drafting Team Leaders:
Wayne Matus
David C. Shonka

Drafting Team:
Michael Bahar
Susan Bennett
Oliver Brupbacher
Conor R. Crowley
Emily Fedeles
Jerami Kemnitz
Brian Ray
Alexander White

Steering Committee Liaison:
Taylor Hoffman

Staff Editors:
David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 6. They do not necessarily represent the views of any of the individual participants or their

employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

The publication may be cited as follows:

> The Sedona Conference, *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, 21 SEDONA CONF. J. 393 (2020).

PREFACE

Welcome to The Sedona Conference *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders ("Commentary")*, a project of The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way. Other WG6 publications provide guidance to individuals and organizations attempting to navigate cross-border conflicts.[1]

The Sedona Conference acknowledges and thanks Drafting Team Leaders David Shonka and Wayne Matus for their leadership and commitment to the project. We thank drafting team member Jerami Kemnitz for his significant efforts. We also thank drafting team members Michael Bahar, Susan Bennett, Oliver Brupbacher, Conor Crowley, Emily Fedeles, Brian Ray, and Alexander White for their efforts and commitments in time and attention to this project. We thank Ava Dixon and Juanda Moore for their assistance. Finally, we thank Taylor Hoffman for his guidance and input as the WG6 Steering Committee Liaison to the drafting team.

---

1. *See* The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, THE SEDONA CONFERENCE (Jan. 2017), https://thesedonaconference.org/publication/International_Litigation_Principles; The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557 (2018); and The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397 (2016).

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG6 who reviewed, commented on, and proposed edits to early drafts that were circulated for feedback from the Working Group membership. Other members provided feedback at WG6 meetings where drafts of this *Commentary* were the subject of dialogue. The publication was also subject to a period of public comment. On behalf of The Sedona Conference, I thank all of them for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG6 and several other Working Groups in the areas of electronic document management and discovery, data security and privacy liability, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
April 2020

TABLE OF CONTENTS

Choice-of-law Principles

Principle 1: A nation has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, natural persons and organizations in or doing business in its territory, regardless of whether the processing of the relevant personal data takes place within its territory.

Principle 2: A nation usually has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, the processing of personal data inextricably linked to its territory.

Principle 3: In commercial transactions in which the contracting parties have comparable bargaining power, the informed choice of the parties to a contract should determine the jurisdiction or applicable law with respect to the processing of personal data in connection with the respective commercial transaction, and such choice should be respected so long as it bears a reasonable nexus to the parties and the transaction.

Principle 4: Outside of commercial transactions, in which the natural person freely makes a choice, a person's choice of jurisdiction or law should not deprive him or her of protections that would otherwise be applicable to his or her data.

Principle 5: Data in transit ("Data in Transit") from one sovereign nation to another should be subject to the jurisdiction and the laws of the sovereign nation from which the data originated, such that, absent extraordinary circumstances, the data should be

treated as if it were still located in its place of origin.

Principle 6: Where personal data located within, or otherwise subject to, the jurisdiction or the laws of a sovereign nation is material to a litigation, investigation, or other legal proceeding within another sovereign nation, such data shall be provided when it is subject to appropriate safeguards that regulate the use, dissemination, and disposition of the data.

I. INTRODUCTION

Businesses today navigate, with difficulty, a bewildering maze of conflicting and confusing data protection and privacy laws. When the free flow of physical goods in global commerce faced analogous constraints in navigating the seas, nations met and resolved the most crucial issues by agreement.[2] We submit that a similar agreement is needed today to ensure the continued flow of necessary information in global commerce. Indeed, the European Union (EU) has intimated as much in Article 48 of the General Data Protection Regulation (GDPR).[3] Although it would be presumptuous to suppose that this *Commentary* might resolve these issues, the Sedona Conference hopes that it will contribute in some small way to the incipient dialogue that is beginning to take place and that sooner, rather than later, there will be an international forum to address, and ultimately resolve, the conflicts between international data protection regimens to the extent they adversely impact global commerce.

The goal of this *Commentary* is to: (1) provide a practical guide to corporations and others who must make day-to-day operational decisions regarding the transfer of data across borders; (2) provide a framework for the analysis of questions regarding the laws applicable to cross-border transfers of personal

2. Today such issues are governed by international conventions such as the United Nations Convention on the Law of the Sea and the Hague Rules (International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading).

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119/1) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents [hereinafter GDPR].

data; and (3) encourage governments to harmonize their domestic laws to facilitate global commerce.

A. The Underlying Tension

Data lies at the crossroads of the inherent tension between the free flow of information on the one hand and security and privacy on the other. Those who support free flow note that the use of that data is now critical to successful enterprise, and that tremendous wealth and power comes to those who can gather and make the best use of it. Yet McKinsey Global Institute reported in 2017 that, "Flows of physical goods and finance were the hallmarks of the 20th-century global economy, but today those flows have flattened or declined. Twenty-first-century globalization is increasingly defined by flows of data and information."[4] And that is because others value security and privacy highly and believe that free flow needs to be limited based upon principles such as consent, data minimization, and security by design. For example, whereas the U.S. generally distinguishes between public and private data, and affords the latter protections in specific areas, Europe protects the underlying right of a natural person to determine the disclosure and use of his or her personal data and affords such right general constitutional protection.

4. By 2015 cross-border data flows were 45 times larger than a decade earlier and were forecast to grow another nine times by 2020. *See* MCKINSEY GLOBAL INSTITUTE, DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS (2016), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx.

B. *Comity*[5]

What is therefore needed, and what this *Commentary* hopes to achieve, is to distill and update key choice-of-law principles with respect to personal data. In our view, comity is the bulwark against chaos, and how comity should be applied is one of the goals of this guide.[6] When comity cannot be the answer, the *Commentary* proposes steps on how conflicts can be resolved. This paper outlines the complex data and legal backdrops that cause conflict and proposes a set of principles to help achieve resolution.

One of the classic statements on "comity" comes from the U.S. Supreme Court, which in *Hilton v. Guyot*, held:

> "Comity," in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to

---

5. *See* Hilton v. Guyot, 159 U.S. 113 (1895). For example, in JP Morgan Chase Bank v. Altos Hornos de Mexico, S.A. de CV., 412 F.3d 418, 424 (2d Cir. 2005), the Second Circuit determined that U.S. courts should ordinarily decline to adjudicate creditor claims that are the subject of a foreign bankruptcy proceeding, and deference should be given to the foreign court, so long as the foreign proceedings are procedurally fair and do not contravene the laws or public policy of the U.S. It is a recognized principle of jurisprudence in the United States. William S. Dodge, *International Comity in American Law*, 115 COLUM. L. REV. 2071 (2015).

6. FED. R. CIV. P. 44.1. Determining Foreign Law requires parties who intend to raise an issue about a foreign country's law to give notice by a pleading or other writing. A recent Supreme Court case held that a district court judge has the duty and power to determine what foreign law is applicable. *See* Animal Science Products, Inc. v. Hebei Welcome Pharmaceuticals, 585 U.S. ___ (2018).

> international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws.[7]

The European Union acknowledges the concept of comity without further describing it. For example, the foundational treaties and case law reference the "mutual regard to the spheres of jurisdiction" of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law.[8]

The United States, with its passage of the Clarifying Lawful Overseas Use of Data (CLOUD) Act explicitly authorizing American law enforcement officials to compel U.S. providers to produce data, even if it is stored outside the U.S., set up an

---

7. *Hilton*, 159 U.S. at 163–64. Other Supreme Court decisions have discussed comity in terms of interpretive canons of restraint. For example, in *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100, 2107 (2016), the Court stated that the extraterritoriality canon when interpreting domestic law "avoid[s] the international discord that can result when U.S. law is applied to conduct in foreign countries," and "the need to enforce the presumption is at its apex" when there is a "risk of conflict between [an] American statute and . . . foreign law" (quotation marks omitted). In addition, under the famous "Charming Betsy" canon, U.S. courts seek to avoid interpreting domestic law in a way that violates the law of nations "if any possible construction remains," and to interpret the domestic law in light of "principles of prescriptive comity" that prohibit "unreasonable interference with the sovereign authority of other nations" (internal quotation marks omitted). F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155, 164 (2004). See also, Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for the Southern Dist. of Iowa, 482 U.S. 522 (1987).

8. *See* The Treaty on European Union arts. 3(5), 21(1), 2008 O.J. C 115/17, 115/28, *available at* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0013:0045:EN:PDF; Case 52/69, Geigy v. Commission, ¶ 11, ECLI:EU:C:1972:73; Case C-366/10, Air Transport Ass'n of America v. Sec'y of State for Energy and Climate Change, ¶ 123, ECLI:EU:C:2011:864.

exception and mechanism to enhance comity.[9] It left undefined, however, what the principles guiding a comity analysis should be.

C. Legal and Practical Complexity

The challenges just identified cut across multiple legal[10] and practical contexts.[11] Existing frameworks for bilateral and multilateral cooperation are insufficient and under increasing stress not only from the rapid expansion of data and difficulty in determining its precise location, but also from significant confusion over the appropriate criteria for showing jurisdictional

---

9. Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 4943, 115th Cong. (2d Sess. 2018). The U.S. legislature, in the CLOUD Act, mandates a judicial comity analysis in certain circumstances, but similarly does not further define it. In its savings clause, the CLOUD Act provides that it shall not "be construed to modify or otherwise affect the common law standards governing the availability or application of comity analysis . . . to instances of compulsory process issued under [the Stored Communications Act [SCA]] and not covered under [Section 2703](h)(2)]." *See* CLOUD Act § 103(c). In other words, for all cases not covered by new Section 2703(h), the CLOUD Act does not change the "common law" comity standards, which currently apply to the SCA process, but it does not define those standards.

10. For a full discussion of the legal complexity and background, please review Appendix: Data Privacy Complexity and Background, *infra*.

11. Data frequently resides across multiple services, providers, and locations, often spanning several jurisdictions. The Cloud Standards Consumer Council has published a report that nicely captures many of the risks that result from confusion over the precise location and movement of data, including: penalties that result from violating conflicting government laws or regulations; increased costs of doing business in countries that require data localization; hiring local staff; and heightened cybersecurity risk due to the multiplication of localized data centers. *See* CLOUD STANDARDS CONSUMER COUNCIL, DATA RESIDENCY CHALLENGES: A JOINT PAPER WITH THE OBJECT MANAGEMENT GROUP, 8 (2017), https://www.omg.org/cloud/deliverables/CSCC-Data-Residency-Challenges.pdf.

nexus. The diverse—and often competing—range of legal issues data implicates, ranging from criminal investigations and civil discovery to human rights and national security, further complicates the picture. Taken together, the factual, political, and legal complexities surrounding data pose new and distinctive challenges for establishing norms and principles to guide transnational cooperation.

At the core of the problem is the lack of robust coordination mechanisms for resolving competing and often conflicting legal requirements from multiple jurisdictions. This primarily procedural issue is magnified by a set of contentious debates over substantive legal issues, including the striking difference in privacy protections between nations. Further compounding these issues is a set of political and economic incentives that have resulted in a marked increase in new regulatory measures designed to increase local control over data through various means, in particular data localization laws.[12]

12. A detailed survey of the origins and status of legal complexity is provided in Appendix, *infra*.

II. CHOICE-OF-LAW PRINCIPLES

At present, there is no universal framework for cross-border data transfers in a globalized context. There are, however, certain generally recognized International Law Principles that apply to all nations, which can serve as a starting point for mitigating the conflict-of-laws issue with respect to personal data.

For example, as with other physical property, states have sovereign rights over any cyber infrastructure, such as servers and computers, located in their territory. According to the Tallinn Manual, which is concerned with cyber law in military operations . . . "[a]lthough territoriality lies at the heart of the principle of sovereignty, in certain circumstances, States may also exercise sovereign prerogatives such as jurisdiction over cyber infrastructure and activities abroad, as well as over certain persons engaged in those activities."[13]

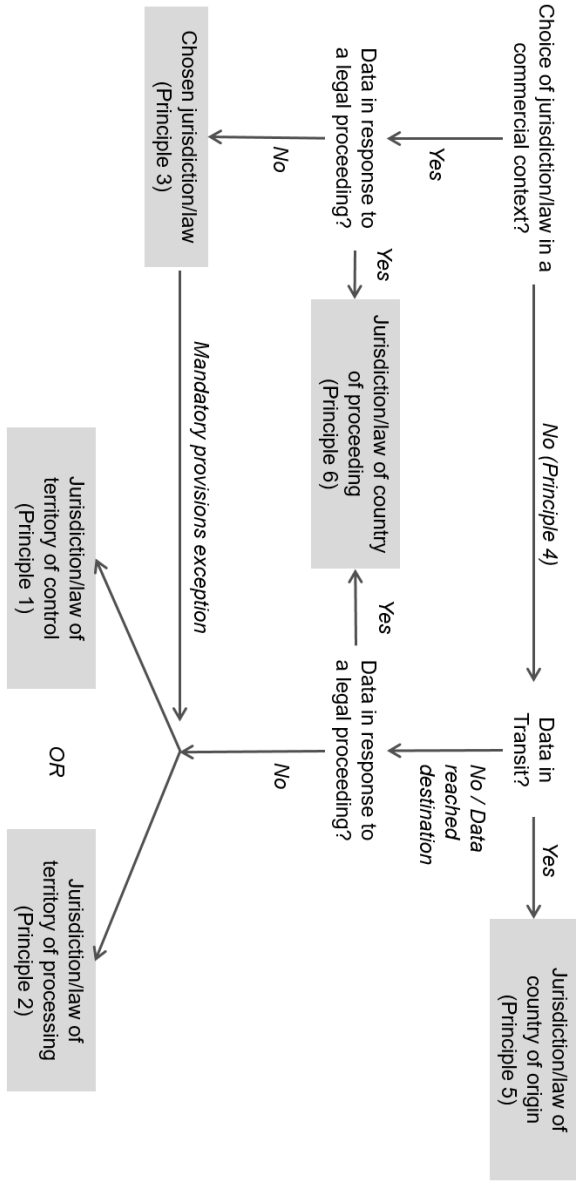
Basic principles of International Law relating to sovereignty, due diligence, jurisdiction, and the rights enjoyed by natural persons can help support a set of principles that can serve as a framework for analyzing cross-border transfers of personal and confidential data in a global economy.[14] The six Principles put

---

13. MICHAEL N. SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 11 (2d ed. 2017).

14. Traditional notions of sovereignty and jurisdiction are, and always have been, linked to territoriality and activities that take place within, or have a direct and substantial affect in, the sovereign's territory. That is the approach we have taken in this *Commentary*. Nothing said here is intended to challenge the existing framework for analyzing jurisdiction. Notably, however, the Internet & Jurisdiction Network's *Global Status Report 2019* (*available at* https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf) questions the merits of the traditional approach with respect to internet jurisdictions and asserts that questions of internet jurisdiction be answered by weighing competing national interests.

forth in this *Commentary* serve to guide readers in determining which nation's laws should apply in a given context. The following diagram illustrates a process for applying the six Principles.



Principle 1: A nation has nonexclusive jurisdiction over, and may apply its data protection and privacy laws to, natural persons and organizations in or doing business in its territory, regardless of whether the processing of the relevant personal data takes place within its territory.

Comment a: Principle 1 focuses on the location of data subjects and organizations, as opposed to the location of data processing, which is the subject of Principle 2.[15] Both Principles are based on the general rule that all persons, with the possible exception of those enjoying diplomatic immunity, within the territorial boundaries of a nation must comply with the laws and legal processes of that country.

Comment b: The starting point is to ask where the organizations or natural persons who control personal data, whether their own or others, are established. That location determines the jurisdiction and the applicable law for any processing of personal data. Conversely, if there is no sufficient connection between a nation and such data subject or organization, the data is not subject to that nation's jurisdiction and laws. That leaves open the

15. This basic approach is in line with the European Data Protection Board (EDPB) Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)—Version after public consultation (adopted on 12 November 2019), *available at* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf). That said, this Principle is not limited to the GDPR, but is grounded in fundamental principles recognized in international law and is thus broadly applicable.

question of which jurisdiction and laws govern such data processing activities. The answer to that question is addressed by Principle 2. Consequently, this *Commentary* accepts the possibility that different jurisdictions and laws could apply to data subjects or organizations that are in one jurisdiction on the one hand, and to parties that process such data but have no other contact with that jurisdiction, on the other.

Comment c: Under existing law, nations have a sovereign right to "territorial" and "political" independence, and there shall be no interference "in matters which are essentially within the domestic jurisdiction of any state."[16] Accordingly, the only restrictions on the rights of nations are either by consent of the nation or by agreed international norms of conduct. Nor is there room for an argument that cyber activities belong to a lawless "global domain" and that it "lacks physicality and is virtual in nature." After all, "[c]yber activities occur on territory and involve objects, or are conducted by persons or entities, over which States may exercise sovereign prerogatives . . . although cyber activities may cross multiple borders, or occur in international waters, international airspace, or outer space, all are conducted by individuals or entities subject to the

16. U.N. Charter art. 2.

jurisdiction of one or more States."[17]

Comment d: Among those matters that are essentially within the rights of a nation is the power to confer or withhold citizenship, residence, or any other type of legal status that conveys upon such data subjects and organizations certain varying rights and obligations.[18] Generally, all citizens, residents, and persons with another legal status within a nation are obligated to comply with laws that compel them to appear before an authority, to produce information, or to suffer penalties for failing to do so. Correspondingly, citizens, residents, or persons with another legal status have an expectation that their nation(s) will protect the rights that it (or they) afford them.[19] Likewise, organizations that engage in purposeful activity (e.g., processing) in the jurisdiction of the sovereign should generally be obligated to comply with a nation's laws and regulations when processing personal information.

Comment e: In the context of such natural persons or organizations within its territory, a nation generally has the right to exercise jurisdiction

---

17. SCHMITT, *supra* note 13, at 11.

18. *See* GERARD-RENÉ DE GROOT, ELGAR ENCYCLOPEDIA OF COMPARATIVE LAW, NATIONALITY LAW, 476–92 (2006).

19. *Cf.* Charter of Fundamental Rights of the European Union art. 8(1), 2010 O.J. C 83/393 (emphasis added): "*Everyone* has the right to the protection of personal data concerning him or her."

over and apply its laws to the control over or the targeting of personal information.[20] By exercising jurisdiction and applying its laws, a nation defines the scope of data subjects' rights and the integrity of the personal data itself, irrespective of whether the data belongs to its own data subjects or other nations' data subjects.[21]

Comment f: Insofar as it refers to personal data belonging to an organization or a natural person, Principle 1 addresses the organization and natural person as data controller in the sense of the GDPR, i.e., as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[22]

Case Study 1: A multinational headquartered in Europe becomes subject to a litigation in New York that seeks the disclosure of personal data in the possession, custody, or control of both U.S. and German affiliates as well as U.S. and German employees of that multinational. Here, both the United States and

---

20. SCHMITT, *supra* note 13, at 16.

21. *Compare* GDPR, *supra* note 3, Recital 14 *with* Singapore's Personal Data Protection Act of 2012, which exempts public authorities from that law's requirements, and Malaysia's Personal Data Protection Act of 2010, which applies only to commercial transactions and does not apply to its Federal and State governments.

22. GDPR, *supra* note 3, art. 4(7).

Germany may assert personal jurisdiction over and apply their laws to the personal data that reference natural persons who are named parties in the proceedings and who are located in their territory. To the extent other natural persons work for the named parties in the proceedings, those parties are to be considered as co-controllers for the purpose of the proceedings. Depending on where the parties are established, U.S. or German jurisdiction and laws may apply to the respective personal data. However, as shown below, Principle 6 would accommodate discovery in the U.S. court proceeding of a foreign data subject's personal data, at least to the extent that appropriate measures are taken to protect the data and limit its use and dissemination to the extent feasible.

Case Study 2: A Singapore company remotely tracks the purchasing habits of Brazilian customers in order to provide them with targeted advertising materials. The analysis of the purchasing habits amounts to monitoring of the behavior of natural persons in Brazil. In that context, Brazil alone has an interest in the personal information of natural persons on its territory and might rightly assert jurisdiction over and apply its laws to the processing of the personal data by the Singapore company, which has possession, custody, or control over the personal information of Brazilian data subjects.

Comment g: Both the data control and the monitoring or collection of personal data must have a sufficient nexus with the territory of the nation asserting jurisdiction and applying its laws. For data monitoring and collection, that criterion is straightforward and merely requires the presence of the data subject in the respective jurisdiction. As GDPR Article 3(2) asserts,[23] a nation may assert jurisdiction over an entity that monitors the behavior of natural persons within its borders or that directs a marketing campaign to natural persons into a country, and thereby collects the personal data of those who respond to the campaign. Although the organization in question may not be physically established within the nation, its activities nonetheless reach into the nation and directly affect natural persons within it. For data control, things are more complex. GDPR Article 3(1) speaks of the "establishment" of a controller in the jurisdiction, defined as the effective and real exercise of activities through stable arrangements, irrespective of the legal form of such arrangements.[24] That nexus or establishment should be more than minimal.[25] Indeed, some commercial activity

23. GDPR, *supra* note 3.

24. *Id.*, Recital 22; Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság, ECLI :EU:C:2015:639, ¶ 28.

25. *Cf.* Case C-191/15, Verein für Konsumenteninformation v Amazon EU Sàrl, ECLI:EU:C:2016:612, ¶¶ 76–77.

led by a foreign data controller entity in another country may be so far removed from the ordinary course of business data processing by this entity that the existence of such commercial activity should not be sufficient to subject that data processing to the jurisdiction and laws of that other country.[26] Consider a variant of the Case Study 1 above: If Human Resource (HR) data of employees of a U.S. affiliate that is a party in the proceedings is stored on a group server in France and can be downloaded by the U.S. affiliate in the ordinary course of business, the mere location of Information Technology (IT) infrastructure should not provide a sufficient nexus to France for it to apply its jurisdiction and laws to such HR data when it is produced in the New York litigation.

Comment h: Likewise, a foreign data controller should not become subject to a country's jurisdiction and laws simply because it chooses to use a processor in that country.[27] The processing is carried out in the context of the controller's own activities, and the processor is merely providing a processing service. Therefore,

---

26. EDPB Guidelines 3/2018, *supra* note 13, at 10.

27. This principle uses the term 'processor' in the same way as that term is defined by the GDPR: "A 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." GDPR, *supra* note 3, art. 2(8). Here too, this Principle is not limited to the GDPR, but is grounded in fundamental principles recognized in international law and is thus broadly applicable. *See supra* note 15.

while the processor may be subject to that country's jurisdiction and laws regarding its own data processor obligations, as governed by Principle 2, this should not cause the foreign controller, or the data itself, to become subject to the data controller obligations of that country.[28] To take the variant of the Case Study 1 a step further: Consider that the HR data of employees of a U.S. affiliate that is a party in the proceedings is stored on a cloud server operated by an external data processor in Ireland. While the operations of that processor may be subject to Irish jurisdiction and laws, the U.S. HR data itself should not.

Comment i: The jurisdiction over personal data afforded by Principle 1 is not necessarily exclusive. In circumstances where a natural person has dual or multiple citizenship, residence, or other legal status, each nation may claim jurisdiction over and apply its laws to a spectrum of issues ranging from privacy to security to the personal data of that natural person. Similarly, as illustrated in the

28. For the EU now supported by EDPB Guidelines 3/2018, *id.*, at 10–11, where the EDPB also refuses to qualify the offering of a processing service as targeting of data subjects in that country. *But see* Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González, ECLI:EU:C:2014:317; and Art. 29 Data Protection Working Party, Update of Opinion 8/2010 on applicable law in light of the CJEU (Court of Justice of the European Union) judgment in Google Spain, Dec. 16, 2015, *available at* https://iapp.org/media/pdf/resource_center/wp179_CJEU-Google-Spain_12-2015.pdf.

comments to Principle 3 below, multiple jurisdictions may be able to properly assert jurisdiction when such data crosses international borders. For example, if a person in State A contracts with a person in State B to engage in activities that have a substantial effect in State C, all three States may have jurisdiction over the personal data of the person in State A.[29]

Comment j: Because of global economic and communications interconnectedness and the mobility of citizens among countries, dual or multiple citizenships and cross-border data transfers are common. While globalization and international legal harmonization have resulted in an increased compatibility with the regulatory frameworks adopted by various nations, there remain significant differences, some of which are exacerbated by competition over data and geopolitical instability. Because of such differences, dual or multiple citizens are subject not only to multiple laws affecting or protecting their privacy, but to some laws that may be conflicting.

Comment k: Courts may resolve such conflicts between the laws of two or more nations by defining data control not in the abstract, but in a specific context. As demonstrated by Case Studies 1 and 2, the context helps identify the

29. *See* SCHMITT, *supra* note 13, at 56.

purposes and means of the processing of personal data and, ultimately, who determines such purposes and means. Another factor courts should consider is the affirmative actions of the natural persons and organizations in question. The choice of a natural person or organization to establish itself predominantly in a particular jurisdiction and avail itself of the rights and benefits of such a jurisdiction, or a decisive and informed step to hand over its data to another jurisdiction, should count toward the primacy of a certain jurisdiction and its laws.

Case Study 3: A person received two citizenships at birth, one from its parents and one from its country of birth. As an adult, the choice to reside in one of the two countries could reflect an understanding of that country's laws and mores, a sympathy for the jurisdiction's manner of justice, and an implicit choice of preference for that country over the other country of citizenship. Further, if the country of the residence is neither of the countries of citizenship, questions of jurisdiction may need to be resolved by balancing all the factors favoring the applications of the jurisdiction and laws of the country of residence against the factors that favor the application of the jurisdiction and laws of the nation(s) of citizenship. Location of residency need not be the sole factor: other affirmative decisions or statements by a natural person may tilt the balance when considering choice of

jurisdiction and thereby demonstrate which country has the greater sovereign interest in the matter.

Principle 1 does not apply to packetized data that is in transit across borders under Principle 5. Principle 1 is also limited by Principle 6 with respect to data that is responsive in foreign legal proceedings. Principle 1 thus focuses on the conduct of actors within its territorial boundaries.

Principle 2: A nation usually has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, the processing of personal data inextricably linked to its territory.

Comment a: Principle 2 focuses on the location of data processing, as opposed to the location of data subjects and organizations, which is the subject of Principle 1. Principle 1 rests upon the proposition that a state may exercise its jurisdiction over and apply its laws to those who control personal data, or whose personal data is targeted, provided they are established in its territory. Where this is not the case, Principle 2 determines under which conditions the processing activities of a data processor fall within the application of a state's jurisdiction and laws.

Comment b: Principle 2 accepts the idea that "processing" may be broadly defined and is not limited to analytic uses of data. As the GDPR explains, data processing may be "any operation or set of operations which is performed on personal data or on sets of personal data, whether or

not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[30]

Comment c: As with Principle 1, the data processing must have a sufficient nexus with the territory of the nation for it to assert its jurisdiction and apply its laws. This Principle may not apply when the level of processing is merely ministerial or incidental to activities of a foreign data controller that predominantly take place outside the country. For example, the Court of Justice of the European Union has recognized that if the activities of an entity in a country are "inextricably linked" to the processing of data carried out by a foreign data controller, that country's laws may apply to the data processing by the foreign controller.[31] Where, for example, the contact with a country is limited to the mere collection of data, without any further processing in the territory, that country

30. GDPR, *supra* note 3, art. 4(2).

31. Case C-131-12, *Google Spain SL*, ¶ 56. *Cf.* also Advocate General's Opinion in Case C-501/17, Google v Commission Nationale de l'Informatique et des Libertés, ECLI:EU:C:2019:15, of Jan. 10, 2019, rejecting a request that search requests outside the EU should be affected by a French request to de-reference search results, thereby limiting the potential extraterritorial effect of European data privacy law in a global context such as the internet.

should ordinarily defer to the jurisdiction with the greater interest in the data subject, which would usually be where the data controller principally resides (as illustrated in Comment i to Principle 1 above). For the same reasons, packetized data that is in transit across borders should not be subjected to Principle 2 but should be governed by Principle 5.

Comment d: As with Principle 1, the jurisdiction afforded by Principle 2 over personal data is not necessarily exclusive. The practical application of Principle 2 is to acknowledge the sovereign right of a state to regulate activities within its borders, while at the same time preserving the rights of a nation to exercise jurisdiction over and apply its laws to its citizens, residents, or data subjects otherwise closely connected to it. Courts may resolve potential conflicts between the laws of two or more nations by defining data processing not in the abstract but in a specific context, by asking which purpose the processing serves.

Case Study 4: Suppose, for example, that a German data subject completes an online survey in which a U.S. company in Nebraska collects the subject's personal data in order build a profile of consumers in the data subject's home country. This case falls squarely into the category of data targeting governed by Principle 1, which affords jurisdiction and

applicable law to Germany. Here, Principle 2 recognizes that Germany's interest in the collected data is greater than that of Nebraska. One arrives at the same answer by identifying the main purpose of the data processing, which in this instance is the profiling in the data subject's home country and not the ministerial data analytics performed in the U.S.

Comment e: If full effect is given to this Principle and to Principle 1, there should be no need for rules requiring data users to store their data only domestically.

Principle 3: In commercial transactions in which the contracting parties have comparable bargaining power, the informed choice of the parties to a contract should determine the jurisdiction or applicable law with respect to the processing of personal data in connection with the respective commercial transaction, and such choice should be respected so long as it bears a reasonable nexus to the parties and the transaction.

Comment a: Principles 1 and 2 recognize that a state may exercise its jurisdiction over and apply its laws to data in the possession, custody, or control of organizations and data subjects, or to data that is subject to targeting activities, as long as there is a sufficient nexus to that state's territory. Principle 3 stipulates that parties should, within certain limits, be allowed to contract on the jurisdiction and data protection law applicable for the processing of their data and for data

protection breaches in connection with their contract. As such, this Principle recognizes that natural persons ought to have the right to determine the uses of their personal information, and that within such right should be the right to consent to the jurisdiction or the application of the laws of a foreign nation in relation to their data so long as the chosen law bears a logical relationship to the parties and the transaction. The practical relevance of Principle 3 is to respect the parties' common intentions, to offer a high degree of certainty in commercial contexts, and ultimately to facilitate access to justice by allowing for a direct determination of the law applicable to personal information without reference to jurisdictional questions. This Principle thus implicates private law, whereas the first two Principles concerned public law and the right of states to assert sovereignty over people, information, and activities that are within their territorial control or that assert a substantial effect within their territory.

Comment b: The openness of a country's law to party autonomy when it comes to choice of jurisdiction and law will depend in part on its underlying conception of data privacy. Party autonomy is an established fundamental principle of private law. However, stricter requirements for individual consents to data processing apply, and burdens for a valid choice of law are

higher where such choices effectively lead to waivers of existing data privacy protections and, as in the EU, data protection laws give effect to a constitutional, personal, or other fundamental right to informational self-determination.[32]

Comment c: However, it is submitted that there should be room for private autonomy in the data privacy context.[33] The right to informational self-determination is not absolute but must be balanced against other freedoms, in

---

32. *E.g.*, GDPR, *supra* note 3, Recital 1 ("The protection of natural persons in relation to the processing of personal data is a fundamental right.") and 32 ("Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement . . . .").

33. In Europe, the CJEU has not yet ruled on the question, and current doctrine and practice appear divided. Under the old Data Protection Directive 95/46/EC, 1995 O.J. (L 281), the Article 29 Data Protection Working Party had opined "that the applicability of European privacy law cannot be excluded by a unilateral declaration or contractual agreement" (Opinion 02/2013 on apps on smart devices, Feb. 27, 2013, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf). *Cf.* also the overview in Maja Brkan, *Data Protection and Conflict-of-Laws: A Challenging Relationship*, 2 EUROPEAN DATA PROTECTION L. REV. 324 (2016). The discussion in Germany provides a good illustration of the debated issues: Judgments of the Landgericht Berlin [LG][Regional Court], Mar. 6, 2012, AZ. 16 O 551/10 (enforcing an choice of applicable data protection law) and the Verwaltungsgericht Schleswig-Holstein [VG][Administrative Trial Court] in Facebook Ireland Ltd v Independent Data Protection Authority of Schleswig-Holstein, Feb. 14, 2013, 8 B 60/12 (rejecting such a choice); GDPR, *supra* note 3, art. 3, *in* KOMMENTAR ZUR DATENSCHUTZ-GRUNDVERORDNUNG (Jürgen Kühling, Benedikt Buchner eds., 2017), at nn.105–06.

> particular, economic freedom.[34] Stated differently, a natural person may be incapable of contracting away all his or her fundamental data rights, but the same person should be allowed to waive such rights under specific circumstances and for a particular purpose. Further, the principle of mutual regard for the jurisdiction of sovereign states provides that nations may apply their laws to data where such data has been designated as governed by their jurisdiction with legally valid consent. To decide differently would mean to assimilate every data subject to the weaker status of a consumer worthy of special protection, and to indiscriminately accept an overriding public interest of one sovereign state in all areas of data privacy law, even where it regulates the relationship between private parties with comparable bargaining power, as is the case in commercial contexts.[35] The benefits of the modern information society can only be

34. Accepted by the GDPR, *supra* note 3, itself (*cf.* Recitals 2, 5, 7, and 9). Significantly, the seminal Volkszählungsurteil ("Census Verdict") of the German Federal Constitutional Court, which created the German constitutional right to informational self-determination, accepts that the guarantee of this right has its limits. Natural persons have no absolute, unrestricted control over their data. Rather, they participate through communication in their respective social contexts. Accordingly, information is a social phenomenon that cannot be exclusively assigned to an affected individual (Census Verdict, BVERFGE 65, 1; AZ. 1 BVR 209/83 *et al.*, Dec. 15, 1983, at n.174).

35. *Cf.* WOLFGANG HOFFMANN-RIEM, INFORMATIONELLE SELBSTBESTIMMUNG IN DER INFORMATIONSGESELLSCHAFT—AUF DEM WEG ZU EINEM NEUEN KONZEP DES DATENSCHUTZES 531–532 (1998).

effectively realized if one accepts some of the risks that go along with it. To consider all jurisdiction and choice-of-law agreements in the data privacy field as inherently unfair would appear anachronistic, given the nature of global commerce. It would also amount to disregarding commercial practice where agreements on jurisdiction and applicable law commonly occur and regularly do not treat data protection issues separately from other contractual issues.

Comment d: A specific individual waiver of rights under the jurisdiction or laws of a foreign sovereign does not per se negate the right of that sovereign to exercise sovereignty over certain data regardless of the location of such data. While Principle 3 stipulates that there should be room for a choice of jurisdiction or law regarding personal data, even where such a choice acts as a waiver of protections of another jurisdiction, it recognizes that the implied derogation of other potentially applicable jurisdictions or laws is limited where such derogation would be contrary to another sovereign's overriding national interests. Accordingly, Principle 3 remains subject to overriding mandatory provisions which, in the absence of choice, would have been applicable according to Principles 1, 2, and 6. This Principle accepts that in such cases, another jurisdiction or law may apply alongside the agreed one, even though they deal with the same data processing. As noted

earlier in the discussion of comity, however, the application of such overriding national provisions should be the result of a balancing of all interests involved and be construed narrowly.

Comment e: In order to ensure the predictability of the agreement's validity, Principle 3 does not subject the choice of jurisdiction or law to any requirement as to form, unless otherwise agreed by the parties. Beyond this, it leaves questions of existence and substantive validity of the choice to the provisions of the chosen law.[36] This appears adequate because it gives effect to the parties' choice, and because the meaning of consent, and the requirements for a valid consent, differ among jurisdictions. For example, Article 4(11) of the GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes."[37] In contrast, in the U.S, the most

36. Hague Conference on Private International Law, Hague Principles on Choice of Law in International Commercial Contracts, art. 5 (March 19, 2015), https://www.hcch.net/en/instruments/conventions/full-text/?cid=135 [hereinafter Hague Principles]; International Law Association, Protection of Privacy in Private International and Procedural Law, at 20, 30–31, (2018), https://www.ila-hq.org/images/ILA/DraftReports/DraftReport_Privacy.pdf.

37. To be freely given, the Article 29 Working Party Guidelines on Consent under Regulation 2016/679 of April 16, 2018, as endorsed by the EDPB, stress the need for free choice, and find that free choice is lacking if there is an imbalance of power in the relationship between the data subject and the controller (such as the employer-employee relationship) and potentially invalid if a service would be denied to the data subject unless he or she gives consent.

fundamental principle for consent is notice, as "without notice a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[38] Accordingly, recurring to the applicable procedural law of the court, let alone to the substantive requirements of the derogated jurisdiction or law, would

---

Specificity requires granular detail: "If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. [. . .] When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e., the separation of these purposes and obtaining consent for each purpose." (https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf) Informed consent requires that all relevant information be provided regarding that consent in plain and clear language. And unambiguous consent requires a clear expression of intent or clear affirmative action by the data subject. Finally, GDPR, *supra* note 3, art. 7(3) requires that consent may be withdrawn as easily as it was given.

38. In the United States, there is no single, comprehensive national law or policy (except with respect to protecting children) regulating the use of personal data or defining consent. There are many federal and state privacy laws with varying definitions, including, most prominently, the Federal Trade Commission Act. "While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information: identification of the entity collecting the data; identification of the uses to which the data will be put; identification of any potential recipients of the data; the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information); whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data." FEDERAL TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7–8 (1998).

endanger the goal of decisional harmony.

Comment f: Principle 3 allows both *ex ante* and *ex post* choices of the jurisdiction and the law applicable to personal data.[39] This is relevant in particular where the laws of a country qualify obligations arising out of violations of privacy and personality rights as noncontractual in nature.[40]

Comment g: In order to protect natural persons who lack bargaining power from unexpected and potentially harmful effects of a specific choice of jurisdiction and law, Principle 3 proposes two limitations.[41]

First, it accepts a free choice of jurisdiction and law only for commercial transactions in which the contracting parties have comparable bargaining power.[42] The commercial nature of a transaction should be defined on a case-by-case basis, having due regard to the nature and aim of a particular contract in the context of trade or professional activity, and not in the abstract by reference to the subjective situation of the person concerned. This is because the same person may act as a commercial operator in relation to certain

---

39. Note that certain jurisdictions may have issues with *ex ante* choices of law for tortious events, such as violations of personality rights.

40. International Law Association, *supra* note 36, at 23.

41. *Cf.* Principle 4, *infra*.

42. *Cf.* Hague Principles, *supra* note 36, art. 1(1).

transactions, and as a consumer in relation to others. It is also proposed to construe exceptions from the commercial nature of a transaction narrowly and limit them to transactions solely for the purpose of satisfying a natural person's own needs in terms of private consumption. The qualification of a transaction should also be irrespective of whether the respective activities are planned for the present or future.[43]

Second, a choice of jurisdiction and law should bear a reasonable nexus to the parties and the transaction. This is of particular importance in jurisdictions where obligations arising out of violations of privacy and personality rights are qualified as noncontractual in nature.[44]

Comment h: A choice of jurisdiction and law may be express or implicit. If the latter, the choice should appear clearly from the provisions of the contract or the circumstances of the case, whereby such circumstances should accord with practices that the parties have established between themselves.[45] Where

43. In line with the CJEU's case law on the Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters: Case C-269/95, Francesco Benincasa v Dentalkit Srl, ECLI:EU:C:1997:337, ¶¶ 15–16; Case C-464/01, Johann Gruber v Bay Wa AG, ECLI:EU:C:2005:32, ¶¶ 36–45. *Cf.* also International Law Association, *supra* note 36, at 20.

44. International Law Association, *supra* note 36, at 24.

45. *Cf.* Hague Principles, *supra* note 36, art. 4, at 20, 30.

data is transferred cross-border in a commercial context, Principle 3 stipulates an assumption of an implied choice of jurisdiction and law in favor of the place of destination. For example, a natural person who freely and voluntarily transfers his or her personal data, or has his or her personal data transferred, for commercial purposes to a nation other than one that would otherwise claim jurisdiction, can be assumed to have consented to the jurisdiction and law of that other sovereign nation for all purposes reasonably expected to be related to such transfer. The practical relevance is to provide certainty to the handling of the large data volumes freely transferred on a regular basis between jurisdictions. Accordingly, this Principle acknowledges that a single cross-border data transfer can include many different purposes and treats them all in the same way as long as it can be assumed that the data subject could, at the time of the transfer, reasonably be expected to know the potential that such purposes could materialize.

Comment i: For comparable bargaining power to exist between the parties, both parties should have knowledge, or should be informed, of the implications of a choice of jurisdiction or law, in particular where it leads to consent to data processing, and to a waiver of protections that would otherwise be afforded by the derogated jurisdiction or law. And such

knowledge may reasonably be assumed among corporations, which are expected to have competent counsel. Absent such comparable bargaining power, the chosen jurisdiction or law should not claim primacy over the jurisdictions or laws which would otherwise be applicable.

Case Study 5: While residing in France, Subject A signs a contract with Subject B, who resides in New York, to perform services in Brazil and attaches his work history and other personal information to the contract, which B then forwards to Customer C, who is in Brazil, where the contract is to be performed. All parties know or should know that courts in New York allow complete pretrial discovery practices, and they nonetheless agree that the courts of New York shall have jurisdiction and the laws of New York will apply to any disputes "regarding the contract's interpretation and performance." A dispute later arises in Brazil regarding the lawfulness of the contract under Brazilian law. Because the nature and aim of the transaction is that of a trade or professional activity, the selection of New York law, and the corresponding derogation of French law, does not impinge on France's sovereign authority. Similarly, settled principles of international law show that Brazil has jurisdiction over all three parties to the extent the effects of their actions materialize in that jurisdiction. As far as the dispute concerns the lawfulness of the contract under its laws,

rather than the performance of the contract, Brazil retains the primary interest, and the courts of New York may, as a prudential matter, refrain from exercising jurisdiction over that issue, or hold any dispute concerning the lawfulness of the contract under the laws of Brazil in abeyance pending the outcome of the issue by the Brazilian administrative or judicial authorities responsible for deciding that issue.

Case Study 6: A U.S. company in Pennsylvania offers an online service that helps doctors stay abreast of treatment options for certain diseases, but it will only sell those services to doctors who accept its terms and conditions online. Its terms and conditions include a jurisdiction and choice-of-law clause in favor of Pennsylvania law with respect to all disputes involving the service. A medical doctor in Germany accordingly submits to the jurisdiction and laws of Pennsylvania for purposes of a specific processing or use of her own personal data collected in dealing with the company. Under the rules of Pennsylvania, this consent is valid; under the GDPR, however, the consent might be considered invalid because it could be considered to amount to a coercive waiver of the doctor's data privacy rights. To the extent that the German doctor enters into the transaction with the Pennsylvania company in her professional capacity, and no data of third parties such as patients are affected, her ability to seek advice before

entering into the agreements and her corresponding right to choose the applicable jurisdiction and law must implicate her ability to give consent.

Principle 4: Outside of commercial transactions, in which a natural person freely makes a choice, a person's choice of jurisdiction or law should not deprive him or her of protections that would otherwise be applicable to his or her data.

Comment a: Like Principle 3, Principle 4 recognizes that every affirmative choice of jurisdiction or law may imply a derogation of protections and standards that may be considered unacceptable by another jurisdiction for a variety of reasons, ranging from consumer protection to protection of sovereign national interests. The practical application of Principle 3 limits the free choice of jurisdiction or law for data to the commercial context and thereby provide certainty and flexibility where the parties to a contract have comparable bargaining power, and data subjects can be expected to foresee and understand the consequences of their choice while maintaining the protections afforded by substantive laws.

Comment b: Although both Principle 3 and Principle 4 recognize that every affirmative choice of jurisdiction or law may imply a derogation of protections, this Principle also recognizes that some cross-border movements of information do not involve any affirmative

or, for that matter, any conscious decisions about applicable law. Specifically, Principle 4 speaks directly to the social communications between natural persons where the cross-border transfer of personal information is merely incidental to the purpose, and there is nothing in the content to trigger any State's sovereign interests or concerns. In other words, this is the flip side of Principle 3 and involves noncommercial transactions. Here, data subjects, assuming they think about it at all, would presumably expect that they would enjoy all the rights and freedoms that their native citizenship allows them; and except when such communications betray an effort or at least an intent to violate the laws of a given jurisdiction, no sovereign has a cognizable concern that would warrant upsetting the sovereign rights of the person's State of citizenship.

Comment c: There are different approaches to distinguishing commercial and noncommercial uses of data. At the highest level, noncommercial use includes artistic, scholarly, educational, personal, family, or other uses, including social media, when they are not associated with the professional or commercial activities of a natural person.

The 2009 Creative Commons report *Defining Noncommercial*[46] lists nine qualitative factors for analyzing noncommercial use.

i. Perceived economic value of the content;

ii. The status of the user as an individual, an amateur or professional, a for-profit or not-for-profit organization, etc.;

iii. Whether the use makes money (and if so, whether revenues are profit or recovery of costs associated with use);

iv. Whether the use generates promotional value for the creator or the user;

v. Whether the use is personal or private;

vi. Whether the use is for a charitable purpose or other social or public good;

vii. Whether the use is supported by advertising or not;

viii. Whether the content is used in part or in whole; and

ix. Whether the use has an impact on the market or is by a competitor.

Comment d: In the commercial context, a choice of jurisdiction or law and related consent to data processing may be more readily assumed than in the noncommercial context.

---

46. *Available at* https://mirrors.creativecommons.org/defining-noncommercial/Defining_Noncommercial_fullreport.pdf (last visited April 20, 2020).

However, as the Comment g. to Principle 3 demonstrates, consent implied or considered given in the commercial context should be limited to such processing and use of personal data that can be considered reasonably related to the fulfilment of the commercial purpose. Consent for processing and use of personal data in excess of what is required for the fulfillment should not be implied or considered given by the operation of law. Information should be available to the natural person regarding the extent and scope of the consent implied or considered given in the commercial context.

Case Study 7: Assume the same facts as those set out in Case Study 5, and also assume that A wrote several letters and emails to his friends and business associates discussing the contract and his understanding of what it involved, and assume that he also maintained a social media account on which he shared with his friends in France his unfavorable views about the court system and elected leaders in New York and his interest in traveling to and working in Brazil. In the ensuing litigation in New York, his opponents seek discovery of all communications he has had relating to the contract and his work in Brazil. In this situation, A's letters and emails to his friends and business associates relating to his understanding of the contract should be discoverable in New York because he has consented to the jurisdiction of its courts and laws. Similarly,

whether the identity of his friends and business associates must be disclosed should be resolved in the first instance by the courts in New York while giving due regard to the sensitivity of that personal data under the laws of France and their importance, or lack thereof, to resolving the pending dispute. Conversely, on the facts as stated, there is no apparent reason why the court should allow discovery of the content of A's social media accounts. A's social media is noncommercial in nature, and he has not consented to disclosure of that information in New York, or anywhere else. Also, while his views on politicians, courts, and foreign travel may be interesting, they are not on their face sufficiently relevant or important for the courts in New York to allow discovery of them in contravention to the laws and policies of Brazil.

Comment e: Similarly, the Advocate General's January 2019 Opinion in the *Google v. CNIL*[47] matter provides an excellent example of the limits of extraterritorial jurisdiction under the EU Data Protection Directive in the context of private usage of internet search engines. That matter concerned a request by certain natural persons that Google delete all links to them on a worldwide basis. After Google refused to comply with a formal notice from the CNIL (*Commission Nationale de l'Informatique*

47. Case C-507/17, Google v. Commission Nationale de l'Informatique et des Libert. . .s, ECLI:EU:C:2019:15.

et des Libert. . .s) and instead limited its de-referencing to the 28 Member States, the CNIL imposed a substantial fine, which Google appealed to the Court of Justice of the European Union. In January 2019, the Advocate General issued his opinion recommending that the Court reject the CNIL's view. In short, he found that an expansive application of the extraterritorial jurisdiction to the right to be forgotten is untenable. That right, he reasoned, must be balanced against the interests of other people and nations in accessing information. He thus concluded that "if worldwide de-reference were possible, . . . persons in third States would be prevented from accessing information, and in turn, . . . third States would prevent persons in the EU Member States from accessing information." Although he reserved the possibility that worldwide de-referencing might be warranted in some situations, he clearly believed that the Google matter was not such a situation.

More specifically, the Advocate General first observed that the provisions of the EU Data Protection Directive did not expressly address the territorial scope issue. In his view, a distinction should be made based on the location of the search request, such that if a search is input outside of the EU, the results should not be impacted by the de-listing of the search results in the EU.

He further explained that the EU Treaties apply to EU Member States and that EU law should not apply beyond the territory of the EU Member States. The Advocate General recognized that EU law may have extraterritorial effect, but such effect only applies in exceptional cases, such as in competition law or trademark law cases affecting the EU internal market.

Finally, the Advocate General stressed that the right to be forgotten must be balanced against other fundamental rights such as the legitimate public interest in accessing the information sought, and that the audience concerned is not worldwide but instead European. In his view, the CNIL's approach entailed a risk that people in non-EU countries would be prevented from accessing information and, in turn, that non-EU countries could prevent people in the EU from accessing information. Accordingly, "a race to be bottom" could occur to the detriment of the freedom of expression at both the European and worldwide levels.

Principle 5: Data in transit ("Data in Transit") from one sovereign nation to another should be subject to the jurisdiction and the laws of the sovereign nation from which the data originated, such that, absent extraordinary circumstances, the data should be treated as if it were still located in its place of origin.

Comment a: When organizations and natural persons

interact across borders, they create potential data transfer situations where the data subject is located in one country and the entity possessing the data is in another. This is because through the course of doing business and defending against claims, data often leaves one nation and crosses into another. Principle 5 (which may be thought of as dealing with "data in motion") rests upon the proposition that in such instances, the jurisdiction and law of the nation in which the person or entity initiating the transfer resides shall be treated as the originating jurisdiction and therefore govern the data until it reaches its country of destination. Where there is a choice of jurisdiction or law, such choice shall be recognized in lieu of the jurisdiction and law of the place of origin.

Comment b: Data transfers may be initiated by different parties depending on the circumstances. This Principle applies equally to data that is placed in transit by the data subject and data placed in transit by a data custodian. Distinguishing between these two individuals would create an uneven playing field and an unwieldy regulatory structure.

Comment c: Data in Transit should be entitled to transit without observation, alteration, or abridgement except for national security or law enforcement purposes. Such Data in Transit should be marked as such, including

information as to its place of origin and final place of destination. This Principle recognizes that even when a sovereign has the power to assert itself with respect to data in all ordinary cases, its interest in particular data or data sets will be minimal, if not wholly nonexistent. In such circumstances, mere respect for the laws and sovereign interests of other nations strongly suggests that the data's transient "host" decline from interfering with the free flow of data across its national borders.

Comment d: Data in Transit for commercial, personal, or governmental purposes shall be presumed to have a lawful purpose and should be transferred unmolested by entities, governments, or natural persons. For example, data lawfully placed in transit in Country A may be carried by fiber-optic cables that pass through Country B on the way to their intended destination in Country C, and no party may have "intended" or even been aware of the data's contact with Country B. In that situation, established principles of International Law recognize that Country B has sovereignty over the data as it passes through its territory.[48] Despite having the power, however, to act with respect to the data while it is in transit, except in limited circumstances where a country may have an overriding interest or even an obligation

48. SCHMITT, *supra* note 13, at 13–14; *cf. id.* at 33.

under International Law to act with respect to such data, it should refrain from impeding the flow of data through its territory.[49]

Comment e: This Principle does not address directly the legal standards for and potential conflicts related to national security surveillance and law enforcement access to Data in Transit. It clarifies, however, that where Data in Transit passes temporarily through a country with less restrictive laws regarding access than those of the county of origin, national security and law enforcement authorities may not take advantage of those less restrictive laws to access the data.

Principle 6: Where personal data located within, or otherwise subject to, the jurisdiction or the laws of a sovereign nation is material to a litigation, investigation, or other legal proceeding within another sovereign nation, such data shall be provided when it is subject to appropriate safeguards that regulate the use, dissemination, and disposition of the data.

Comment a: A fundamental right of all people is to have their claims adjudicated by a fair and impartial tribunal and to able to defend against claims made in proceedings before such tribunals. Nations have broad discretion in developing tribunals and procedures that give meaning to that fundamental right and

49. *Id.* at 33–34.

those tribunals. It therefore follows that the requirements of those tribunals are entitled to deference and respect by other nations.

Comment b: A fundamental right of all people is to have their health, safety, and welfare protected by the nations in which they reside and through which they traverse. When questions arise concerning possible law violations, all people similarly have a fundamental duty to respond to lawful inquiries from fair and impartial investigators. Here, too, nations have broad discretion in establishing investigative authorities and procedures that give meaning to the nature and scope of these duties. Those investigative procedures are entitled to the utmost deference and respect by other nations.

Comment c: It therefore follows that when courts or investigative authorities provide for the adequate protection of data transferred to the country of interest, then the data should be produced to the party that needs it, to the extent such data is relevant and material to the adjudicative proceeding or law enforcement investigation in question. Privacy laws should not restrict transfer where the data is adequately protected by appropriate safeguards.

Case Study 8: A U.S. federal agency issues a subpoena that seeks personal information about particular data subjects and relates to a law enforcement investigation the agency is

undertaking. The subpoena's recipient asks that the agency stipulate to protecting the data it produces from any public disclosure and to destroy or return the information at the end of the investigation. The agency declines to so stipulate, noting that it is subject to various statutes that preclude it from making the information it receives in investigations public, unless it first gives notice to the interested parties and gives them an opportunity to seek court-ordered protections. It also notes that the Federal Records Act and other laws regulate how it disposes of records at the end of its investigation. If the party then refuses to comply, a court may properly conclude that the personal data in question is adequately protected within the meaning of Principle 6. Similarly, a Supervisory Authority who receives a complaint from the data subjects about the transfer of personal data to a U.S. federal agency should consider the legitimate interests of the U.S. government in conducting the investigation and the statutory protections that apply to the data the agency receives in the course of its investigation.

Case Study 9: In a private action to enforce a contract, the defendant issues a request for production to the plaintiff demanding that it turn over documents containing personal data that is stored in the EU and pertain to EU data subjects. The plaintiff refuses to produce the requested information, claiming that it is forbidden from doing so because of the GDPR.

The defendant offers to limit its demand to documents that are uniquely in the EU and that are necessary and relevant, but adequate for the case. It also offers to stipulate to a protective order that commits it to securing the data, using it only for the litigation in question, to protect it from any further disclosures, and return or destroy the data at the end of the litigation to the extent it can do so consistent with its obligations to the client. On a motion to compel, a U.S. court may properly find that the defendant's offer does not risk any significant harm to data subjects, and that the plaintiff should therefore comply with the request. Similarly, a Supervisory Authority, if called upon to review the matter, may properly conclude there are adequate assurances that the data will be secured and that the defendant has properly applied data minimization principles to its request for data. It may therefore conclude that the risk of harm to data subjects is minimal, if not nonexistent.

Comment d: The complexities of commerce and transnational business arrangements on occasion give rise to multiple contemporaneous litigations or governmental investigations (or both) pending in various jurisdictions. While we believe that, as a general proposition, it is in the best interests of all concerned parties (and authorities) to cooporate on some level and work together to ensure that all matters proceed more or less in tandem, and to ensure that the end

results are, if not uniform, at least not inconsistent or mutually exclusive, we also realize that in some situations one or more of the parties may not think that cooperation or coordination is in its own best interest. In those circumstances, it may be incumbent on the presiding tribunals (in the case of litigation) and the responsible government authorities (in the case of investigations) either to "encourage" any reluctant party to cooperate or, where that is not possible, to exercise its powers to maintain progress in its pending matter and prevent any unjustified delay.

APPENDIX: DATA PRIVACY COMPLEXITY AND BACKGROUND

A. Origins of Data Privacy Concepts

What we mean today by data privacy begins in the modern era, roughly by the end of the 17th century, with the rise of the individual, the emergence of the modern, bureaucratically organized state, and the tensions between the two.[50]

It was not until well into the 19th century, mainly building upon the recognition of human rights in the French and U.S. constitutions, that the hitherto largely philosophical concept of individual privacy achieved legal effect. Two U.S. lawyers, Samuel Warren and Louis Brandeis, are credited with having first developed privacy protection into a coherent notion, conceptualized as "an instance of the enforcement of the more general right of natural persons to be let alone."[51]

In the early 20th century, the two main data privacy paradigms, the European and the American, evolved. As privacy law across the globe diverged, they remained motivated by a concern for governmental abuse of personal data. From the end of the 20th and by the beginning of the 21st century, the history of data privacy has been shaped by two developments: the appearance of new actors on the data privacy stage, in

---

50. For a more detailed history of information privacy, *cf.* Kai von Lewinski, *Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive, in* DATENSCHUTZ. GRUNDLAGEN, ENTWICKLUNGEN UND KONTROVERSEN 23 (Jan-Hinrik Schmidt & Thilo Weichert eds., 2012); Daniel J. Solove, *A Brief History of Information Privacy Law, in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE (Kristen J. Mathews ed., 2d ed. 2016), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271.

51. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193 (1890), at 205.

particular large private corporations with access to significant data in the banking, insurance, advertising, healthcare, and information technology industries; and the expansion of the internet and related information technologies. The latter led to an exponential growth of data volumes, de-localization of data processing through the development of encryption and cloud computing, and quickly shifting societal and cultural concepts of privacy.

B. Different Conceptions of Data Privacy

The foundations for the U.S. data privacy paradigm were laid by the Supreme Court rulings in the 1960s and 1970s. Building upon Warren and Brandeis' work and an earlier decision in *Griswold v. Connecticut*,[52] the Court in *Katz v. United States* defined the right to privacy by referring to a private vs. public dichotomy: "What a person knowingly exposes to the *public*, even in his own home or office, is not a subject of Fourth Amendment Protection [which provides broad limitations on the government's power to search and seize; added]. But what he seeks to preserve as *private*, even in an area accessible to the public, may be constitutionally protected."[53] In *Whalen v. Roe*, the Court then framed the U.S. data privacy paradigm as "individual interest in avoiding disclosure of personal matters."[54]

---

52. Griswold v. Connecticut, 381 U.S. 479, 484 (1965), finding the right to privacy to be enshrined in the "penumbras" of many of the ten amendments of the Bill of Rights.

53. Katz v. United States, 389 U.S. 347, 351 (1967) (emphasis added).

54. Whalen v. Roe, 429 U.S. 589, 599–600 n.26 (1977). The Court also identified a second individual "interest in independence in making certain kinds of important decisions" and characterized these decisions as dealing with "matters relating to marriage, procreation, contraception, family relationships, and childrearing and education." It noted that in these areas "it has

Around the same time, in 1983, the German Federal Constitutional Court in its seminal *Census Verdict* ("Volkszählungsurteil") created the German constitutional right to informational self-determination. Rooted in article 2 paragraph 1 (right of personality) and article 1 paragraph 1 (right to human dignity) of the German Constitution, such right guarantees, in principle, the power of natural persons to make their own decisions regarding the *disclosure and use* of their personal data.[55] The Court emphasized that it is not possible to limit the question of worthiness of protection exclusively to the nature of the information. Knowledge of the context in which data is used and collated is necessary to establish the importance of data and the admissibility of a restriction of the right to informational self-determination.[56]

By 1979, general data protections laws had been enacted in seven member states of the European Economic Community (Austria, Denmark, France, Federal Republic of Germany, Luxembourg, Norway, and Sweden). In three countries (Austria, Portugal, and Spain), data protection was incorporated as a fundamental right in the constitution. In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), the first legally binding international instrument in data protection, which became the foundation of the 1995

been held that there are limitations on the States' power to substantively regulate conduct."

55. Census Verdict, BVERFGE 65, 1; AZ. 1 BVR 209/83 *et al*., Dec. 15, 1983, at n.173. *Cf.* also Hans-Jürgen Papier, *Verfassungsrechtliche Grundlegung des Datenschutzes, in* SCHMITT, *supra* note 13, at 67.

56. *Census Verdict*, at nn.176–77.

European Data Protection Directive.[57] In the U.S., meanwhile, privacy protection receded. For example, financial privacy was curtailed throughout the 1970s. And in the 1980s, the U.S. Supreme Court decided a series of cases adopting a narrow view of what constitutes a protected reasonable expectation of privacy.[58]

Since the 1980s, the U.S. Congress has passed major statutes to address emerging privacy issues. The U.S., however, regulates data privacy sectorally and narrowly.[59]

The U.S. largely has followed the distinction between public and private data, and it has afforded the latter protections over the former. Germany set out to protect the underlying right of a natural person to determine the disclosure and use of his or her personal data, and this conception of data privacy influenced

57. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281), *available at* http://www.refworld.org/docid/3ddcc1c74.html. For an overview of the European developments *cf.* SIAN RUDGARD, ORIGINS AND HISTORICAL CONTEXT OF DATA PROTECTION LAW 9 (2012), https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf; Hielke Hijmans & Owe Langfeldt, *Datenschutz in der Europäischen Union*, *in* DATENSCHUTZ. GRUNDLAGEN, ENTWICKLUNGEN UND KONTROVERSEN, *supra* note 50, at 403.

58. Solove, *supra* note 50, at 1–28, with further references. *Cf.* also DATENSCHUTZ. GRUNDLAGEN, ENTWICKLUNGEN UND KONTROVERSEN, *supra* note 50, at 420.

59. Solove, *supra* note 50, at 1–40.

European data privacy, from the case law of the European Court of Human Rights[60] to the GDPR.[61]

Thus in Europe, *all* processing of personal data requires a legal (constitutional) basis.[62] In the U.S., processing of personal data is allowed *unless* it is forbidden under specific circumstances.[63]

C. *The European Data Privacy Paradigm*

The GDPR replaces the EU Data Protection Directive and seeks to provide a comprehensive[64] data privacy framework

---

60. Rotaru v. Romania, App. No. 28432/95, Eur. Ct. H.R. (2000) at n.43, relating to European Convention of Human Rights, art. 8: "Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings: furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of 'private life.' [. . .] Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities."

61. GDPR, *supra* note 3, Recital 26.

62. *Id*., art. 6.

63. A general limitation of the processing of personal data would arguably be seen in the U.S. as an interference with the autonomy and responsibilities of the state and the economic freedom of individuals. For the different paths that have come to define the European and U.S. data privacy paradigms *cf.* Thilo Weichert, *Datenschutz und Überwachung in ausgewählten Staaten*, *in* DATENSCHUTZ. GRUNDLAGEN, ENTWICKLUNGEN UND KONTROVERSEN, *supra* note 50, at 419.

64. Nevertheless, the GDPR is part of a broader data privacy "puzzle." Activities not covered by the GDPR include those falling outside the scope of EU law (such as activities concerning national security) and data processing by competent authorities for the purpose of the prevention, investigation, detection, or prosecution of criminal offenses and associated matters (GDPR, *supra* note 3, Recital 19). The GDPR is also "without prejudice" to the rules in the E-commerce Directive (Directive 2000/31/EC, 2000 O.J. (L 178/1);

intended to ensure a consistent level of protection for natural persons throughout the European Union and to prevent divergences hampering the free movement of personal data within the Union's free market.[65] The GDPR continues to pursue the broad European paradigm of data privacy as a fundamental right,[66] and it conceptualizes privacy as the right to informational self-determination: "The principles of data protection should apply to *any information* concerning an identified or identifiable natural person."[67]

Despite this conceptual breadth, the GDPR leaves complexities and uncertainties for data in an international context.[68]

GDPR, *supra* note 3, Recital 21), in particular to those concerning the liability of intermediary service providers. Finally, the GDPR is not intended to impose additional obligations on top of the obligations contained in the ePrivacy Directive dealing with the processing of data across public communication networks, which therefore is to be amended to ensure consistency across the two regimes (Directive 2002/58/EC, 2002 O.J. (L 201/37) as amended by Directives 2006/24/EC, 2006 O.J. (L 105/54) and 2009/136/EC, 2009 O.J. (L337/11); GDPR, *supra* note 3, Recital 173.

65. GDPR, *supra* note 3, Recitals 10 and 13.

66. Rooted in article 8(1) of the Charter of Fundamental Rights of the European Union (2010 O.J. C 83/393) and article 16(1) of the Treaty on the Functioning of the European Union (2012 O.J. C 326/47). *Cf.* "Everyone has the right to the protection of personal data concerning them." GDPR, *supra* note 3, Recital 1.

67. GDPR, *supra* note 3, Recital 26 (emphasis added).

68. For the following *cf.* LINKLATERS, THE GENERAL DATA PROTECTION REGULATION. A SURVIVAL GUIDE (2016), https://www.linklaters.com/en/insights/publications/2016/june/guide-to-the-general-data-protection-regulation; BIRD & BIRD, GUIDE TO THE GENERAL DATA PROTECTION REGULATION (2019), https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en&hash=D7EC7D1FADB322CE5A05FF4C47A645D1E398E7C4..

The GDPR claims significant extraterritorial effect. First, EU-"established" controllers or processors fall into its scope where personal data is processed "in the context of their activities."[69] If these tests are met, the GDPR applies, regardless of whether the actual data processing takes place in the EU.[70] Second, the GDPR asserts jurisdiction over non-EU-"established" organizations where an EU data subject's personal data is processed in connection with the "offering of goods or services" to her or him, or where the behavior of natural persons within the EU is "monitored."[71] Yet it provides no clear criteria for determining when

69. GDPR, *supra* note 3, art. 3(1).

70. It remains to be seen in practice whether, and how much, legal certainty can be provided for these tests. As for the establishment test, the CJEU under the EU Directive adopted a broad and flexible interpretation that should not hinge on legal form and instead qualified an organization as established where it has "any real and effective activity—even a minimal one—exercised through stable arrangements" in the EU. *See* Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság, ECLI :EU:C:2015:639. Data processing was qualified by the CJEU as being "in the context of the activities" of an EU establishment where such processing was "inextricably linked" to the establishment's activities, such as in the case of EU sales offices which promote or sell advertising or marketing targeting EU residents. See, Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González, ECLI:EU:C:2014:317, at n.6, asserting a far-reaching "right to be forgotten."

71. GDPR, *supra* note 3, art. 3(2).

goods or services are offered to EU data subjects[72] or when their behavior is monitored.[73]

As a Regulation, the GDPR is directly effective in member states without the need for implementing legislation. The GDPR leaves room, however, for EU member states to legislate on data privacy matters.[74] For example, member states may limit rights under the GDPR in areas such as judicial proceedings, criminal prosecutions, and national security; they may provide for further restrictions on the processing of employee data; and they may pass legislation to reconcile data protection with freedom of expression and information as well as to protect information subject to professional secrecy.[75] A significant number of data

72. *See, e.g.*, Kevin Kish, *What does territorial scope mean under the GDPR?*, IAPP THE PRIVACY ADVISOR (Jan. 23, 2018), https://iapp.org/news/a/what-does-territorial-scope-mean-under-the-gdpr/. In a separate context, the CJEU applied the test whether activities were "directed to" EU member states. It cautioned, however, that the question should be determined on a case-by-case basis (Pammer v. Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v. Heller [Joined cases (C-585/08) and (C-144/09)] ECLI:EU:C:2010:740). Broadly applicable factors such as the use of a language or a currency generally used in a member state with the possibility of ordering goods or services in that language, or the mentioning of customers or users who are in the EU, are considered as relevant. GDPR, *supra* note 3, Recital 23.

73. Monitoring refers to the tracking of individuals online to create profiles, including where this is used to take decisions to analyze or predict personal preferences, behaviors and attitudes (GDPR, *supra* note 3, Recital 24).

74. While the GDPR says when it shall be applicable, it does not prescribe the same applicability rules for national implementation laws. This leads to a "conundrum" of diverging national implementation laws rather than to the harmonization intended by the GDPR. *Cf.* Lokke Moerel, *GDPR Conundrums: The GDPR applicability regime—Part 1: Controllers*, IAPP THE PRIVACY ADVISOR (Jan. 29, 2018), https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-1-controllers/.

75. GDPR, *supra* note 3, arts. 23, 85, 88, 90.

processing activities depend on member-state laws, including where the GDPR provides room for a public interest recognized under member-state law to provide a basis to transfer personal data outside of the EU or to restrict such transfer.[76]

Finally, the GDPR provides for one or more regulators, or supervisory authorities, in every member state.[77] While the European Data Protection Board has strong powers to provide guidance and coordinate enforcement of the GDPR through a consistency mechanism,[78] differences in resources and attitudes of supervisory authorities may result in variations in enforcement.

D. The U.S. Data Privacy Paradigm

No single, comprehensive federal law regulates the collection and use of personal data in the United States. Instead, multiple federal and state laws and regulations govern specific sectors and aspects of data privacy and security. In addition, several federal and state agencies have issued guidelines and created frameworks for data collection and use. The following are the most prominent federal privacy laws:[79]

- The Federal Trade Commission Act[80] (FTC Act) is a federal consumer protection law that

---

76. *Id.*, art. 49(4) and (5). Other examples include the right of member states to provide additional justifications for the processing of personal data (art. 6(1)(c)) and to restrict the processing of personal data relating to criminal convictions and offenses (art. 10).

77. *Id.*, art. 51.

78. *Id.*, arts. 63–76.

79. These summaries are adapted from, Ieuan Jolly, *Data Protection in the United States: overview*, THOMPSON REUTERS PRACTICAL LAW (July 1, 2016), https://www.practicallaw.com/dataprotection-guide.

80. 15 U.S.C. §§ 41-58.

prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The FTC is also the primary enforcer of the Children's Online Privacy Protection Act[81] (COPPA). The FTC Act applies to companies and persons doing business in the U.S.

- The Financial Services Modernization Act[82] (Gramm-Leach-Bliley Act (GLB)) regulates the collection, use, and disclosure of financial information. It applies broadly to financial institutions and to other businesses that provide financial services and products. The GLB Act applies to financial institutions and to affiliated and nonaffiliated third parties that receive nonpublic personal information from financial institutions. It also prohibits fraudulent efforts to obtain or disclose nonpublic personal financial information.
- The Health Insurance Portability and Accountability Act[83] (HIPAA) regulates medical information. It can apply broadly to healthcare providers, data processors, pharmacies, and other entities that come into contact with medical information. HIPAA regulations apply to the collection and use of protected health information (PHI) and provides standards for protecting medical data and standards for the electronic

81. 15 U.S.C. §§ 6501-6506.

82. 15 U.S.C. §§ 6801-6827.

83. 42 U.S.C. § 1301.

transmission of medical data.[84] Certain business associates of covered entities may also have contractual obligations to safeguard PHI, including those operating outside of any U.S. jurisdiction.

- The Fair Credit Reporting Act[85] and the Fair and Accurate Credit Transactions Act,[86] which amended the Fair Credit Reporting Act, apply to consumer reporting agencies, those who use consumer reports (such as a lender), and those who provide consumer-reporting information (such as a credit card company). Consumer reports are any communication issued by a consumer reporting agency that relates to a consumer's creditworthiness, credit history, credit capacity, character, and general reputation used to evaluate a consumer's eligibility for credit or insurance.
- The Controlling the Assault of Non-Solicited Pornography and Marketing Act[87] (CAN-SPAM Act) and the Telephone Consumer Protection Act[88] regulate the collection and use of email addresses and telephone numbers, respectively.

84. 45 C.F.R. §§ 160 and 162.

85. 15 U.S.C. § 1681.

86. Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108–159, December 4, 2003, 117 Stat 1952 (2003).

87. 5 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037.

88. 47 U.S.C. § 227.

- The Electronic Communications Privacy Act[89] and the Computer Fraud and Abuse Act[90] regulate the storage, use, and interception of electronic communications, and computer tampering, respectively.

All 50 states have passed laws relating to the collection and use of personal data, and all 50 states, plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private or governmental entities to notify affected people of security breaches of information involving personally identifiable information. These state laws fall into two broad categories: (i) Data breach notification laws[91] and (ii) substantive protections for specific types of personal information.[92]

---

89. 18 U.S.C. § 2510.

90. 18 U.S.C. § 1030.

91. Data breach notification laws typically define: (1) who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc.); (2) the scope of "personal information" (e.g., name combined with social security number, driver's license or state ID, account numbers, etc.); (3) what constitutes a breach (e.g., unauthorized acquisition of data); and (4) notice requirements (e.g., timing or method of notice, who must be notified); and contain exemptions (e.g., for encrypted information). There are also some federal regulators who enforce breach notifications.

92. For example, the New York Department of Financial Services Cybersecurity Regulations, 23 NYCRR § 500 (2017), apply to any individual or nongovernmental partnership, corporation, branch, agency, association, or other entity operating under a license, registration, charter, certificate, permit, accreditation, or similar authorization under New York banking, insurance, or financial services laws, a group that includes both foreign and domestic entities. The Regulations impose minimum standards that exceed existing federal standards and introduce additional requirements. State laws and regulations like this add further complexity and create additional potential for conflict with both federal law and the laws of other jurisdictions.

The new California Consumer Protection Act (CCPA) arguably represents a third, broader category of state laws intended to protect consumer privacy more generally.[93] The CCPA draws from the European model and provides a more comprehensive, individual-rights-based approach to protecting privacy. While it is limited to California residents, both the size of California and the fact that other states are looking to it as a potential model mean that the CCPA will significantly influence data privacy policies in organizations throughout the U.S.

U.S. law generally limits the extraterritorial effect of domestic law, including data privacy laws. Choice-of-law principles create a general presumption against extraterritorial application of domestic law.[94] Most federal privacy laws do not preempt state laws, so businesses can face multiple, at times conflicting, obligations even where they operate solely within the U.S.[95] While the proliferation of new state laws in this area has prompted numerous calls for comprehensive federal legislation that would preempt state laws, privacy advocates, state regulators, and others have argued that any federal standard should

93. CAL. CIV. CODE § 1798.140(c) (West 2020).

94. *See, e.g.*, RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090 (2016); Kiobel v. Royal Dutch Petrol. Co., 569 U.S. 108 (2013); Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247, 255 (2010).

95. These state laws limit their application to persons or businesses that conduct business in the state and therefore apply to non-U.S. entities only when they engage in activities meeting that definition. In most states there is very little case law interpreting this requirement, but at least some commentary has suggested the requirement should be read as "coterminous with 'doing business' as applied by courts to personal jurisdiction analysis involving non-residents." For a complete listing of relevant state statutes and comparison of their requirements, *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 205–13 (5th ed. 2017).

merely establish a floor, leaving states free to impose more stringent standards.

E. International Frameworks

The Council of Europe's Convention 108 remains the first, and to date the most comprehensive, binding international framework to set standards for protecting personal data while also seeking to balance those safeguards against the need to maintain the free flow of personal data for the purposes of international trade. It has been ratified by 55 countries, but not by China, the U.S., or some of the other major trading nations.

The UN Special Rapporteur on the right to privacy, Professor Joseph Cannataci, in his 2018 annual report refers to consultations for the development of principles for regulating big data and open data, indicating they should be drawn from international agreements for data protection as representing "best practice." The report states, "[a]t present, these are the EU's GDPR and the 'modernised' Convention 108 (Convention 108+, 2018) which originated at the Council of Europe but is open to accession globally by States which have enacted consistent principles."[96]

The Special Rapporteur states that, "Convention 108 is steadily being globalized," while noting that Convention 108 includes many, though not all, of the GDPR's new elements. He concludes that, "it is likely, in the next five to ten years, that the extraterritorial effects of GDPR with the ever-widening club of Convention 108 countries, will have a significant effect on the deepening world-wide privacy culture. The precise nature of this evolution is still emerging . . . ."[97]

---

96. Office of the High Comm'r. for Human Rights, Report of the Special Rapporteur on the right to privacy, A/73/45712, at 98 (Oct. 17, 2018).

97. *Id.* at 101.

The Special Rapporteur's comments suggest that a trend toward a comprehensive international standard may be emerging. In the European Commission's own words: "The primary purpose of [the EU data protection legislation] is to ensure that when the personal data of Europeans are transferred abroad, the protection travels with the data."[98]

This trend is also driven by the need to square the territorial-based rules governing law enforcement with the inherently fluid nature of data.[99] The question has been set out most prominently in *United States v. Microsoft*, which led to passage of the CLOUD Act. On the other side of the Atlantic, the European Commission has been tasked with preparing legislative proposals to address obstacles in cross-border access to electronic evidence. Access may become more efficient and faster, including by eliminating data localization requirements, while ensuring fundamental rights of natural persons in criminal proceedings and data privacy.[100] At the same time, the Cloud Evidence Group, a working group of the Cybercrime Convention Committee that represents the state parties to the Council of Europe's

98. European Comm'n., Commc'n from the Comm'n. to the European Parliament and the Council, *Exchanging and Protecting Personal Data in a Globalized World*, at 4 (Jan. 10, 2017). On Jan. 31, 2018, the European Commission endorsed horizontal provisions for cross-border data flows and personal data protection in trade negotiations, whereby the preferred avenue for the EU are adequacy decisions (*available at* http://europa.eu/rapid/press-release_MEX-18-546_en.htm). If agreed on by the EU member states, this approach can be expected to serve as a starting point for negotiations on provisions to be included in Free Trade Agreements and Bilateral Investment Treaties between the EU and third countries like Japan and Korea.

99. *See* Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 220–32 (2018).

100. *See e-evidence*, EUROPEAN COMMISSION MIGRATION AND HOME AFFAIRS, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en (last visited April 20, 2020).

Budapest Convention on Cybercrime, is exploring solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions.[101]

Despite a plethora of transnational coordination initiatives and regimes, the current system for data protection is highly fragmented and complex, with diverging and sometimes conflicting global, regional, and national regulatory approaches.[102]

In such a context, basic questions of choice of law and jurisdiction have a profound implication not just for privacy and business interests but, as one commentator put it, most fundamentally for "our understanding of and ability to shape policy going forward."[103]

F. Data Localization Laws

While the GDPR seeks to cloak European personal data in its protections wherever it goes and prohibits it from going certain

---

101. *See Cloud Evidence Group*, COUNCIL OF EUROPE, https://www.coe.int/en/web/cybercrime/ceg (last visited April 20, 2020).

102. In 2018, The United Nations Conference on Trade and Development (UNCTAD) assessed that 21 percent of countries had no data protection legislation and that many national data protection legislations contained significant gaps and exemptions depending on, e.g., business and data size, types of data, and subject, sensitivity, sources or sector-specificity of data (UNCTAD, *Data Protection and Privacy Legislation Worldwide*, http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (last visited April 20, 2020)). Many national laws and regional initiatives further allow individual companies to determine the scope of data protection (e.g., by subjecting certain activities to data protection regimes such as the EU-U.S. Privacy Shield) or to exclude certain activities from protection in their public privacy policies. *See* UNCTAD, DATA PROTECTION REGULATIONS AND INTERNATIONAL DATA FLOWS: IMPLICATIONS FOR TRADE AND DEVELOPMENT (2016), at 8–10, https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

103. Daskal, *supra* note 99.

places if certain conditions are not met, other countries take an even more restrictive approach to cross-border data flows by requiring all data to be stored and processed within its own territory. Data localization laws either require organizations to store and process data on servers physically located within national borders, or they subject the export of personal data to conditions. Although these laws present a significant challenge to the flow of data in commerce, [104] they also help nations protect the privacy of their citizens, as well as their sovereignty over data within their borders.

There are many reasons governments enact data localization laws. First, limiting the unfettered export of personal data can help protect citizens from those who would collect information and use it without their knowledge or consent. Second, and relatedly, data localization laws both enhance the ability of the relevant nation's consumers to seek remedies against those who misuse personal data and facilitate local law enforcement. Third, localization laws make clear to the world that protecting personal information is a national priority. Fourth, the laws have an incidental benefit of encouraging IT investment in the national economy by those who wish to do business with the nation and its residents. Fifth, such laws arguably enhance information security against foreign intelligence operations by requirement foreign intelligence agencies to "come and get" the information they seek.[105] Sixth, and on a darker note, they also

---

104. Ruslan Synytsky, *New GDPR Laws Ahead—Are Privacy Concerns Inhibiting Global Business*, FORBES (Dec. 6, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/12/06/new-gdpr-laws-ahead-are-privacy-concerns-inhibiting-global-business/#4beb3fb1719f.

105. The Edward Snowden revelations in 2013 that the U.S. National Security Agency was monitoring internet traffic of foreign governments and their citizens provided a platform for governments to posit that data localizations laws are necessary. As Anupam Chandler and Uyên P. Le identified:

enable countries that are so inclined to maintain tighter controls over their citizens and residents.[106]

As of this writing, data localization laws take many forms. For example, Russia's Personal Data Law,[107] which became law in September 2015, requires that data operators who collect personal data about Russian citizens must "record, systematize, accumulate, store, amend, update and retrieve" data using databases physically located in Russia. In a similar vein, China's Cybersecurity Law, which took effect in June 2017, seeks to ensure network security, safeguard cyberspace sovereignty, national security, and the societal public interest, and protect the lawful rights and interests of citizens. The law imposes a data localization requirement on personal information and important data collected and generated by the operators of critical information infrastructure. All data must be stored within China, and a security assessment must be conducted before

---

> 'Efforts to keep data within national borders have gained traction in the wake of revelations of widespread electronic spying by United States intelligence agencies. Governments across the world, indignant at the recent disclosures, have cited foreign surveillance as an argument to prevent data from leaving their borders, allegedly into foreign hands. As the argument goes, placing data in other nations jeopardizes the security and privacy of such information.' (Anupam Chandler & Uyên P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 679–680 (2015).

106. Chandler and Le argue that notwithstanding the arguments for data localization, it "increases the ability of governments to *surveil* and even oppress their own populations." *Id.* at 680. It is against this background that there has been in recent years a growing number of countries implementing data localization laws such as those now in force in Russia and China.

107. On Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure of Personal Data Processing in Information-Telecommunications Networks, Russian Federal Law No. 242-FZ.

cross-border transfer of data. On a lesser scale, Australia and South Korea impose specific restrictions on transferring personal data cross-border in health and finance because of its sensitivity. Malaysia and the Philippines have strict consent requirements and regulatory approvals for cross-border transfer of personal data.[108]

The Albright Stonebridge Group illustrated the spread of globalization in the following table, which highlights the spectrum of data localizations laws and regulations.[109]

108. Other countries that have data localization laws include: Switzerland, Turkey, Brazil, Vietnam, Brunei, Iran, India, Indonesia, and Nigeria.

109. ALBRIGHT STONEBRIDGE GROUP, DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION 5 (2015), http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf. We have added the U.S. to the table due to the Electronic Communications Privacy Act of 1984, 18 U.S.C. §§ 2510-23.

Data localization laws	Jurisdiction
Strong: Explicit requirements that data must be stored on servers within the country.	Brunei, China, Indonesia, Nigeria, Russia, Vietnam
Partial: Wide range of measures, including regulations applying only to certain domain names and regulations requiring the consent of an individual before data about them is transferred internationally.	Belarus, India, Kazakhstan, Malaysia, South Korea
Mild: Restrictions on international data transfers under certain conditions.	Argentina, Brazil, Colombia, Peru, Uruguay
Sector-specific: Tailored to specific sectors, including healthcare, telecom, finance, and national security.	Australia, Canada, New Zealand, Taiwan, Turkey, Venezuela, United States
None: No known data localization laws.	Remaining Countries

Despite the asserted advantages of data localization laws, they may not be an unmitigated good. Proponents of free trade argue that data localization laws are a barrier to companies seeking to expand physical facilities or sell to consumers through the internet. The laws limit the flow of data and increase the compliance costs of doing business. While larger international businesses may more easily assimilate the costs, the costs for smaller- to medium-sized businesses and businesses from less developed economies are barriers to trade. In litigation and regulatory investigations, the cost of cross-border processing and transfer of personal data between jurisdictions will also increase. The higher cost of doing business must be reflected either in higher prices for consumers or in fewer goods or services being made available to them.

As the Albright Stonebridge Group 2015 report states:[110]

> "On a macro basis, studies indicate that data localization regulations can have damaging long-term consequences. Potential disruptions in information flows cause uncertainty among companies and lead to lower levels of foreign investment. In addition to its impact on businesses, localization tends to reduce services and increase prices for domestic consumers."

The Albright Stonebridge Group report also referred to the study by the European Centre for International Political Economy, which examined the overall impact of localization measures in seven jurisdictions—Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam—and found negative impacts on GDP and foreign investment. The 2014 study found that localization regulations cost EU citizens an estimated $193 billion per year, due in part to higher domestic prices, and that Vietnam's strict 2013 data localization requirement had reduced its GDP by 1.7 percent.[111]

Data localization laws will continue to be an issue for companies operating globally, faced with complying with different regulatory regimes and increased costs. Cohen, Hall and Wood conclude:[112]

---

110. *Id.* at 7.

111. MATTHIAS BAUER ET AL., EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY, THE COSTS OF DATA LOCALISATION: FRIENDLY FIRE ON ECONOMIC RECOVERY (2014), https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf, referred to in Albright Stonebridge Group, *supra* note 110, at 7.

112. Bret Cohen, Britanie Hall, & Charlie Wood, *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy*, ANTITRUST, Vol. 32 No. 1, Fall 2017, at 107.

> "As these data localization laws proliferate, the cost of doing business globally increases because complying enterprises must either open new data centers, change their network architecture, or use a local cloud vendor. Meanwhile, privacy and security suffer as companies are forced to store data in a way that is not the most efficient or effective.
>
> "Data localization laws are here to stay. As companies invest in compliance and governments without these laws see the short-term benefits that accrue to the localizing government in the form of increased access to data and a boost to the local economy, more nations may want to get in the localization game. Without coalitions or policies to combat data localization efforts, the struggle between global business and nationalistic interests will most likely amplify over the years ahead."

G. Transnational Coordination Regimes

i. EU GDPR

The GDPR, on one view, is a data localization law, because personal data can only be transferred to countries outside the EU or an international organization where an "adequate level" of protection is guaranteed (Article 44). Furthermore, Article 48 states that, "[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may not be recognized or enforceable in any manner unless based on an international agreement, like a mutual legal assistance treaty in force between the requesting third (non-EU) country and the EU or a member state."

Transfers may take place to a third country or international organization where the EU Commission has decided that it ensures "an adequate level of protection" (Article 45(1)). The adequacy decisions under the EU Directive[113] remain in force under the GDPR, and those jurisdictions determined by the EU Commission to provide "an adequate level of protection" are: Andorra, Argentina, Canada (commercial organizations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay. (Japan was added in 2019.) There are ongoing adequacy talks with South Korea. Transfers to the U.S. are permitted pursuant to the Commission's July 2016 decision on the adequacy of the protection provided by the EU/U.S. Privacy Shield, but only for those companies that are Privacy Shield certified.[114]

Transfers are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable individual rights and effective legal remedies for the data subject are available (Article 46). Appropriate safeguards include:

- Approved binding corporate rules that enable transfers within a multinational group of companies (Article 47).[115]

---

113. *See Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (last visited April 20, 2020).

114. *See EU-US data transfers: How personal data transferred between the EU and US is protected*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en (last visited April 20, 2020).

115. *See Binding Corporate Rules: Corporate rules for data transfers within multinational companies*, EUROPEAN COMMISSION, https://ec.europa.eu/info/

- Standard data protection contractual clauses approved by the EU Commission.[116]
- Approved code of conduct under Article 40, and the recipient gives binding and enforceable commitments to apply appropriate safeguards.
- Approved certification mechanism under Article 42, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards.

ii. Trans-Pacific Partnership

In March 2018, 11 countries—Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam—signed the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CP-TPP). Although the U.S. was a party to the negotiations for the TPP-12, it withdrew from the agreement following the change of administration in 2017, and it is now called the TPP-11.

The TPP-11 sets out rules reflecting that the internet is an essential tool for those companies within the TPP-11 doing business in the global economy. The principles for digital free trade under the TPP-11 are that servers can be set up in any country, data can be transferred across borders, and source codes need not be disclosed.

---

law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en (last visited April 20, 2020).

116. *See Standard Contractual Clauses: Standard contractual clauses for data transfers between EU and non-EU countries*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en (last visited April 20, 2020).

For the first time in a trade agreement, TPP-11 countries guarantee the free flow of data across borders for service suppliers and investors as part of their business activity. Article 14.2 states, "The Parties recognize the economic growth and opportunities provided by electronic commerce and the importance of frameworks that promote consumer confidence in electronic commerce and of avoiding unnecessary barriers to its use and development."[117]

TPP-11 governments can maintain and amend regulations related to data flows but have undertaken to do so in a way that does not create barriers to trade. Article 14.11: Cross-Border Transfer of Information by Electronic Means states:

> 1. The Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
>
> 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
>
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
>
> (a) is not applied in a manner which would constitute a means of arbitrary or

117. *See* Trans-Pacific Partnership, Ch. 14: Electronic Commerce, https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf (last visited April 20, 2020).

unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on transfers of information greater than are required to achieve the objective.[118]

Data localization is prima facie banned under the TPP-11. TPP-11 countries have committed not to impose localization requirements on computing facilities; this aims to provide certainty to businesses as they look to optimize investment decisions. Article 14.13 provides:

1. The Parties recognize that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.

3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

   (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

118. *See Id*.

> (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.[119]

iii. APEC Cross-Border Privacy Rules

The APEC (Asia-Pacific Economic Cooperation) Cross-Border Privacy Rules **(**CBPR**)** system was developed to build consumer, business, and regulator trust in cross-border flows of personal information. APEC members who have joined include Canada, Japan, Mexico, the United States, South Korea, Singapore, Australia, and Chinese Taipei.

The APEC CBPR System requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework. These policies and practices must be assessed as compliant with the program requirements of the APEC CBPR System by an Accountability Agent (an independent APEC CBPR system recognized public- or private-sector entity) and be enforceable by law.

Principle 48 states:

> Member Economies should endeavor to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable cross-border data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and

119. *See Id*.

> bureaucratic burdens for businesses and consumers.[120]

Part IV of Section B sets out the framework for International Implementation and provides:

> IV. Cross-border transfers
>
> 69. A member economy should refrain from restricting cross-border flows of personal information between itself and another member economy where (a) the other economy has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it.
>
> 70. Any restrictions to cross-border flows of personal information should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross-border transfer.
>
> V. Interoperability between privacy frameworks
>
> 71. Recognizing that personal information flows do not stop at regional boundaries, member economies should encourage and

120. *See* ASIA-PACIFIC ECONOMIC COOPERATION, APEC PRIVACY FRAMEWORK (2015), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

> support the development of international arrangements that promote interoperability amongst privacy instruments that give practical effect to this Framework.
>
> 72. Improving the global interoperability of privacy frameworks can bring benefits in improved personal information flows, help ensure that privacy requirements are maintained when personal information flows beyond member economies and can simplify compliance for personal information controllers and processors. Global interoperability can also assist individuals to assert their privacy rights in a global environment and help authorities to improve cross-border privacy enforcement.[121]

While the CBPR system provides a regional multilateral cross-border transfer mechanism, it is a voluntary scheme with, so far, only eight countries participating out of the twenty-one APEC member countries. Furthermore, only the U.S. and Japan have appointed accountability agents to certify organizations as CBPR compliant. When the GDPR came into effect in May 2018, with its greater restrictions on cross-border transfers and stronger enforcement mechanisms, including severe penalties, it appeared that the future of CBPR could be bleak. However, the CBPR was explicitly included in the United States-Mexico-Canada Agreement, and it has been reported that there are several other countries interesting in joining the CBPR system.

---

121. *See Id.* at 31.

iv. APEC, CBPR, and the United States-Mexico-Canada Agreement

The United States-Mexico-Canada Agreement (USMCA), which was agreed to in September 2018 and is still to be ratified, includes a digital trade chapter. The USMCA recognizes the CBPR as a valid mechanism to facilitate cross-border information transfers while protecting personal information.

It provides that "no [p]arty shall prohibit or restrict the cross-border transfer of information, including personal information . . . for the conduct of the business of a covered person."[122] Article 19.11.2 then provides restrictions may be imposed to achieve a "legitimate public policy objective" provided that it is not "arbitrary" or a "disguised restriction on trade," and it "does not impose restrictions on transfers greater than are necessary to achieve the objective."[123]

Article 19.8 deals with personal information protection and requires that the parties adopt or maintain a legal framework for the protection of personal information of the users of digital trade. In the development of the framework, the parties are required to "take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the Organisation for Economic Co-Operation and Development (OECD) Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)."[124]

---

122. *See* United States-Mexico-Canada Agreement, Ch. 19: Digital Trade, 19-6, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf (last visited April 20, 2020).

123. *See Id*.

124. *See Id*. at 19-4, 19-5.

Article 19.8.6 states that, "[t]he Parties recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information."[125] And, Article 19.14.1(b) provides that recognizing the global nature of digital trade, the parties shall endeavor to, among other things, "cooperate and maintain a dialogue on the promotion and development of mechanisms, including the APEC Cross-Border Privacy Rules, that further global interoperability of privacy regimes."[126]

H. Other developments—EU and Asia

In August 2017, the APEC Electronic-Commerce Steering Group's Data Privacy Subgroup (DPS) met with the European Commission to discuss issues related to personal data protection regimes and the facilitation of global data flows. A release following the meeting stated:

> "The DPS and the Commission exchanged information on the APEC Cross-Border Privacy Rules (CBPR) System and the EU's GDPR, which goes into effect in May 2018, with the aim of exploring interoperability between the two systems. The Commission explained that the reform facilitates data flows by simplifying the use of existing transfer mechanisms and introducing new tools for transfer. The Commission also informed the DPS about ongoing work with Asia-Pacific countries on possible adequacy findings with a view to fostering regulatory convergence and facilitating trade, and expressed its interest in strengthening

125. *See Id*. at 19-5.

126. *See Id*. at 19-7.

> enforcement cooperation between data protection authorities in the APEC region and the EU."[127]

There is considerable focus within the Asia Pacific region on the ongoing implementation of the APEC CBPR system across the region. The announcement of the adequacy decision concerning Japan and the ongoing adequacy talks with South Korea in 2018, referred to above, highlight the continuing focus on the Asia Pacific region.

A further initiative took place in early in February 2018, when ninety experts and high-level government officials in the region met in Singapore at the Asian Legal Business Institute's Forum "Towards A Shared Legal Ecosystem for International Data Flows in Asia." This event was the first time in Asia that representatives from government, data protection regulators, industry, and the legal community representing 19 jurisdictions met to discuss how to achieve a common Asian framework to share and transfer information across international borders. The Asian Legal Business Institute (ABLI) stated:

> "The fragmented data privacy laws and data localisation requirements in Asia are considered one of the biggest stumbling blocks to the development of the digital economy and e-commerce and for pushing up the costs of doing business in the region. The Forum is part of ABLI's Data Privacy

127. *See Data Privacy Subgroup Meeting with European Union*, ASIA-PACIFIC ECONOMIC COOPERATION, http://publications.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union (last visited April 20, 2020).

> Project which aims to help address these challenges."[128]

It is clear that the GDPR has set an international benchmark for the protection of personal data, which is impacting new legislation in the Asian region. This includes India's Personal Data Protection Bill 2018,[129] which uses the GDPR as a model. It requires copies of Indian personal data be stored in India and puts in place similar restrictions to the GDPR for data transfers out of India.

128. *See Towards A Shared Legal Ecosystem for International Data Flows in Asia*, ASIAN BUSINESS LAW INSTITUTE, https://abli.asia/NEWS-EVENTS/Whats-New/ArticleType/ArticleView/ArticleID/52 (last visited April 20, 2020).

129. *See* The Personal Data Protection Bill, 2018, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

THE SEDONA CONFERENCE COMMENTARY ON LAW FIRM DATA SECURITY

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editors-in-Chief and Steering Committee Liaisons:

David Moncure Neil Riemann

Contributing Editors:

Guillermo Christensen Anthony Lowe

Sheryl Falk Gita Radhakrishna

Michele Gossmeyer Daniel Sutherland

Christopher King Alexander White

Jana Landon

Staff Editors:

David Lumia Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on Law Firm Data Security*, 21 SEDONA CONF. J. 483 (2020).

PREFACE

Welcome to the July 2020 final version of The Sedona Conference *Commentary on Law Firm Data Security* ("*Commentary*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editors-in-Chief Neil Riemann and David Moncure for their leadership and commitment to the project. We also thank contributing editors Guillermo Christensen, Sheryl Falk, Michele Gossmeyer, Christopher King, Jana Landon, Anthony Lowe, Gita Radhakrishna, Daniel Sutherland, and Alexander White for their efforts. We also thank Elise Houlik and Robert Levy for their contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of the *Commentary* were the subject of dialogue. The publication was also subject to a period of public comment. On behalf of The Sedona Conference, I thank all of them for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
July 2020

TABLE OF CONTENTS

I. INTRODUCTION

Client organizations[1] undertake considerable business risk when they entrust law firms with personal, proprietary, or otherwise confidential data to facilitate effective representation. Law firms undertake similarly substantial liability and reputational risks by accepting such data.

Organizations have legal and market-based obligations to ensure their data is protected and remains secure. One of those obligations is a duty to choose outside counsel who will protect such data properly and to ensure that outside counsel do so.

Outside counsel have a duty to protect client data. The duty arises from the ethical rules applicable to attorneys; federal and state statutes and regulations; foreign laws, where applicable; the common law; and contractual obligations the firm has agreed to undertake.

Notwithstanding these complementary duties, organizations and law firms do not always approach data security the same way. Although sound risk management supports treating different enterprises differently, organizations may prefer to impose the same data security requirements on all service providers. Organizations often resist pleas from law firms to be treated differently than other service providers. Law firms provide an expensive, high-margin service. They operate under the same statutes and common law that govern other providers. They can undertake specific contractual obligations to secure organization data, just like other service providers. Firms use many of the same technologies used by organizations and the organizations' other service providers. From the organization

1. Some of the discussion in this *Commentary* may prove useful to individual clients as well as organizational ones, but it does not focus on individual clients or the ways the situation of an individual client may differ from that of an organizational one.

perspective, law firms may be different than other vendors, but are they materially different for purposes of imposing data security requirements?

Law firms, on the other hand, see valid reasons for distinctive treatment. First and foremost, they are—unlike most service providers—ethically bound to maintain the confidentiality of client information, regardless of contractual obligation. Second, but related, law firms are ethically obligated to pursue the best interests of their clients, not just maximize profits. Organization demands for special, one-off handling of organization data can impair effective representation by altering the firm's workflow or requiring the use of alternative tools.

While strides have been made in understanding and addressing data security at law firms, there is consensus that more must be done to secure the sensitive data held by law firms. Tensions have grown as cybersecurity vaults to the top of the national agenda, and it has become increasingly obvious that law firms are more attractive targets for information theft, and less capable of preventing it, than previously thought.

In recent years, organizations have developed a host of approaches to this problem. Law firms have struggled to keep up with the volume and variety of demands for information about their data security posture. Firms continue to differ in their understanding of data security issues and the sophistication with which they can address and have addressed them. While some large firms have embraced collaboration with their peers on data security issues, smaller firms lack readily accessible vehicles for such interfirm cooperation, and efforts to collaborate tend to focus on the mechanics of security rather than streamlining the process of addressing organization inquiries about data security.

In response to these problems, the Sedona Conference's Working Group 11 developed a brainstorming group, and then

a drafting team, to identify ways that organizations and law firms should approach and address organization concerns about law firm data security. This *Commentary* is the result of that effort. The *Commentary* is intended to foster respectful and mutually beneficial dialogue between organizations and their firms regarding organization expectations and law firm capabilities. The *Commentary* seeks to move this dialogue forward by providing best practices focused on data security requirements that are meaningful considering the organization's obligation to protect the data, the type of data the organization is providing to the law firm, and the law firm's operating environment. In short, this *Commentary* intends to provide an effective road map for more efficient, effective communication to address data security issues and scenarios confronted by organizations and the law firms they engage.

While the *Commentary* may be of interest to other audiences, it is primarily directed toward two: first, to in-house counsel and an organization's technical personnel charged with ensuring that organizational service providers handle data securely; and second, to the law firm professionals and technical personnel overseeing and implementing data security at law firms.

The Sedona Conference has done prior work relating to data security, to which the reader is also referred. The most directly relevant work is *The Sedona Conference Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers.* This Commentary was developed by Working Group 1, which focuses on Electronic Document Retention and Production. It provides guidance to law firms on the sources of their duties to protect client information and, more importantly, on the development of a risk-based data security program. Less directly relevant work that nevertheless touches on the law firm's handling of client information includes work by Working Group 2 that concern protective orders and public access to litigation documents; numerous

papers developed by Working Groups 1 and 6 that address various aspects of information governance and the protection of client information in the discovery process; and this Working Group's Draft *Commentary on Privacy and Information Security in Civil Litigation.*

Note that the drafting team has not undertaken to comprehensively analyze the data security situation faced by every organizational client seeking to retain counsel. The team recognizes that some organizations work in regulated fields or have highly particularized data security needs, like those in the health care, financial, and classified contracting sectors. While most of the considerations taken up in this *Commentary* will apply to organizations in these sectors as well, they do not analyze in detail the legal requirements governing their specialized data.

Additionally, the *Commentary* does not address privacy concerns. The drafting team declined to undertake that task for a few reasons. First, ensuring the secure handling of any personal information an organization conveys to a law firm is necessary to protect privacy, but it is not sufficient. Personal information can be divulged in violation of privacy laws despite a perfectly secure environment, and security practices can also pose privacy risks. Second, privacy law is a multi-jurisdictional enterprise that imposes different requirements in different locales, and privacy laws apply differently to different types of personal information and different types of custodians. Finally, privacy issues have not, to date, led to the same proliferation of competing questionnaires and extended interactions between organizations and firms as have data security issues.

The *Commentary* that follows contains three distinct sections. In the first, the *Commentary* identifies some common criteria and protocols for assessing information security at law firms. The discussion focuses first on organization expectations for outside counsel in terms of the law firm's governance, as well as the

technologies, people, and third-party service providers that make security happen. Following extended discussion of these topics, brief consideration is given to what organizations might expect from law firms with international operations and what organizations might expect of law firms in terms of cooperation with information-sharing efforts around data security.

In the second section, the *Commentary* discusses the practicalities of an organization's communications with law firms regarding data security. Nine topics are discussed, covering the entire relationship life cycle by addressing matters that should be considered before a firm is even consulted all the way through to matters that should be addressed with firms throughout the life of the relationship.

The third and final section consists of two appendices. Appendix 1 offers some model clauses regarding data security that could be used in an engagement letter. These are merely a starting point; the actual clauses should turn on the outcome of the organization's discussion with the firm. Appendix 2 offers a model questionnaire for organizations to present to law firms as a way of initiating a conversation about data security. The latter includes some sample answers and some commentary about how the actual answers should be evaluated.

No single *Commentary* will satisfy every use case for every engagement. As stated above, it is hoped that this one provides an effective road map for more efficient, effective communication to address most of the data security issues and scenarios confronted by organizations and the law firms that handle and store their data.

II. COMMON CRITERIA AND PROTOCOLS FOR ASSESSING INFORMATION SECURITY AT A LAW FIRM

The goal of this section is to develop a set of common criteria and protocols for organizations to use when assessing the cybersecurity of a law firm. Where possible, the objective of this proposed approach is to fashion a set of criteria and protocols that allows for organizations to use the same or similar types of questions to get to the same information about a law firm.

A. Organization Expectations for Outside Counsel

Organizations and firms alike have explicit or implicit expectations about how law firms should secure their information systems and the organization's data. Organizational concerns are increasingly extending beyond the protection of confidences. Organizations expect timely, effective advice and representation, as well as for the law firm to have a comprehensive security program that includes a holistic approach of managing people, processes, and technology. A security incident that prevents a firm from providing advice and representation can be as injurious to the organization as a security breach that discloses its confidences. Similarly, organizations also have an expectation that firms will provide services effectively and timely by relying on technology to achieve efficiencies. The following sections consider information security expectations organizations might reasonably have for outside counsel in the areas of governance, technology, people, use of third-party service providers, and insurance.

1. Governance

Governance, not technology, should be the starting point for an organization's assessment of a firm's security posture. This section discusses six key questions about governance that organizations should ask—and firms should expect to answer—

about how they govern their information security apparatus. An added benefit of focusing on governance is that it can address not only cybersecurity systems and tools but also the culture of a law firm, which may not be adequately assessed when the spotlight is focused on technology.

1. Any lawyer should have the authority to require security measures, but which lawyers bear the ultimate responsibility for any failure of those measures?
2. Can the firm establish that it satisfies the expectations of its governing bar(s) and other general legal requirements?
3. Can the firm establish that it can satisfy the requirements of other laws, regulations, industry standards, and frameworks that apply or should be considered, given the type of information the organization is providing the firm or the magnitude of the engagement?
4. What policies and procedures does the firm have in place to implement the agreed requirements and ensure the confidentiality, integrity, and availability of the organization's information?
5. How does the firm assess and ensure that the applicable lawyers, support personnel, and service providers have the knowledge and experience necessary to successfully implement these policies and procedures, including required training of all personnel?
6. How do the organization and the firm propose to address a firm security incident that exposes the organization to potential legal liability or reputational harm?

(a) Authority and Responsibility

As discussed in more detail below, lawyers are required to safeguard client confidences. In many jurisdictions, explicit or implicit duties are imposed on lawyers to develop and maintain the technological competence necessary to do that. For those reasons, every firm, regardless of size, should have one or more *lawyers* who have the authority to require the firm and other lawyers to implement information security measures. These may be a combination of General Counsel, Chief Security Officer, Managing Partner, and Practice Lead/Relationship Partner. Typically, these same lawyers bear ultimate responsibility for the failure of those measures. Organizations should reasonably expect to know the identity of the lawyers who are accountable for providing answers about their firm's information security programs.

While it may be important for organizations to understand who is making the firm's information security decisions, most firms will be relying heavily on professional information technology staff, information security staff, or service providers to provide the information necessary for the firm's lawyers to make those decisions. However, the final authority should rest with the lawyer leader(s) of the firm who carry the ethical duties noted above. Evaluation of this capability is discussed below.

(b) State Bar Requirements for Protecting Client Confidences and Secrets

Once the accountable law firm personnel are identified, organizations will likely wish to explore, at varying degrees of depth, whether those lawyers understand the efforts required of them, starting with the requirements of professional ethics. Rule 1.6 of the American Bar Association's ("ABA's") Model Rules of Professional Conduct—adopted with minimal variation by most state bar regulators—requires as an enforceable matter of

professional ethics that lawyers safeguard the confidentiality of information relating to their representations of organizations. This includes a duty to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to" that information.[2] Comment 18 to the Rule discusses the concept of reasonable efforts in some detail. Both firms and organizations should expect organizations to explore how well the accountable personnel understand those requirements.[3]

Rule 1.1 of those same rules requires the lawyer to act competently in fulfilling the command of Rule 1.6. In most American jurisdictions, the official commentary on this duty of competence now makes explicit reference to the need for lawyers to keep abreast of changes in technology.[4] For that reason, it is also appropriate for organizations to explore the technological competence of the accountable lawyers and any nonlawyer technology advisors to ensure that the commands of the Rules of Professional Responsibility can be and are being met.

In 2017, the ABA issued Formal Opinion 477R on Securing Communication of Protected Client Information,[5] which further

2. MODEL RULE OF PROF'L CONDUCT r. 1.6(c): Confidentiality of Information, AM. BAR ASS'N, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/ (last visited April 2, 2020).

3. MODEL RULE OF PROF'L CONDUCT r. 1.6 Confidentiality of Information—cmt. 18, AM. BAR ASS'N, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/ (last visited April 2, 2020).

4. MODEL RULE OF PROF'L CONDUCT r. 1.1 Competence—cmt. 8, AM. BAR ASS'N, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/ (last visited April 2, 2020).

5. ABA Formal Op. 477R: Securing communication of protected client information (June 2017), https://www.americanbar.org/news/abanews/pub

emphasizes the ethical duties of counsel (based on the Model Rules Referenced above) to protect communications with clients and the general obligation to ensure that an organization's information remains confidential. The Opinion cites to attorneys' general obligations of (a) technological competency (Comments to Model Rule 1.1) and (b) taking reasonable measures to prevent inadvertent or authorized disclosure of information relating to the representation (Comments to Model Rule 1.6). This Opinion also notes the responsibility of law firms to ensure that their software and infrastructure service providers have appropriate controls in place to protect the organization's data stored on a provider's systems, particularly cloud systems.

The following year, the ABA extended its guidance on these matters with the issuance of Formal Opinion 483, addressing a lawyer's duties to clients following a data breach. Citing Rules 1.1, 1.6, 5.1, and 5.3, the ABA there concluded that Rule 1.4's obligation to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation" requires a lawyer to notify current clients and take other reasonable steps "[w]hen a data breach occurs involving, or having a substantial likelihood of involving, material client information."[6] The opinion makes clear that this obligation is in addition to other legal obligations the lawyer may have with respect to data breaches. In addition to a notification obligation, the obligations suggested by the opinion include making reasonable efforts to detect breaches, acting reasonably

lications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/.

6. ABA Comm. On Ethics & Prof'l Responsibility, Formal Op. 483, Lawyers' Obligations After an Electronic Data Breach of Cyberattack (Oct. 17, 2018), https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf.

promptly to stop the breach and mitigate damage, making reasonable efforts to determine what client information was accessed, and considering client confidentiality when disclosing details of the breach to third parties. While the ABA's opinion does not establish a similar duty with respect to nonclients or former clients, at least one state bar has already expanded the duty established in Formal Opinion 483 to reach former clients.[7]

(c) Other Applicable Regulations, Industry Standards, and Frameworks

The aforementioned bar guidance is codified in state law by many jurisdictions. It will be, for many firms, the only legal requirement governing law firm information security, at least as it relates to the organization's information. However, many organizations will have additional compliance concerns centered around statutes, regulations, industry standards, and frameworks relevant to their lines of business. These concerns will lead many organizations to vet firms and impose minimum security requirements on them based on security frameworks like the National Institute of Standards and Testing's (NIST) Cybersecurity Framework or the International Standards Organization's ISO 27001 standard for Information Security Management. Organizations undertaking that kind of vetting process will need to assess whether firms understand the information security requirements for service providers under such frameworks.

We discuss below some considerations regarding the security requirements of international organizations or offices, as well as domestic security requirements that sector-specific

7. Board of Overseers of the Bar for the State of Maine, Op. #220, Cyberattack and Data Breach: The Ethics of Prevention and Response, https://www.mebaroverseers.org/attorney_services/opinion.html?id=1267989 (Apr. 11, 2019).

regulation in the United States might impose on law firms handling certain types of information.

(d) Law Firm Data-Security-Related Policies and Procedures

Organizations and firms should be prepared to discuss the firm's data-security-related policies and procedures to ensure they are adequate to implement the requirements of state bar rules and any other laws identified by the analysis described above. The adequacy of such policies and procedures should be evaluated considering the size of the firm, the volume and sensitivity of the organization's data being shared, and any requirements imposed by applicable law. While a firm's small size will not excuse the absence of policies and procedures related to data security, it may be relevant to the detail with which those policies and procedures are documented and the way they are implemented. It may not make sense, for example, to ask for detailed written training materials from, or impose guest-name-badge requirements on, a firm composed of two lawyers and one assistant operating in a 1000-square-foot office. The absence of such materials or requirements in this context does not mean that the small firm is insecure. Indeed, depending very much on the circumstances, a larger firm might be more vulnerable due to size, systems budget, and complexity.

(e) Knowledge and Experience

Organizations will want to explore the knowledge and experience of the firm personnel who will be accessing and protecting their data. While the accountable lawyers should understand the issues of concern at some level, organizations should not ordinarily expect the accountable lawyers themselves to have technical security knowledge. They should expect instead that a firm can demonstrate that it has the professional staff who have that knowledge and experience. Firms without in-house

information technology and information security staff should be able to demonstrate the necessary knowledge and experience via vetted service providers.

(f) Incidents and Breaches

Organizations and law firms should strive to reach agreement within the scope of their engagement as to the firm's obligation in the event of a security incident or breach that threatens to or does result in the misuse or theft of the organization's data. Organizations are increasingly likely to demand that law firms go beyond any state or federal laws mandating disclosure of data breaches, particularly since many existing data breach laws only address personal data and do not address disclosure or compromises of types of nonpersonal data that organizations consider sensitive.

Firms should plan notification protocols in advance: Will the firm notify any third parties, such as state Attorneys General, of the breach? Will it notify the organization itself? Who will bear the cost of any necessary breach notification? Will the firm defend or indemnify the organization against claims arising because the firm suffered a breach and the organization's information was disclosed?[8]

During due diligence, organizations may request that law firms provide data on previous incidents or breaches as a means of evaluating the firm's information security program. In any negotiation on the exchange of security information like this, the focus must be on how the data would help engage the parties in a discussion regarding resources and risk evaluation. Each party needs to understand the duty associated with handling the

8. Some firms take the position that indemnification imperils their ability to vigorously represent clients. Discussion of this topic is beyond the scope of this paper.

other party's data and should limit the volume to only that which is necessary.

There are a variety of reasons for such a request for security details. Organizations may wish to use the descriptions of incident handling and breach response to evaluate the maturity of the organization or assess whether resources are directed appropriately. A lack of investment in security resources could be an important risk factor to the organization. They may use this data to better understand if the law firm has been a target in the recent past. Some organizations may wish to have ongoing updates regarding incidents or breaches even after the relationship has been formalized to continuously evaluate the law firm according to their own level of risk comfort.

Note that incident details will be of less practical value in evaluating a law firm's maturity than breach details. An incident includes every attempted intrusion or mere chance of data breach. All law firms will address incidents, and often these incidents pose little to no risk of harm, thanks to existing controls or closer analysis of the situation in the context of the prevailing regulations. If a firm states that it experiences no incidents, an organization may want to question the firm's awareness of security risks. However, if a firm provides full details of all incidents, the organization may get a false impression about the firm's ability to keep data secure. The organization may conflate mere incidents with confirmed breaches or may struggle to identify and evaluate true causes of concern due to the sheer quantity of incidents. Organizations should find more value in examining confirmed breaches and the details of how the firm responded to those breaches.

In providing information about incidents and breaches to organizations,[9] law firms must contemplate the risks created by sharing this data. A full description of a breach may include details of the personal or confidential information that was disclosed; however, the law firm could create a new instance of a data breach by providing such details to an organization. Any information shared should be carefully evaluated against relevant data protection laws, and regulations and should be presented in summary fashion or, if necessary, in more detail but with all legally protected information appropriately redacted, anonymized, or pseudonymized before sharing. The law firm should focus on sharing details regarding its breach response process, including its ability to effectively remedy the cause of the breach, instead of sharing specific and confidential details.

Above all, law firms should ensure they maintain their own privacy and confidentiality commitments. Sharing data with client organizations should only be done according to an established procedure that includes a secure method of transfer and appropriate administrative controls, such as nondisclosure agreements. Organizations should identify the purposes behind such a request, to ensure that the details they receive are only those relevant to meeting their goals.

Firms should clearly plan their protocols for advising organizations in the event of breaches. Organizations will want to learn early of any issues that might impact their data or

9. Considerations may differ when firms contemplate whether to share information with the government or with Information Sharing and Analysis Centers or Organizations. Some sharing mechanisms, notably those set forth in the Cybersecurity Information Sharing Act, 6 U.S.C. § 1501 *et seq.*, contain protections from liability and mechanisms designed to protect against the inadvertent redisclosure of personal information. Organizational inquiries regarding firms' information sharing practices are discussed briefly in Section I.C.

interests. Firms that withhold early notification run the significant risk of alienating relationships, even if the strict letter of the law did not require disclosure. Many larger organizations will have substantial expertise in-house that can provide additional resources to support a law firm facing an attack or breach situation. Law firms are well served to consult in advance of any incident with leading information security service providers as well as outside counsel with expertise in this field, particularly if the firm does not have internal expertise. Firms should run annual tabletop exercises and include a list of key contacts with government, service providers, and outside counsel who can advise in the event of a breach.

2. Technology and Infrastructure

Interactions between law firms and organizations on the issue of cybersecurity often revolve around organizational expectations of the firm's technology and infrastructure used to store and process the organization's data. Technology can be easier for an outside party to evaluate and audit than data governance, but the latter is often more important. Most security vulnerabilities and their associated risks tend to be caused by business practices and the way human beings interact with information systems and data, which cannot be mitigated through technology alone. For this reason, organizations may want to focus more on the human element and less on technology solutions in isolation. The approach suggested in this section is to focus any assessment of technology on those aspects that can most reliably mitigate human errors or malicious behavior.

The elements of technology impacting cybersecurity that are likely to be of key concern to organizations break down into several areas, all of them primarily concerned with: (1) the protection of the organization's data (confidentiality and integrity), and (2) ensuring that the firm can detect, respond, and recover from any attacks on its systems (availability). These two areas of

concern can arise in many technology areas that organizations should consider assessing. The priority/ranking will vary depending on the types of data involved and environment in which it is handled.

(a) Authentication and Access Controls

Most serious breaches and compromises of information systems and data typically involve unauthorized access into a firm's network, email system, or other information services. Current best practices are to ensure that access to a firm's information systems should be protected by additional measures beyond a login and password. Multifactor approvals are a commonly used security approach, but other developments in the authentication area that rely on more complex methods to authenticate a user are increasingly available.

In addition to authentication, organizations should examine the way a firm regulates levels of access/privileges on network accounts. A guiding principle should be to provide the lowest level of privilege needed for a particular user, a concept known as "least privilege" or "need to know." Additionally, notification systems and split passwords are becoming the standard for empowering administrative personnel with powerful IDs.

Given the myriad issues with insider threats and disgruntled employees, organizations should expect that firms will integrate governance of user accounts with human resources (HR) and physical security processes to ensure that employees who depart or are terminated are removed from access. The existence of multiple generic administrative level accounts used by Information Technology (IT) personnel or other administrative functions should also be audited.

(b) Mobile Devices

The sophistication and large data storage capabilities of mobile devices (smartphones, tablets, laptops) present a particularly challenging and growing risk to a firm's cybersecurity. Organizations should consider examining the degree to which a firm incorporates governance and technical measures focused on the security of mobile devices. These may include the use of mobile-device management applications to limit access to information and to provide means to remotely erase or lock devices that may be lost or stolen. Additionally, organizations may seek to understand the scope of information that a firm may provide through its mobile devices. Organizations will increasingly expect that firms will curtail or prohibit the use of certain types of mobile devices such as USB drives or portable hard drives, which pose a higher risk if they are misplaced, stolen, or used to exfiltrate large amounts of data.

(c) Encryption

As more regulators consider the use of encryption to enhance data privacy or protect export-controlled technology or information, legal industry standards have developed to expect at-rest and in-motion/in-transit encryption, particularly regarding internal firm data. The capability to secure communications between organizations and firms will also increasingly be viewed as necessary, and some organizations are mandating encryption at the transport level (TLS) between the lawyer and organization domains (or at the very least the use of opportunistic TLS encryption when both sides use encryption tools). For organizations with particularly sensitive matters or those involving risks of surveillance by nation states, more secure communications capabilities such as those offered by applications designed for point-to-point encryption may be required.

(d) Backup and Restore Capabilities

The resiliency of a law firm's network is of considerable interest to organizations, something that has been made clearer in the aftermath of recent attacks aimed at destroying access to systems and data. Organizations will be expected to focus on the extent to which a firm has the proven and tested capability to restore systems, whether from an attack, a power outage, or another natural or man-made emergency. Organizations may expect firms not only to have such plans in place, but to be able to demonstrate that they test these on a regular basis. This is one area where extensive industry practices exist, and organizations can rely on these best practices to audit a firm, including ensuring backups are stored in different locations.

(e) Cloud-Based Storage and Services

Any communication system connecting two entities raises the potential for compromise and the dissemination of malware or other attacks. The primary concern most organizations have regarding law firm use of cloud services revolves around this cybersecurity issue and its potential impact on the organization's confidential information, so organizations may need to review whether a firm has in place methodologies or protocols for addressing the risks posed by these systems. Some organizations with particularized needs because of their work with export-controlled information may also have requirements to ensure that such information is segregated and is not being exported due to being hosted on a cloud service or being accessible to unauthorized persons. A firm should expect to be asked for an inventory of cloud-based storage and services and for assurances that the firm has undertaken diligence of these services and appropriate contract provisions to safeguard confidential information.

(f) eDiscovery Tools and Databases

The proliferation of eDiscovery applications used in litigation or databases for the review of confidential deal information risks exposing massive amounts of the organization's data, sometimes involving the most sensitive aspects of an organization's operation. Firms involved in litigation, acquisitions, or other work involving the review of organizational or opposing party information may be expected to factor in the security of these systems, but this may pose challenges when these systems are put in place by the organization versus being maintained by third parties. To the extent the law firm is involved in the vetting and selection of these systems, it should put in place a process to ensure that the litigation support department—typically in charge of these resources—adequately reviews cybersecurity risks and vulnerabilities, including periodically reviewing and testing service provider controls as appropriate.

(g) Billing Software/E-Billing Connections

As with cloud-based services, the extent to which privileged or sensitive information is shared by the law firm with e-billing service providers will be an area of concern for organizations, particularly if the system is a cloud-based application.

(h) Server and Infrastructure Protection

The protection of physical and electronic access to electronic systems should be considered a priority by organizations. Law firms should expect to be queried regarding their process to ensure physical security of server rooms and other sensitive equipment as well as system controls. The server rooms and sensitive equipment should be segregated, protected by industry-standard endpoint protection, and access limited to authorized users, with logging of access. However, firms should not be expected to provide detailed information regarding these measures, as

doing so will put these measures at risk of unauthorized disclosure. Third-party certification can be effective in resolving an organization's concerns regarding the sufficiency of these controls and protections.

(i) Auditing and Network Monitoring

Organizations may increasingly expect that law firms will have in place more extensive network security tools to permit in-depth monitoring of activity, including indications of large-scale exfiltration of data or efforts to conduct reconnaissance inside the network. Such capabilities will need to be integrated into the firm's operations to ensure that information, when received, is acted upon timely. Organizations also are likely to be concerned about logging and preservation of network activity, which will help identify the nature and extent of any compromise post-incident. These logs should also be a part of retention policies to minimize the complexity of managing old data.

(j) Firewalls, Antivirus Software, and Malware Protection Tools

Organizations will look for law firms to have in place the standard suite of firewall, antivirus, and malware security tools. Organizations may press firms to have regular reviews and updates to the technology as such technologies advance. A key challenge for firms and organizations will be finding consensus on the utility of these evolving technologies relative to the cost and complexity to manage.

(k) Records Retention

Law firms should implement an appropriate records retention policy that considers both legally required retention as well as best practices related to the disposition of data. Firms should work with organizations to clarify how long the organization's data will be retained following the completion of a matter or the

end of the relationship. This should be driven by a retention policy that is consistently followed. Firms that fail to appropriately dispose of data increase their vulnerability to breaches and may face a difficult defensibility argument if the firm's failure to timely dispose of information prejudiced the organization in the event of a breach.

3. People

One of the main areas of concern for most organizations is and will continue to be managing the cybersecurity risks posed by a firm's lawyers and staff. These risks break down into several main areas, each with unique challenges for mitigation.

(a) Malicious Insider Threats

Malicious insiders who steal or destroy law firm systems are a difficult vulnerability to mitigate. Organizations may increasingly expect that firms of a certain scale, or those working with particularly sensitive information such as national security or critical infrastructure, have in place some type of insider threat program. Implementing these programs is challenging even for larger organizations with extensive security resources and requires close integration of management, HR, IT, and security. Such programs also have resource implications involving the education of staff and lawyers and putting in place more focused monitoring of employees. For example, a firm may require lawyers and staff to undergo regular background checks and to self-disclose life events that may be early indicators of heightened risk. This needs to be considered in conjunction with jurisdictional regulations and appropriate handling of this data.

(b) Lack of Technical Competence

Organizations will assess how well a law firm manages the human factor in cybersecurity by focusing on the firm's policies and governance, the way the firm educates and trains its

employees, and how it implements remedial measures. Taken together, these factors likely will be perceived by organizations as equating to a security culture rating for the firm. Organizations may want to look at these issues through several prisms:

- Education—focused on broader concepts and expectations around information security.
- Training—focused on mandatory training for all computer users, including competency or testing assessments built into the training modules; competency on systems and software; and familiarity with risks, vulnerabilities, and threats.
- Governance—standards the firm sets for lawyers and staff through policies and expectations and how these standards are enforced through discipline.

Organizations should be particularly mindful that law firm culture often is markedly different than those of many organizations, public or private. Many firm partners function effectively as their own CEO, leading to more prevalent risks from behaviors that are not in compliance with firm policies but are not addressed by the firm's professional staff, who may perceive they lack the standing or influence to challenge lawyer, and particularly partner, behavior.

It is also particularly important to ensure that law firms have committed to training requirements for all personnel that includes intra-course tests to determine whether the participants comprehended the learning offered in the course. One of the weaker links of a law firm security system can be the vulnerability of partners who are focused on billable work and less attentive to security issues. Effective phishing and malware strategies focus on these vulnerabilities by designing campaigns intended to encourage partners to "fall for" malicious emails.

(c) Service Providers

Organizations will want to look at the law firm's selection and contracting processes for service providers that provide legal services for the organization. This is particularly true when firm service providers will receive the organization's sensitive data, such as a cloud-based service for file transfer or document management. Best-practice checklists and frameworks have been published by other organizations and may be useful resources to identify detailed topics of discussion between organizations and firms.[10]

Organizations likely will be interested in how firms selected any service providers who might handle the organization's data. Two key questions organizations may have about a firm's provider selection process are: (1) Does the firm use a selection process that will provide the firm with a sound understanding of a provider's service delivery model; and (2) Does the firm use a selection process that will select providers who facilitate, rather than undermine, the firm's own assurances to organizations. It is important for organizations to approach these inquiries with the right frame of mind, recognizing that for many or most law firms, deployment of service providers is as likely to improve security as to undermine it.

Fundamentally, if a firm selects a service provider on behalf of an organization or otherwise uses a provider's services for

10. The Vendor Contracting Project of the American Bar Association's Cybersecurity Legal Task Force published a Cybersecurity Checklist that addresses vendor selection and contracting, *available at* https://www.americanbar.org/content/dam/aba/images/law_national_security/Cybersecurity%20Task%20Force%20Vendor%20Contracting%20Checklist%20v%201%2010-17-2016%20cmb%20edits%20clean.pdf (Oct. 17, 2016). The Draft Version 1.1 of NIST's Cybersecurity Framework includes discussion on supplier selection, contracting, and oversight, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (April 16, 2018).

law firm systems, the law firm has an ethical duty to ensure that the provider is appropriately addressing cybersecurity issues, particularly if the provider's systems hold data that if released or compromised would prejudice the organization. Where firm service providers may gain access to the organization's data or to a firm's critical information systems, organizations have an interest in the firm's vetting of those providers and their privacy and security posture.

4. Insurance Coverage

Organizations have an interest in understanding how firms have chosen to transfer or share the risk of a cybersecurity incident. These questions and their answers can indicate the law firm's ability to make the organization whole if the latter is harmed by such an incident. Details about a firm's insurance coverage can indicate a level of cybersecurity maturity. The insurance company may have performed an assessment of a firm's cybersecurity practices or provided guidance on appropriate risk management actions.

A firm may have a variety of insurance coverages to protect against risks, such as damage to property or malpractice lawsuits. The following questions may provide an organization with insight about cybersecurity issues. Since the insurance market for cybersecurity risks is far from standardized, and many insurers create their own, custom coverage forms, the organization and firm may wish to review, in high-level terms, the scope of the coverage and the organization's protection under it.

- Does the law firm use insurance to supplement information security?
- If so, does the insurance coverage provide:
    - First-Party Coverage: to reimburse the firm for costs that occur when a breach is

discovered? These costs may arise from hiring professional investigators and advisors, notifying affected individuals and providing credit monitoring, and restoring the firm's operations so they can continue to serve organizations.

- Third-Party Coverage: to reimburse third parties, such as the organization itself, for harm that results from a breach? This coverage may include the cost to defend the firm against lawsuits and cover regulatory penalties.

These coverage details will indicate to the organization that a cybersecurity incident is not necessarily an existential or solvency risk to the law firm.

Firms should indicate if organizations will be named as an additional insured, which provides an organization with an added benefit by making their coverage claims easier to verify. Organizations should consider requesting a copy of the additional insured endorsement. Firms should explain how the policy will address incidents that occur before the effective date of the coverage, since cybersecurity incidents can be ongoing or can take time to discover.

Additional questions regarding audits and security practices:

- Did the insurer perform an audit or other assessment as part of the application or underwriting, and may the organization access or receive a copy of their report?
- Does the insurance policy require the firm to meet minimum security practices, or include an exclusion for the firm's failure to follow such minimum practices? If so, what procedures and

risk controls are set forth in the application or policy?

- Does the firm perform audits directed by the insurance broker to assess risks, and may the organization access or receive a copy of the latest version?

Additional details (if desired):

- What coverage and limits does the insurance provide for customer data?
- What deductible, if any, could an organization have to pay for a claim?
- Does the policy cover losses caused by third-party vendors of the law firm?
- Does the policy cover ransomware and/or cyber extortion?
- Does the policy cover misdirected email or other "Business Email Compromises"?
- What is the claims process? Do additional insureds control their rights to recovery?
- Is the policy a duty-to-defend or duty-to-reimburse-defense-costs policy? Do defense costs exhaust the policy's limit? What are the provisions regarding the selection of defense counsel?
- Will the law firm provide a certificate of insurance at the outset of the engagement and annually?
- Does the law firm need or have international coverage or separate social engineering attack coverage?

B. Outside Counsel with International Operations

Due to modern technological and regulatory advancements, many organizations now conduct some level of operations in an international jurisdiction other than the one in which they are domiciled. Likewise, law firms may represent organizations in international matters and have worldwide offices as part of a global practice, or they may simply employ a third-party service provider based in another country who has access to the firm's data.

Firms should provide organizations with details regarding the parties with whom, and locations where, their data will be shared. Organizations should consider cross-border security issues in the context of both: (1) the firm's ability to comply with jurisdictional requirements, and (2) what elements of risk will be introduced if the organization's data travels across borders.

Some jurisdictions may have unique information security requirements, along with unique mandates relating to an individual's ability to access data about oneself. While it is beyond the scope of this document to list all possibilities, of note in this regard is the European Union (EU) General Data Protection Regulation (GDPR), which organizations must follow if they collect or process information relating to residents of the EU. Organizations whose data includes information on EU residents should request details on how firms will ensure their practices comply with GDPR requirements.

Governments vary in their abilities and willingness to abrogate confidentiality and compel the disclosure of data held by private parties. Organizations must be cognizant of the fact that data stored in or passing through a country other than their own may become subject to that foreign jurisdiction's laws and enforcement mechanisms, and they should inquire whether firms with international offices have considered local-law limitations on the use of encryption or VPNs and rule-of-law challenges

posed by less-developed search-and-seizure frameworks in the countries where they use or store client information—paying particular attention to any policies the firm has in place regarding travel across borders with confidential information.

Organizations should ensure they understand any outside parties in international jurisdictions with whom law firms will share the organization's data, such as local contract or agency attorneys. For example, firms that rely extensively on contract attorneys for patent work or document review in local jurisdictions should have a more developed process to assess the risks of sharing information and work product with these service providers. Organizations should request details on this risk assessment if this situation applies to their data.

C. *Efforts to Coordinate Among Industries and to Set Common Standards*

Organizations may also have questions about law firm efforts to coordinate among themselves. Mature firms should consider participating in Information Sharing and Analysis Centers (ISAC) or Organizations (ISAO) or other risk-focused groups that disseminate the most recent intelligence about threats, incidents, and mitigating steps the firm can take to prevent or reduce risk. Organizations should request details on the firm's participation in such information sharing groups and other cybersecurity and data protection trade organizations.

The Cybersecurity and Infrastructure Security Agency (CISA) has engaged in outreach, including to law firms, designed to provide resources and guidance on trends and tools and to serve as a clearinghouse for information sharing. Under the Cybersecurity Information Sharing Act of 2015, private entities, including law firms, receive antitrust protection if they participate in information sharing activities. Further, the provision of cyber threat indicators and defensive measures to the

government does not waive an otherwise applicable privilege or legal protection. Finally, properly designated shared information remains proprietary and exempt from scrutiny under freedom of information acts. CISA and the Department of Justice regularly hold joint conferences on cybersecurity issues, including conferences for lawyers that focus on the unique exposures facing the legal industry.

The FBI also provides extensive support to the private sector, including law firms, on cybersecurity issues. Law firms should reach out to their local FBI and Secret Service field offices to develop a relationship with these law enforcement personnel who can serve as a resource as well as a key contact in the event of a cybersecurity incident.

III. CONSIDERATIONS FOR HOW AN ORGANIZATION SHOULD COMMUNICATE WITH OUTSIDE COUNSEL ABOUT THE SECURITY OF THE ORGANIZATION'S DATA

This section will discuss practical steps regarding communications about data security between an organization and its law firm(s), including how to begin such discussions and how to maintain an ongoing dialogue about data security. No single approach is appropriate for every organization. Factors to consider include: the nature of the organization's business, the degree of regulation of data security and privacy applicable to the organization's business or information, the nature of the work done for the organization by a firm, the type of information received from or created for that organization that the law firm will retain, and issues of organizational culture.

A. How Outside Counsel's Data Security Becomes Part of the Process at the Organization

The best way to encourage stakeholders at the organization to focus on law firm data security will depend upon the structure and culture of the organization. In most instances, it is likely that the in-house counsel function will take a leadership role. In most instances, outside counsel is engaged through the organization's legal function, and the in-house counsel's office acts as gatekeeper. In organizations where outside counsel hiring is decentralized, or delegated to a nonlegal function, in-house counsel's role may be one of educating the gatekeepers about the importance of data security and providing them the tools with which to protect organization data. In all organizations, the people performing the IT function and responsible for data security should be consulted. For example, suppose responsibility for the selection of outside counsel to defend insurance coverage litigation is delegated to the leadership of the underwriting function. In those circumstances, the office of the

chief legal officer, working in conjunction with the organization's IT security personnel, might create information security standards with which outside counsel should comply, provide those standards to the underwriting function leadership, and then provide training to that leadership about the data security issues behind the standards and best practices for their implementation.

B. When to Engage Outside Counsel about Its Data Security Practices

In theory, outside counsel's data security capabilities should be thoroughly evaluated and approved *before* outside counsel is engaged. Where the law firm regularly does work for the organization, or is part of an outside counsel panel, data security vetting can readily be implemented before outside counsel is engaged. However, there will be many instances due to a matter of urgency in which the organization must engage counsel who is not on a panel or with whom the organization has not previously worked. Examples of such an urgent situation include litigation in an unfamiliar jurisdiction or requiring specialized expertise, government or internal investigations, and certain types of transactions. In those instances, organizations may address law firm data security at a high level during the initial engagement phase and follow up with a more detailed process as time permits. Such basic information might include the law firm's data security policy and information about the law firm's cybersecurity insurance coverage.

Alternatively, or in addition, organizations can mitigate risk by disclosing the organization's data to the law firm via a secure site already vetted for data security and controlled by the organization. For example, suppose an organization is sued in a preliminary injunction action in a rural state court and needs to retain counsel immediately. The case involves trade secrets, including the secret formula for the organization's largest

selling product. The best lawyer for the matter is a solo practitioner with a very basic computer setup who relies upon a local cloud storage provider for most data storage. The organization does not have time to investigate the data security practices of either the solo practitioner or the cloud service provider before substantial work must be done. Instead of transmitting highly sensitive documents to outside counsel, the organization could instead use a third-party hosting platform maintained by a tier-one provider whose data security practices previously have been investigated rigorously by the organization.

C. Who Engages Outside Counsel about Its Data Security Practices

Who at the organization engages in the conversation with outside counsel about law firm data security will depend on a variety of factors. In some instances, in-house counsel leads the conversation. If a specific business unit is responsible for the law firm relationship, the conversation might be led by the business unit. For example, where engagement of outside counsel is managed by the procurement department, then the procurement department may take the lead. Some organizations look to their IT function to manage law firm data security. Regardless who takes the lead in the conversation, it is advisable for the leader to get input from each stakeholder within the organization so that their needs are met. In larger organizations, it may be beneficial and efficient to form interdisciplinary teams to manage communications with counsel. For example, some larger or more heavily regulated organizations have established formal information risk management, data security, or cybersecurity functions.

Consideration should be given to segmenting outside counsel into groups by the nature and volume of the organization's information shared with each group of law firms. For example, consider an organization in the health care services business. It uses three regional law firms in Group A to handle disputes

with patients and medical insurance providers. It uses five law firms in Group B to handle its commercial real estate needs. The organization's procurement department engages the law firms in Group B for the real estate matters. The information provided to the law firms in Group A is subject to far more extensive and detailed regulation than the information provided to the law firms in Group B. In these circumstances, it is advisable for in-house counsel with knowledge of the applicable data privacy regulations to take the lead on communications with law firm Group A, whereas it may be reasonable to rely upon the procurement function to take the lead on communications with law firm Group B, with appropriate input from the legal and IT functions.

Where communications are handled by the procurement or IT functions, they will sometimes use the same questionnaires and communications for law firms as they do for other types of vendors.[11] In-house counsel may wish to review those communications. Law firms are different from other vendors in many respects, and consideration should be given to whether the same information should be sought from both outside counsel and other, non-law-firm vendors. As set out elsewhere in this paper, there are numerous data security considerations that are unique to law firms, and there are data security issues that are important to non-law-firm providers but do not apply to law firms. Corporate counsel should review "one size fits all" vendor questionnaires that are sent to law firm and non-law-firm vendors to confirm that all important issues are addressed. Deference should be given to questions from the model questionnaire set out in Appendix 2 of this *Commentary*.

11. The term "vendor" is used here to refer broadly to providers of goods and services to the organization and not narrowly to providers of services to the legal function.

The organization should also consider the impact of privacy rules that limit to whom within the organization particular information may be disclosed. Such privacy rules may affect who communicates with a law firm about the information subject to such rules.

D. The Organization's Point of Communication at Outside Counsel

The organization also should consider with whom at the law firm they communicate about data security issues. Law firms follow a variety of approaches to managing their data security function. In some instances, communications are handled at the law firm by the relationship partner. Sometimes the law firm will designate someone within the IT organization to respond. In other instances, law firms that have an in-house "general counsel" function may designate lawyers from the general counsel function to respond. Some larger law firms may designate a multidisciplinary team to respond.

Should in-house counsel leave it to the law firm to decide who should handle communications? Not necessarily. In-house counsel has an interest in making sure that it is getting the information it needs and that the information appears to be complete and reliable. In making that determination, in-house counsel should consider the nature and volume of the organization's information shared with counsel. Law firms should welcome a dialogue with their existing and prospective clients about how best to collaborate on securing collective data.

E. Data Security Questionnaires

1. Questionnaires and Their Alternatives

Data security questionnaires are used widely by organizations to create the foundation for discussions with outside counsel about the law firm's data security. While this *Commentary* advocates for the use of the Model Questionnaire in Appendix

2, there may be other ways to gather information. For example, in some situations, such as urgent matters described above, in-person or short "email interviews" may be conducted in lieu of a lengthier questionnaire process.

2. Documentation Requests

Each organization should consider which documents the law firm should be required to disclose. Which documents to request will depend upon nature of the organization's business, the nature of the work performed by the law firm, and the types of documents and information provided by the organization to the law firm. At a minimum, the organization should expect the law firm to be able to make available for review the firm's data security policy, a statement of its cybersecurity insurance coverage, and validation of the security assessments the firm has performed with any subcontractors that will hold the organization's data and information.[12] It is in the best interests of both the organization and the law firm to share information by screen share rather than requiring the law firm to send copies of data security documentation to the organization. Keeping the law firm's information secure within the firm's own systems helps maintain the confidentiality of the firm's data security practices, which ultimately benefits both the firm and the organization whose information the firm holds. Moreover, an organization

12. An organization's first instinct might be to also request the law firm's data breach response plan. Each organization should consider whether such a request is in its best interest. Data breach response plans can reveal confidential aspects of the law firm's data security architecture. It is in all parties' interests to minimize the dissemination of such key information. Therefore, organizations should strongly consider relying upon the law firm's representation that it has a data breach response plan.

may not want to assume additional risk to itself by retaining sensitive data security documents of other organizations.[13]

3. Questionnaire Format

A wide variety of practices are currently used for presenting questionnaires to law firms. Some larger organizations use web-based forms to collect the information and automatically populate database tools that synthesize the information on the organization's end. Other organizations use forms created in a word processing program such as Microsoft Word or Google Docs or spreadsheet programs such as Microsoft Excel.[14] Still other organizations use third-party hosting systems or tools to elicit information.[15] Whichever approach the organization decides to use, the form needs to be sufficiently flexible to permit the law firm to make needed disclosures. Organizations should recognize that law firm network architecture and security processes may vary widely. If the organization decides to use a heavily formatted form to present its questionnaire—for the valid purpose of receiving uniformly formatted responses—the

13. If the organization decides to obtain copies of the law firm's data security documentation, it should return or securely destroy the materials promptly upon completion of its review to minimize the risk of unintended disclosure of sensitive law firm information that could jeopardize the security of the organization's own information in the hands of the firm. Law firms may include confidentiality clauses in their nondisclosure agreements (NDAs) to address proper handling, including retention and destruction of any data collected in relation to audits/assessments.

14. Macro-enabled forms, such as spreadsheets, are often blocked by law firm security systems as a risk-control measure. The organization should consider providing flexibility to disable macros to reduce security risk to both parties' systems.

15. If using a third-party system or tool, the organization should carefully vet the vendor and only use vendors with which the organization would trust its own information. Law firms may include "right to audit" clauses if an organization chooses to use a third party to store assessment data.

organization should also provide a space for the law firm to provide additional information in free-text form. Organizations also should recognize that law firms will often need to obtain input from multiple people within the firm to respond to the different questions. Therefore, the organization should permit the law firm to export the questionnaire into a format the firm can work on "in draft."

4. Processing Questionnaire Responses and Documentation

The organization should have a reliable process for reviewing questionnaires and following up. The organization should involve personnel with sufficient technical expertise to identify issues that are significant to the organization. Smaller organizations that do not have in-house security functions should consider engaging an outside IT consultant to assist in evaluating the responses. If the questionnaire is worded with care and precision, insufficient answers (e.g. incomplete or nonresponsive replies) should be obvious on their face. Organizations should consider documenting both their review process and the conclusions reached at the end of the process. Organizations should be entitled to accept their outside counsels' responses as accurate. The attorney-client relationship is governed by stringent ethical rules not found in most other businesses, including enhanced obligations of disclosure and candor. In addition, outside counsel have strong incentives to preserve their good reputations.

5. Addressing Unsatisfactory Responses

If an answer from the law firm does not satisfy the organization's requirements, the organization should initiate a dialogue with outside counsel to gain a more detailed understanding of counsel's data security processes and practices. The organization should request additional information about the responses of concern. Sometimes counsel's response may be based upon a

misunderstanding. The organization may determine that counsel has security processes and practices that mitigate the risks indicated by the answers of concern. Dialogue will also inform the organization's understanding of the materiality of the deficiency and may suggest alternatives to protect organization data. The organization should consider requiring outside counsel to alter its data security practices only in the case of material deficiencies that threaten information of significant sensitivity.

F. Frequency of Review

The frequency with which the organization reviews outside counsel's data security practices should depend upon several factors, including: the nature of the organization's business, the degree of regulation applicable to information shared with counsel, and the nature of the organizational documents and information provided to the law firm. Generally, the more extensive and sensitive the information provided, the more frequent the review should be. Organizations should recognize that reviews consume organizational resources. It is appropriate for organizations to balance the benefit of more frequent reviews against the cost of internal resources required to conduct and follow up on the review. Organizations also should recognize that these reviews impose burdens upon law firms that increase the firm's cost of doing business. Organizations and law firms might consider a hybrid approach under which the organization does a comprehensive review every three to five years, with partial updates annually between full reviews. There may be a few questions from the Model Questionnaire that the organization wants to address annually with its law firm(s).

G. Audit Requests

Audits of a law firm's data security practices can provide additional protections to an organization. Audits can also provide advantages to law firms. Law firms that take security seriously

may see the audit process as an opportunity to collaborate closely and build relationships with an organization that is an established or prospective client.[16] But audit requirements should not be imposed by organizations reflexively. Organizations should first consider the goal of the audit and ask whether the organization's goals might be achieved in a different and less expensive way. For example, if the goal of the audit is to test data breach response processes, would a request for evidence of a tabletop exercise be more effective?

Organizations also should consider limiting the audit to the portions of the law firm's activities that involve the organization's most sensitive information. For example, if the organization only transacts business with a law firm by email or secure file transfer, it may be unnecessary to audit the law firm's website or application development process. If the audit is conducted by the law firm itself, organizations should consider how much value the audit provides. Third-party audits are of greater value to the law firm and the organization but may entail considerable cost. Ultimately, organizations and law firms should work together to create a certification program that will enable firms to satisfy data security requirements for multiple institutional clients, without the need for costly audits.

H. Privilege and the Organization's Communications with Outside Counsel

Ordinarily, the attorney-client privilege covers confidential communications between an attorney and a client with respect to obtaining legal advice from the attorney.[17] There is an issue

16. Providing a law firm with opportunities to discuss its client's data security needs may enhance the law firm's development of more secure solutions, which benefits both the organization and the law firm.

17. *See* United States v. Upjohn, 449 U.S. 383, 390 (1981) ("[T]he privilege exists to protect not only the giving of professional advice to those who can

as to whether communications about the law firm's data security practices are for the purposes of legal advice that the firm will give to the organization. It is likely to be argued that the information relates to nonlegal, technical, and business advice. A party opposing application of the privilege may also argue that the law firm is not a disinterested counselor in that the firm is seeking to be engaged to represent the organization and therefore cannot give impartial, disinterested advice as to the adequacy of its own data security practices. Whether communications between the law firm and the organization will be considered privileged will depend on the facts and circumstances applicable to each specific communication. Therefore, the organization may want to approach its communications with the law firm, including due diligence, with the knowledge that the communications may not be privileged and manage its communications accordingly.

I. Outside Counsel Data Security and the Engagement Letter

An organization should include in its engagement letter with outside counsel the data security requirements that will apply to the law firm. Data security requirements should address issues both during the engagement and after the engagement's conclusion. Model clauses to include in the engagement letter are provided in Appendix 1 to this paper.

---

act on it but also the giving of information to the lawyer to enable him to give sound and informed advice.").

APPENDIX 1—MODEL CLAUSES FOR AN ENGAGEMENT LETTER

Information Security Guidance Addendum To Retained Counsel Agreement

This Information Security Addendum is incorporated, effective _____, 20__, into the Retained Counsel Agreement dated (the "Agreement") [INSERT DATE] between [INSERT FIRM NAME] ("Retained Counsel") and [INSERT ORGANIZATION NAME] ("Organization"). Guidance will be updated as necessary to reflect changing technology and new security threats. In addition to the terms set forth in the Agreement, Retained Counsel agrees to the following provisions:

1) Retained Counsel has and will maintain and document a comprehensive Information Security Program that complies with all applicable laws and regulations and is reasonably designed to identify, protect against, detect, respond to, and recover from threats to nonpublic information obtained by or provided to Retained Counsel that was created, compiled, modified, or received by Organization or its agents, whether that information belongs to Organization or to a third party ("Organization Information"), when that information is created or collected, in transit, being processed, at rest in storage, or destroyed.

2) Retained Counsel will use Organization Information only for the purposes for which Organization provides it, as described in the Agreement. Retained Counsel will not distribute, share, or provide Organization Information to any other party, except as authorized in connection with the representation, without the express permission of Organization, except as required to comply with a regulatory or legal process;

3) Retained Counsel has designated one or more specifically named employees responsible for the administration of its Information Security Program and will provide the names and titles of the individual(s) and their direct contact information to Organization;

4) Retained Counsel will regularly identify, assess, and mitigate the risks to the security, privacy, and confidentiality of Organization Information in Retained Counsel's operations and evaluate the effectiveness of the safeguards controlling against these risks.

5) Retained Counsel will regularly monitor its Information Security Program and assess the program at least once per year and be prepared to inform the Organization of any results upon request.

6) Retained Counsel will restrict access to Organization Information to those employees, agents, or subcontractors having a need to know the information to perform their jobs regarding Retained Counsel's representation of Organization, including but not limited to individuals involved with Information Technology maintenance, security, and forensic investigation.

7) Retained Counsel will maintain an Incident Response Plan that identifies, analyses, and, if needed, corrects an information security incident to prevent a future incident reoccurrence, which it will review and update at least annually.

8) Retained Counsel will, at its own expense, provide notice to Organization of any occurrence that could compromise or threaten the confidentiality, integrity, or availability of Organizational Information or the receipt of a complaint

regarding the privacy or security practices of the law firm (a "Security Incident"), if that Security Incident exposes Organizational Information (a "Breach") within 72 hours of discovery, along with any information reasonably requested by Organization to understand or remediate the Breach, to the extent allowed by law. Information to be provided will include, but will not be limited to, the name and contact information of an employee of Retained Counsel who will serve as Retained Counsel's primary security contact, who will cooperate fully and assist Organization in and understanding the nature, root cause, and resolution of the Breach. The notice called for in this section will be given to:

[ADD ORGANIZATION CONTACT NAME
and an alternate designee]

9) Retained Counsel will, at its own expense, take reasonable steps to remedy any Breach and minimize risk of future Security Incidents or Breaches in a timely manner and in accordance with all applicable laws and regulations. Retained Counsel will reimburse Organization for reasonable costs incurred by Organization in responding to, and mitigating damages caused by, any Security Incident or Breach attributable to Retained Counsel, including all costs of notice and/or remediation deemed necessary by Organization to comply with applicable laws. Organization will have the right, at its option, to solely provide and/or control any notice(s) to Organization customers, employees, or others impacted or potentially impacted by such Security Incident or Breach. Retained Counsel will not provide any notices or discuss any Security Incident or Breach with any other party without Organization's prior written consent, except as required by law, by other contractual agreements like this one, and as

needed to investigate and remediate the Security Incident or Breach. Retained Counsel shall be able to notify its clients of the existence of a security incident and/or breach, although no identifying information regarding the Organization shall be provided.

10) Upon reasonable notice, Retained Counsel will allow Organization to review, assess, and inspect Retained Counsel's Information Security Program upon request and upon execution of appropriate Nondisclosure Agreements. Organization may conduct an annual review of Retained Counsel's comprehensive Information Security Program by providing to Retained Counsel a questionnaire to be completed by Retained Counsel and returned to Organization.

11) Retained Counsel will, at Organization's request, destroy or return all Organization Information in its possession and certify to Organization in writing that Retained Counsel has done so, unless necessary to require with Retained Counsel's legal obligations and/or any disputes with Organization within the applicable statute of limitations. If Retained Counsel destroys Organization Information rather than returning it, Retained Counsel will use destruction methods that comply with all applicable state and federal laws and regulations. This obligation to return or destroy information will not, to the extent reasonable, apply to Confidential Information that is stored in backup or other disaster recovery systems, archives, or other storage systems that make it impractical to destroy the information. If Retained Counsel continues to hold Confidential Information after Organization requests return or destruction of the information, its obligations

under this Agreement will continue to apply for so long as it continues to hold such information.

12) Retained Counsel shall not use or collect any Organization-supplied information and/or information accumulated about Organization during the representation (e.g., analytics, statistics, etc.) unless such information is anonymized and/or Organization is given reasonable notice of its use or collection.

13) Retained Counsel will obtain Organization's written consent before using any third party to provide services to Organization or involving Organization Information if that third party's handling of Organization's data is significantly different than already agreed/approved systems. Retained Counsel will require all third parties providing services regarding Retained Counsel's representation of the Organization to agree, in writing, to provide safeguards and breach notice for Organization Information equivalent to those as set forth in this Addendum. Specifically, Retained Counsel has confirmed that any records, data, information, and/or analytics that a third party creates regarding Retained Counsel's representation of the Organization shall be owned entirely by the Organization. This obligation does not apply to general purpose vendors used by Retained Counsel to provide general services to the entire law firm, provided Retained Counsel has reviewed and approved the information security controls of such vendor and has bound them by contract to protect Organization Information.

14) Retained Counsel agrees to carry out a background check on its non-attorney employees with access to the Organization's information, including a review of their references, employment eligibility, education, and criminal

background to help minimize risk to the security of Organization Information or Organization employees and further agrees to ensure the credibility and reliability of its employees with access to the Organization's information. Retained Counsel will at the request of the Organization provide a report of its background check without revealing the identity of its employees.

15) Retained Counsel and Organization will safeguard all information and items provided to each other in order to allow other party to access Information, including but not limited to, other party's computer networks, premises, service providers, clients, keycards, codes, usernames, passwords, keys, badges, etc., as well as information that, if disclosed, would compromise the security of Organization or Retained Counsel Information, such as the designs of other party's networks, information controls, or design of its computer systems.

16) Retained Counsel will store, to the extent possible, all media that encode or contain Organization Information, including hard drives, flash drives, or other media, in a secure, protected media storage area that is physically and environmentally controlled and protected, with appropriate physical security to prevent unauthorized access.

17) Retained Counsel has implemented or will implement the following safeguards for systems that process, store, or transmit Organization Information as agreed upon with Organization:

- Identity and Access Management that includes but is not limited to the use of complex passwords that comport with the latest guidance from the NIST.

- Encryption of particularly sensitive Organization Information (PII, PHI, etc.) in transit (e.g., via email, FTP, internet, etc.);
- Encryption of portable media, laptops, desktops, smartphones, mobile devices, and any new technologies that store Organization Information;
- Multi-factor authentication for remote access to Retained Counsel's networks;
- Training of all employees, agents, and subcontractors with current or potential access to Organization Information upon hire and at least annually thereafter, regarding their obligations to implement Retained Counsel's Information Security Program;
- Disciplinary measures, up to and including termination of employment or engagement, for employees who violate Retained Counsel's Information Security Program;
- Measures to prevent former employees, agents, and contractors from accessing Organization Information after the termination of their employment or engagement by Retained Counsel;
- Appropriately configured and updated firewall, antivirus, and anti-malware software;
- Prompt addition of vendor-recommended security patches and updates to systems and other applications;
- Intrusion detection and prevention systems with appropriate logging and alerts to monitor access controls and assure data integrity and confidentiality;

- Separation of Duties;
- Infrastructure and Physical Security; and
- Disaster Recovery Planning.

[INSERT NAME OF RETAINED COUNSEL]

By: _____

Name: _____

Title: _____

Date: _____

[INSERT NAME OF ORGANIZATION]

By: _____

Name: _____

Title: _____

APPENDIX 2—SAMPLE LAW FIRM QUESTIONNAIRE

GLOSSARY

Breach: A Security Incident that exposes Organization Information.

Incident Response Plan: A documented plan for responding to and recovering from a Security Incident.

Information Security Program: A set of policies and processes designed to identify, protect against, detect, respond to, and recover from threats to digital and non-digital information when information is created or collected, in transit, being processed, at rest in storage, or destroyed.

Organization Information: Any nonpublic information obtained by or provided to Retained Counsel that was created, compiled, modified, or received by Organization or its agents, whether that information belongs to Organization or to a third party.

Security Incident: Any occurrence that could compromise or threaten the confidentiality, integrity, or availability of information maintained by a law firm or its third-party vendors or the receipt of a complaint regarding the privacy or security practices of the law firm.

QUESTIONNAIRE

	Rating[18]	Evidence Required?[19]	Name of Document
1. General Security			
Question 1.1.			
Do you have a documented Information Security Program? If so, please be prepared to provide it.		Yes	
Sample response: Yes, our firm maintains an Information Security Policy and Health Insurance Portability and Accountability Act (HIPAA) Policy.			
Comments: All law firms should have an Information Security Program. If the firm handles information for covered entities under HIPAA, it should also maintain a HIPAA Policy. Other policies (e.g., Payment Card Industry (PCI) compliance) may be needed depending on the law firm's practice areas and client base.			

18. Rating scale: 1 = unacceptable; 2-3 = questionable, may want to ask further questions; 4-5 = reasonable.

19. Evidence Required: Yes indicates evidence should be prepared to be shared via screen-share or on-site visit following an executed NDA.

	Rating[18]	Evidence Required?[19]	Name of Document
Question 1.2:			
Are the policies and processes in the Information Security Program cross-referenced to and based on applicable laws, regulations, industry standards, business standards, or operational standards (e.g. National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), HITRUST, International Organization for Standards (ISO), etc.)? If so, please list which ones.			
Sample response: Our firm's Information Security Policy is consistent with industry standards and is mapped to NIST.			
Comments: Many firms use the NIST Cybersecurity Framework; other acceptable standards may include ISO27001.			
Question 1.3			
Who must comply with the policies in the Information Security Program (partners, employees, service providers, contractors, etc.)?			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: All users with network access must comply with the policies in our Information Security Program.			
Comments: Law firms must ensure that service providers and consultants comply with appropriate aspects of the Information Security Program. No "exceptions" should be given for attorneys unless they are reviewed by the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or appropriate management.			
Question 1.4:			
What security certifications and attestations do you have?			
Sample response:			
Comments: The need for these certifications may vary depending on the law firm's size, work, and client base, and some may be cost prohibitive for smaller firms. Organizations should consider whether it is sufficient for a firm to meet the standards of ISO27001 without the certification process. Further, consider asking what specific functions/services are covered by the certification; ISO27001 and Service Organization Control (SOC) are scoped at the discretion of the organization being assessed. Various consultants can review these reports to determine if they cover areas crucial to in-house counsel.			
Question 1.5:			
Will your certifications and attestations remain in place for the duration of the contract?			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes, all certifications are anticipated to remain in place.			
Comments: This question is to ensure that any certifications that exist as of the day the questionnaire is completed do not expire, thereby exposing the organization to unnecessary risk.			
Question 1.6			
Do you have accredited third parties assess your security controls? If so, who performs them and how frequently?			
Sample response: Our firm has an annual security assessment performed by [accredited third party] that assesses all internal and external controls firmwide. Additionally, our firm meets quarterly with a third-party security consultant to assess any new software, policies, procedures, or other material changes that have been implemented in the Information Technology (IT) environment that may affect security.			
Comments: Most law firms should consider regular third-party security assessments that test both internal and external controls. It is particularly important to assess the security implications of new or modified software and hardware. Firms should also rotate their assessment companies regularly.			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 1.7			
What is the scope of the assessment(s) performed?			
Sample response: See prior response.			
Comments: While it is a best practice for assessments to be firmwide and assess all controls, organizations should determine what constitutes their largest risk and ensure the law firm is addressing those areas.			
Question 1.8:			
Will you provide the organization with the most recent and future versions of the applicable assessments?		Yes	
Sample response: Subject to execution of an appropriate nondisclosure agreement (NDA), the firm will provide this material upon request.			
Comments: Because audit reports contain information that could, if revealed, compromise the security of a firm, firms may ask organizations to execute NDAs before the reports are shared or may elect to provide information about the report verbally rather than in writing.			
Question 1.9:			
Do you perform information security risk management assessments on any companies that will be handling organization data for this representation?			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes.			
Comments:			
Question 1.10:			
Do you have a document retention and destruction policy? If so, please be prepared to provide a copy.		Yes	
Sample response: Yes, we have a document retention/destruction policy. Subject to execution of an appropriate NDA, the firm will provide this material upon request.			
Comments: Because document retention policies contain sensitive information that may compromise the security of the firm, an organization may be asked to execute an NDA before the firm shares this information. Most organizations want to ensure that any document retention policy provides for the secure destruction of organization data at the end of an engagement. In today's environment, a law firm should not hold organization data indefinitely, but firms do have ethical and loss-control requirements that may limit their ability to destroy data as soon as the engagement ends.			
Question 1.11:			
Please provide an organization chart for your Information Technology and Information Security departments or teams that includes the percentage of time each member devotes to information security activities.		Yes	

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: The firm will provide this material.			
Comments: For a larger law firm, you should expect to see a separate CISO who ideally does not report to the CIO. For smaller firms, this area may be outsourced entirely to a third-party service provider.			
Question 1.12:			
Please describe the policies and processes you have in place to ensure that you are complying with all applicable privacy laws and regulations.			
Sample response: We understand our ethical and legal duties to properly protect personal data under various U.S. and international laws and regulations. We provide our attorneys with training and education in this area.			
Comments:			
2. Risk Assessment			
2.1 Cybersecurity Considerations			
Question 2.1.1:			
Will Organization Information be segregated from other firm data at all times during the engagement? If so, describe how.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes. We can maintain security controls on all Organization Information so that only your legal team has access to Organization Information in the course of the engagement.			
Comments: This may not be possible for many law firms, particularly smaller law firms with less sophisticated information management systems. Firms should discuss, among other things, segregation processing, document review hosting, production, storage, and archiving.			
Question 2.1.2:			
Do you have a policy for business continuity? Please be prepared to provide a copy of the policy.		Yes	
Sample response: Yes, our firm has a policy for business continuity. The policy is updated annually.			
Comments: It is not unusual for firms to refuse to provide a copy of the policy for security reasons. If this is the case, consider asking for a redacted copy, a table of contents, or a remote viewing session via WebEx or similar technology. Alternatively, ask for specifics regarding topics, implementation date, review dates, and whether the policy is approved by management.			
Question 2.1.3:			
Do you have a policy for disaster recovery? Please be prepared to provide a copy of the policy.		Yes	

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes, our firm has a policy for disaster recovery. The policy is updated annually.			
Comments: See prior response.			
Question 2.1.4:			
Do you have a secondary site for disaster recovery purposes? If so, how far away is the disaster recovery site from the current servers that will house Organization Information?			
Sample response: Our law firm maintains a disaster recovery site more than 100 miles away from our normal servers.			
Comments: Most law firms should have an offsite disaster recovery site. Although a number of factors go into the appropriate distance from servers (e.g., physical access to the site, whether a third-party service provider is handling data, redundancy options, whether or not the law firm is in an area with a high likelihood of natural disasters, etc.) distances between 25-100 miles are considered sufficient for most businesses.			
Question 2.1.5:			
What is the current Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for your disaster recovery solution? When was the last disaster recovery test performed?			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Our RTOs and RPOs vary based on system and function. As examples, the RTO for our email system is 2 hours and for our financial systems is 8 hours to full resumption of activity. Our last test of disaster recovery was on [xx/xx/xxxx].			
Comments:			
Question 2.1.6:			
Do you remain up to date with system, network, and software security patches?			
Sample response: Yes.			
Comments: All law firms must answer this question in the affirmative.			
Question 2.1.7:			
If the answer to 2.16 is yes, please describe your patching process.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Our firm provides monthly system and security patches, with additional patches being provided on an as-needed basis if a threat develops. All patches are tested before implementation.			
Comments: Firms should discuss, among other things, the types of patches and the frequency of implementation. Because security patches are sometimes incompatible with law firm software, firms may purposely not patch vulnerable systems in order to maintain functionality.			
Question 2.1.8:			
Do you remain up to date with system, network, and software security patches? In the event of notification of a zero-day vulnerability, how long will it take for firms to apply and implement necessary security patches? Describe the process.			
Sample response: Our response will depend on the vulnerability and the systems affected. We promptly investigate and remediate known vulnerabilities.			
Comments: Firms should recognize that there is not a "one-size-fits all" solution. This sets a standard for the organization to measure firms against if a security issue arises.			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 2.1.9:			
Do you perform an annual risk assessment?			
Sample response: Yes.			
Comments:			
2.2 Event Reporting			
Question 2.2.1			
Do you have an Incident Response Plan that covers incidents affecting both physical and electronic files?			
Sample response: Yes, we have an Incident Response Plan that covers incidents affecting both physical and electronic files.			
Comments: If firms do not provide a copy of the policy, organizations should ask for specifics regarding topics, roles and responsibilities, implementation date, review dates, and whether the Incident Response Plan has been approved by management.			
Question 2.2.2:			
Do you have a client notification plan in the event of Security Incidents or Breaches? If so, describe when the plan is put into action or be prepared to provide documentation.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Client notification is an element of our Incident Response Plan. Clients are notified within 48 hours of proper investigation of a Breach if their unencrypted data is affected.			
Comments: While many organizations would like firms to provide evidence of any Breach or Security Incident, this would be onerous for many law firms. Requiring notification when there is a Breach involving unencrypted Organization Information, regardless of whether it contains Personally Identifiable Information (PII)/Protected Health Information (PHI)/Payment Card Industry (PCI) presents a reasonable compromise.			
Question 2.2.3:			
Does your Incident Response Plan include appropriate contacts (including law enforcement)?			
Sample response: Yes.			
Comments:			
Question 2.2.4:			
Please describe your process for notifying organization management of a Security Incident.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: This varies by engagement but typically is done via relationship partner with consultation from our Office of the General Counsel (OGC) and IT security teams.			
Comments:			
Question 2.2.5:			
Have you created remedial plans to address deficiencies in your audits? If so, please be prepared to provide documentation to support.		Yes	
Sample response: Yes, we have created such remedial plans, which include an action log with owners and due dates.			
Comments: Firms may not provide this information, because it is typically regarded as proprietary and confidential.			
Question 2.2.6:			
Do you have the ability to track and manage incident investigations? If so, describe your process.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes, as part of our Incident Response Plan, we track and manage incident investigations and document any findings.			
Comments:			
2.3 Service Provider Due Diligence			
Question 2.3.1			
Do you anticipate using third-party service providers to store Organization Information, including but not limited to cloud storage, or any third-party tools not hosted in your environment to process Organization Information? If so, please describe the service providers and their services or tools and indicate why you are using them.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: We use third-party service providers to store and process Organization Information for document production [vendor x], litigation management [vendor y], and other purposes [vendor z].			
Comments: Subcontractors and service providers can be a weak link. Organizations should ensure that firms know which service providers will be used with the representation and their current cybersecurity posture, and make sure these service providers are being audited on a regular basis.			
Question 2.3.2:			
For any service providers described in 2.3.1, do you maintain an inventory of Organization Information stored (other than temporary storage under 90 days) with these service providers?			
Sample response: Yes, we maintain a list of this information.			
Comments:			
Question 2.3.3:			
Have you performed security assessments on the service providers identified in 2.3.1? If so, please describe any steps you have taken to address identified security vulnerabilities.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes, we perform annual security assessments on the listed service providers. Material security vulnerabilities are identified, and service providers are required to remediate the vulnerabilities within a reasonable period of time.			
Comments: Consider whether the amount and type of data being stored is worth this additional cost.			
Question 2.3.4:			
For any service providers described in 2.3.1, have these service providers experienced a Security Incident within the last two years? If so, please describe.			
Sample response: We know of no such incidents.			
Comments:			
Question 2.3.5:			
Are there other subcontractors and/or suppliers who may have access to Organization Information? If so, please list those subcontractors and suppliers and describe the process for sharing/managing information for each.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: In addition to the third-party service providers listed above, other subcontractors and suppliers like couriers and delivery services may have limited or transient access to Organization Information. The firm assesses information security practices when determining which of these subcontractors and suppliers to contract with, and it takes steps that are reasonable under the circumstances to prevent any inadvertent disclosure of Organization Information to these subcontractors and suppliers.			
Comments:			
Question 2.3.6:			
Does the firm have an ongoing service provider governance/risk management program? If so, please describe it.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes. As noted above and below, we evaluate and select subcontractors and suppliers based in part on their information security practices, and we expect them to return or destroy Organization Information obtained during an engagement, to maintain Organization Information as confidential during the engagement, and to maintain an appropriate Information Security Program. Wherever possible, we enforce these requirements by contract.			
Comments:			
Question 2.3.7:			
In your service provider agreements, do you require your service providers to (1) return or destroy all Organization Information at the end of an engagement; (2) maintain the confidentiality of Organization Information; (3) maintain an appropriate Information Security Program; and (4) have a plan to transition Organization Information in the event the provider or the firm are replaced?			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes.			
Comments: Add additional terms as necessary.			
Question 2.3.8:			
Do you outsource any of your systems, services, or infrastructure to vendors outside of the U.S.? If so, please provide the locations and percentage of the work performed outside of the U.S., as well as a description of how the outsourced systems, services, employees, or infrastructure are vetted.			
Sample response: No, no systems, services, or infrastructure are outsourced outside of the U.S.			
Comments: Storing data or accessing data from foreign locations may require the organization and the firm to analyze their liability for cyber incidents under foreign regulations.			
2.4 Representations and Warranties			
Question 2.4.1			
Do you, and will you continue to, comply with any information security requirements included in your agreement with the organization?			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes.			
Comments:			
2.5 Confidentiality			
Question 2.5.1			
Will Organization Information be appropriately protected from unauthorized access or disclosure? Describe all standards and systems currently in place to provide protected environments.			
Sample response: Yes. The firm has in place an Information Security Program that will protect Organization Information (including any Protected Health Information (PHI), Personally Identifiable Information (PII), Nonpublic Personal Information (NPI), or Payment Card Industry (PCI)) from unauthorized access and disclosure and maintain it in compliance with all applicable laws and regulations.			
Comments: Consider whether Organization Information for the engagement(s) will include PHI, PII, NPI, or PCI information that may require additional protections (encryption, monitoring, role-based restricted access, etc.)			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 2.5.2			
If you have any data that may subject to the European Union (EU) General Data Protection Regulation (GDPR), do you have a protocol for handling this data in compliance with the aforementioned authority? If so, please describe.			
Sample response: We have mapped where data subject to EU regulations is stored for each client, and we comply with all GDPR requirements for storing and processing that data. At a client's request, we will execute an EU data processing agreement.			
Comments: If the firm has access to personal information regulated by the GDPR, the firm must comply with the GDPR. This may include appointing a Data Protection Officer or contracting with a third-party service provider for these services. Firms with international clients or U.S.-based clients that have an international reach (e.g., e-commerce) should apprise themselves of these regulations.			
Question 2.5.3			
If you have any data that may be subject to other non-U.S. data protection regulations, do you have a protocol for handling this data in compliance with the aforementioned authority? If so, please describe.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response:			
Comments: This answer will depend on the data to which the law firm has access.			
2.6 Termination			
Question 2.6.1			
Do you have a transition plan to facilitate the orderly winding up and transfer of data and services back to the Organization or to another law firm? If so, please describe.			
Sample response: Yes. Our departure procedures outline departure steps to be executed for both personnel and Organization Information.			
Comments:			
2.7 Insurance			
Question 2.7.1			
Do you have cyber liability insurance with an insurance company having a minimum credit rating of A– from S&P or an equivalent rating agency? If so, please provide evidence of coverage.		Yes	
Sample response: Yes.			
Comments:			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 2.7.2			
With regard to the coverage referenced in 2.7.1, please describe the coverages and sublimits that you maintain.			
Sample response:			
Comments: Depending on the scope of services, the organization may not need this level of detail from a firm.			
Question 2.7.3			
Will you add the organization as an additional insured to the coverage referenced in 2.7.1?			
Sample response: We cannot.			
Comments: Some policies will not permit this, will not permit it for a reasonable price, or do not have additional insured endorsements with appropriate limits on the firm's exposure.			
Asset Security			
3.1 Inventory of Authorized and Unauthorized Devices			
Question 3.1.1:			
Do you use an automated asset inventory discovery tool to build and maintain an asset inventory of systems connected to your public and private networks (yes or no)?			
Sample response: Yes.			
Comments:			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 3.1.2:			
Does the asset inventory include the following elements: (yes or no)? ● Network address ● Machine name ● Asset purpose ● Asset owner ● Associated department ● Asset location			
Sample response: Yes.			
Comments:			
Question 3.1.3:			
Upon discovery of an unauthorized device, how long does it take your IT staff to remove the device from the network, disable it, or eliminate access to the network (in minutes)?			
Sample response: Unauthorized devices cannot connect to our private network and may access our public Wi-Fi network only if the user can supply the appropriate password.			
Comments:			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 3.1.4:			
When IT equipment is retired, do you sanitize or securely destroy all Organization Information on the equipment? If so, what standards do you use, and do you require written certification of destruction if you use a third-party service provider?			
Sample response: Yes. Equipment is sanitized or destroyed using Department of Defense destruction methods. We require written certification of destruction when we use a third-party service provider.			
Comments:			
3.2 Inventory of Authorized and Unauthorized Software			
Question 3.2.1:			
Do you perform regular scanning and generate alerts when unapproved software is installed on a computer?			
Sample response: Yes.			
Comments:			
Question 3.2.2:			
Do you deploy software inventory tools for all servers and workstations?			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes.			
Comments:			
Question 3.2.3:			
Do you have a change control/review process for software patches and updates? If so, please describe.			
Sample response: Yes. This is covered in our change control procedures, with weekly review meetings for approvals.			
Comments:			
Question 3.2.4:			
If application development is performed in-house (including interfaces, add-ons, modules, plug-ins, etc.), then describe your software development security procedures.			
Sample response:			
Comments: Organizations should also consider whether the firm's in-house application development indirectly involves third parties.			

	Rating[18]	Evidence Required?[19]	Name of Document
3.3 Continuous Vulnerability Assessment and Remediation			
Question 3.3.1:			
Do you perform INTERNAL vulnerability scanning and/or penetration testing annually? If so, please provide the date of your last test.			
Sample response: Yes. [xx/xx/xxxx].			
Comments: Ensure that the date is within last 12 months or that the next test date is in the not too distant future.			
Question 3.3.2:			
Do you perform EXTERNAL vulnerability scanning and/or penetration testing annually? If so, please provide the date of your last test.			
Sample response: Yes. [xx/xx/xxxx].			
Comments: Ensure that the date is within last 12 months or that the next test date is in the not too distant future.			
3.4 Physical Security			
Question 3.4.1:			
Do you have a physical security policy that includes all data centers and office locations? If so, please be prepared to provide.		Yes	
Sample response: Yes.			
Comments: Pay particular attention to visitor policies and video monitoring.			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 3.4.2:			
Do you have policies or programs in place to support the ongoing management of environmental controls (i.e. HVAC, fire detection and suppression, fuel/generator, etc.) for your offices and facilities? If so, please describe.			
Sample response: Yes. [Describe specifics.]			
Comments: Primary focus here would be on data-center environment.			
Question 3.4.3:			
Are there secure facilities and processes at each location for disposing of confidential materials (e.g., shredders, locked bins, etc.)? Please describe.			
Sample response: Yes. [Describe specifics.]			
Comments:			
Question 3.4.4:			
Is access to your facility controlled by the use of an electronic access control system (e.g., badge reader, biometric scanner)?			
Sample response: Yes.			
Comments:			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 3.4.5:			
Do you physically maintain your own data centers? Whether yes or no, please provide details about who maintains them and where they are geographically located.			
Sample response:			
Comments: The exact location may be confidential, so consider if confirmation of high-level details will be acceptable.			
3.5 Malware Defenses			
Question 3.5.1:			
Is there an anti-malware policy or program that includes workstations, servers, and mobile devices?			
Sample response: Yes.			
Comments:			
Question 3.5.2:			
What is the percentage of systems with anti-malware systems deployed, enabled, and up to date?			
Sample response: Approximately 90 percent.			
Comments:			

	Rating[18]	Evidence Required?[19]	Name of Document
3.6 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches			
Question 3.6.1:			
Have you defined secure configurations for each type of network device in writing?			
Sample response: Yes.			
Comments:			
Communications and Network Security			
Question 4.1:			
Do you encrypt Organization Information at rest and in transit? If so, please describe how.			
Sample response: Yes. All workstations and servers are encrypted with 256-bit encryption.			
Comments: This is especially important if PHI/PII/PCI will be involved in the representation.			
Question 4.2:			
Do you have network security mechanisms in place (e.g., firewalls, intrusion-detection/intrusion-prevention systems (IDS/IPS), etc.)? If so, please describe.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes. We have firewalls at our perimeter and at key points within network for segmentation.			
Comments:			
Question 4.3:			
Do you monitor audit logs for your network? If so, please describe your policies and processes, and include in your description how often the logs are reviewed.			
Sample response: Yes. We use a log aggregator with key alarms set for notification to our security team.			
Comments:			
Question 4.4:			
If a system fails to log properly, how long does it take for an alert about the failure to be sent?			
Sample response: Varies per system; key systems report within 60 minutes.			
Comments:			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 4.5:			
Do you have a corporate wireless network or a guest wireless network? If you have a guest network, is it segregated from the corporate network? Is Wi-Fi Protected Access 2 (WPA2) encryption and enterprise authentication implemented for the corporate wireless network?			
Sample response: Yes for all.			
Comments:			
Question 4.6:			
What information security policies and processes are in place that are specific to access from portable devices and mobile devices?			
Sample response: Our mobile devices are covered in our encryption policy (all require encryption).			
Comments:			
Question 4.7:			
Does your email system support Transport Layer Security (TLS) for encryption?			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes.			
Comments:			
Question 4.8:			
Do you use secure configuration standards for network and server infrastructure?			
Sample response: Yes.			
Comments:			
Question 4.9:			
Do you restrict access to websites that can be used to exfiltrate confidential data (e.g. Gmail, Yahoo!)? If so, please describe the restrictions.			
Sample response: Yes. Webmail is blocked.			
Comments:			
Question 4.10:			
Do you utilize intrusion-detection systems (IDS) or intrusion-prevention systems (IPS) on your network? If so, please describe them, and include in your description whether they work within your network or at its perimeter.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes, we utilize IDS on the perimeter of our network.			
Comments: Perimeter detection should be deployed. Best practice is to also have internal detection that looks for abnormalities within the environment, as well as malware.			
Question 4.11:			
Do you utilize a data loss prevention (DLP) solution, and do you have a written policy prohibiting data exfiltration?			
Sample response: Yes.			
Comments:			
Identity and Access Management			
Question 5.1:			
Are protections in place for remote access, including authentication mechanisms, encryption algorithms, and account management process? If so, please be prepared to describe them.		Yes	
Sample response: Yes. All listed procedures are in place.			
Comments:			

	Rating[18]	Evidence Required?[19]	Name of Document
Question 5.2:			
Do you screen all partners, employees, service providers, and contractors, including a criminal background check, prior to hiring? If so, please be prepared to describe your screening policies and procedures.		Yes	
Sample response: Yes, all the listed personnel are screened, and the screening of all but contractors includes a criminal background check. Individual employees of certain contractors may be screened if they have access to sensitive information.			
Comments:			
Question 5.3:			
Are access controls in place that cover adding users, setting their permissions, monitoring their activities, changing their access, and deleting users? If so, please be prepared to describe these controls.		Yes	

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes, all the listed controls are in place.			
Comments: Sound access control requires firms to establish role-based access based on the principle of least privilege, to segregate key duties, to review user access with reasonable frequency, and to promptly adjust user access in the event of role changes or terminations.			
6. Security Operations			
Question 6.1:			
Are new employees required to sign agreements relating to confidentiality and information security upon hire?			
Sample response: Yes.			
Comments: Law firms should have agreements that address both confidentiality and information security.			
Question 6.2:			
Is there a security awareness training program? If so, please describe it, and include in your description which employees must participate and how often.			

	Rating[18]	Evidence Required?[19]	Name of Document
Sample response: Yes, we train all new employees with access to sensitive data at the time they are hired, and we also have an annual mandatory security training and updates that are circulated by email.			
Comments: Ideally, law firms should have regular modules and training (e.g., quarterly or monthly). Training upon hire and annual training should be the minimum.			
Question 6.3:			
Does your security awareness training program include specialized content for employees with access to sensitive data (e.g., Accounting, Human Resources (HR)) or privileged accounts (e.g., IT)?			
Sample response: Yes, additional training is given to employees with access to sensitive data and those with privileged accounts.			
Comments:			

THE SEDONA CANADA COMMENTARY ON PRIVACY AND INFORMATION SECURITY FOR LEGAL SERVICE PROVIDERS: PRINCIPLES AND GUIDELINES

A Project of The Sedona Conference Working Group 7 (Sedona Canada)

Author:

The Sedona Conference

Drafting Team:

Molly Reynolds
William Ellwood
David Outerbridge
Sarah Millar

Editor-in-Chief:

David Outerbridge

Staff Editor:

David Lumia

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 7. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just

click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

The Sedona Conference, Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines, 21 SEDONA CONF. J. 577 (2020).

PREFACE

Welcome to the final, August 2020, version of *The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines*, a project of the Sedona Canada Working Group (WG7) of The Sedona Conference. This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

This *Commentary* was first published for public comment in October 2019. Where appropriate, the comments received during the public-comment period have been incorporated into this final version of the publication.

The *Commentary* builds on similar principles and guidelines regarding privacy and information security for legal service providers produced by the Sedona Conference Working Group 1 for the United States. However, these Principles and Guidelines focus on the regulatory and practice requirements of the Canadian legal profession.

The Sedona Conference acknowledges the efforts of Editor-in-Chief David Outerbridge, who was invaluable in driving this project forward. We thank drafting team members Molly Reynolds, William Ellwood, and Sarah Millar for their dedication and commitment to this project. We also thank prior members Martin Felsky and Duncan Fraser for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG7 and several other Working Groups in the areas of electronic document retention and production; international electronic information management, discovery, and disclosure; patent damages and patent litigation

best practices; data security and privacy liability; trade secrets; and other "tipping point" issues in the law. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
August 2020

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Principles and Guidelines set out in this *Commentary* are designed specifically for lawyers, law firms, and other legal service providers ("LSPs"). They address the privacy and information security protections that LSPs should implement in order to protect themselves and their clients, and comply with legal and ethical obligations.

Advances in technology present new risks to privacy and the security of information that LSPs hold. Personal and confidential information ("PCI") is increasingly vulnerable to unauthorized access, loss and theft. Yet the ethical responsibility and legal obligation of LSPs to protect such information has not changed. Nor does an LSP's duty depend on the size or resources of the professional who holds such information.

While the duty is constant, the means of fulfilling it will vary. Effective privacy and information security does not allow for, or require, a one-size-fits-all solution. The nature of the information, the needs of the client, the circumstances in which the information is held, and other factors affect the methods that an LSP should adopt to protect PCI entrusted to its care.

Perfect security practices are not achievable. What is required are well thought-out policies and practices—rigorously and systematically implemented and updated over time—that are both reasonable and appropriate to the circumstances.

This *Commentary* is intended to help all LSPs—sole practitioners, law firms of all sizes, paralegals, law clerks, and legal support entities—determine which policies and practices are best suited for them. They aim to give practical guidance to LSPs by exploring "real-life" scenarios involving the loss of PCI, or the breach of security measures designed to protect it, commonly experienced in practice. Examples will be explored throughout this *Commentary* to illustrate the Principles and Guidelines in action.

The *Commentary* is divided into four sections.

Guiding Principles: Section I sets out six governing principles that should guide all Canadian LSPs when designing and maintaining PCI security programs.

Obligations: Section II examines the ethical and legal obligations requiring LSPs to protect PCI.

Security Risk Assessment: Section III describes the recommended elements of a security risk assessment that LSPs should perform in respect of their practice.

Best Practices: Section IV describes, in step-by-step format, recommended best practices for the development of appropriate policies and practices to protect PCI. The table of contents for Section IV serves as a high-level checklist of these best practices.

I. GUIDING PRINCIPLES

A. Introduction

Legal service providers (LSPs) as well as the third-party service providers (TPSPs) assisting them[1] in their legal practice rely on various forms of technology to communicate, create, share, and store information in the course of business. Technology poses risks to privacy and information security, including the confidentiality of privileged communications. This *Commentary* sets out a framework for mitigating these risks.

The focus of the Commentary is on personal and confidential information ("PCI"). Personal information is any information about an identifiable individual, such as contact information, medical or financial information, or biometric identifiers such as an individual's voice recording. Confidential information may relate to individuals or legal entities and includes any information subject to a lawyer's duty of confidentiality or a class of privilege.

Ethical rules, statutes, regulations, and the common law all impose duties on lawyers, paralegals, and less directly, on much of the legal services industry, to safeguard PCI belonging to clients and third parties. Engagement agreements may also contain requirements about the safekeeping and handling of PCI. This *Commentary* suggests some prospective and remedial measures that LSPs should consider in order to meet or exceed these obligations.

---

1. As used herein, the term "Legal Service Provider" (LSP or "provider") includes lawyers, law firms, and any other person or entity directly engaged in providing legal advice and counsel, and the term "Third-Party Service Provider" (TPSP) includes the other professionals and organizations who play an integral part in the provision of legal services, such as auditors, outside experts, consultants, and eDiscovery service providers.

The discussion in this *Commentary* is informed by the following guiding principles:

Principle 1: **Know the law**: LSPs should know the relevant law in order to identify, protect, and secure PCI they control in their practices.

Principle 2: **Understand the PCI you control**: LSPs should understand what PCI is, and know the types of PCI in their control.

Principle 3: **Assess risk**: LSPs should periodically conduct a risk assessment of the PCI within their control. The risk assessment should consider the PCI's sensitivity and vulnerability, and the harm that would result from its loss or disclosure.

Principle 4: **Develop policies and practices**: After completing a risk assessment, LSPs should develop and implement appropriate policies and practices to mitigate the risks identified in the risk assessment.

Principle 5: **Monitor regularly**: LSPs should monitor their operations on a regular basis for compliance with privacy and security policies and practices.

Principle 6: **Reassess**: LSPs should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

B. Principles Explored

Principle 1: Know the law

LSPs must take reasonable steps to protect and secure PCI by understanding applicable requirements for such information.

These requirements arise from many sources, including ethical rules, federal and provincial privacy laws, common law, foreign laws, court rules, and contractual requirements. On a general level, LSPs need to understand the following about the Canadian legal landscape:

- the professional obligations applicable to all members of the LSP, including privacy and confidentiality guidance established by applicable law societies;
- the federal and provincial privacy laws applicable to the LSP, such as the Personal Information Protection and Electronic Documents Act and similar statutes in British Columbia, Alberta, and Quebec;
- the circumstances under which foreign privacy laws may apply to information the LSP is handling, such as when acting on cross-border matters or representing a client based in another country; and
- the terms of any agreements the LSP has signed that govern their rights to use information (e.g., corporate client external counsel guidelines, terms of use for land titles, or drivers' license registries) or give other parties rights to information under the LSP's control (e.g., cloud storage or document review software services).

Principle 2: Understand the PCI you control

LSPs should understand what constitutes PCI.

The following are types of personal information often collected by LSPs**:**

- "know your client" information, such as identity cards, contact details, and billing information
- medical or financial assessments obtained in the course of litigation or estate planning
- due diligence information gathered under a non-disclosure agreement in a corporate or real estate transaction
- employee information, such as Curriculum Vitae (CV), payroll information, and performance reviews
- financial or social security information belonging to customers of the LSP's client

Confidential information controlled by LSPs can include:

- all information provided to the LSP by clients or potential clients;
- information obtained from third parties during the course of providing legal services to a client, such as corporate information about an acquisition target or records relating to an opposing party in litigation; and
- information subject to a confidentiality agreement or undertaking.

LSPs should also understand how this PCI comes into their control, where they store it, who has access to it, and how sensitive it is. LSPs should keep in mind that as technology evolves, the types and methods for collection and storage of PCI may also need to change.

Principle 3: Assess risk

LSPs need to perform a risk assessment tailored to meet the specific needs of their legal environment, including information practices, storage locations, employees, work practices, Information Technology (IT) infrastructure, and client security policies, to name a few. The LSP can conduct the risk assessment on its own or, if unfamiliar with the area of privacy and information security, use a professional or consultant knowledgeable in the area.

Regardless of who conducts the risk assessment, the following steps are key to the process:

- Identify and evaluate the sensitivity of the various types of information within the LSP's control, and the potential harm that would result from unauthorized disclosure, breach, loss, or theft of that information.
- Identify specific threats and vulnerabilities that could result in unauthorized disclosure, breach, loss, theft, alteration, or unavailability.
- Assess the risk of harm posed by each threat or vulnerability.

Principle 4: Develop policies and practices

Each LSP should develop and implement a scaled and prioritized set of policies and practices to respond to any risk to PCI identified in the risk assessment. These policies and practices should:

- factor in and respond to the sensitivity of different types of information;
- respond to the threats and vulnerabilities identified in the risk assessment and minimize the risks that would result in unauthorized disclosures, breaches, loss, or theft;

- respond to client-created data privacy and security requirements while enabling the LSP to meet its day-to-day business needs;
- address privacy and security outside the office environment, in transit, or where data is accessed remotely;
- focus on individual training;
- respond to actual data loss and breaches; and
- mandate how and when information is shared with third parties, such as outside experts, consultants, other TPSPs, co-counsel, adversaries, and courts.

The goal is to keep PCI free from corruption or loss, and accessible only to those who need to use it.

In this regard, larger LSPs should consider hiring one or more full-time employees with expertise in these areas to develop and implement the LSP's policies and practices. As with the conduct of a risk assessment, it is acceptable for smaller LSPs to hire a consultant to address both information security and privacy and assist in creating the LSP's policies and practices in this area. In the end, it is important to have a senior-level person within the LSP's practice who has the authority to implement and enforce the policies and practices developed, and who is held accountable for their success.

Practically speaking, good policies and practices respecting PCI will: (1) limit access to confidential information to those with a bona fide role-based need for access; (2) provide for physical security; (3) implement information access controls (e.g., multiple-factor authentication and attribute-based access control); (4) consider intrusion detection and prevention technologies; (5) employ appropriate use of encryption technologies; (6) provide for secure backup/disaster recovery; and (7) ensure the

prompt disposition of information that is no longer needed (and hence at risk of theft or loss with no offsetting potential benefit).

Any policies or practices should include a clear incident response plan to address the unauthorized disclosure, breach, loss, or theft of PCI. The incident response program should include procedures for: (1) reporting each incident to a designated person responsible for implementing the LSP's response plan; (2) identifying the source of the breach; (3) undertaking steps to stop the breach; (4) investigating the extent of any loss or compromise of private or confidential information; (5) providing appropriate notice to the client, relevant law enforcement authorities, and insurers, as necessary; and (6) abiding by applicable data breach notification requirements.

Human beings are the weakest link in any information, privacy, or security program. A well-designed program to protect PCI will contain robust provisions for training in protecting information, and ongoing monitoring. The best and most effective training sessions are interactive and involve testing to confirm that the recipient understands the material. Accordingly, LSPs should seek to conduct or sponsor formal training at regular intervals (ideally annually) for all personnel.

Principle 5: Monitor regularly

It is important to be vigilant on a continuous basis. Security breaches can come from many sources, internal and external. Breaches may occur at any time, and the damage they cause may spread at incredible speed. Accordingly, to minimize the likelihood of any breach and to mitigate its consequences, LSPs need to engage in real-time monitoring of risk and compliance with policies and practices.

Monitoring should be tailored to the organization. Each LSP should establish a mechanism for assessing the various components of its information security environment, policies, plans,

and practices, including those relating to physical security, information-access controls, intrusion prevention and detection systems, encryption technologies, and the maintenance, transfer, and disposition of information. For some providers, such monitoring may be relatively simple and straightforward. Others may need to employ, depending on their industry or situation-specific requirements, standard auditing frameworks, such as SSAE 16 (formerly SAS), the ISO 27000 series standards, or another framework capable of being measured, assessed, and improved with demonstrable and documented criteria and according to a fixed schedule. Of course, as technology changes, so will these lists. Periodic auditing for any organization is important and strongly recommended.

Principle 6: Reassess

Once a risk assessment is completed and policies and practices developed, LSPs cannot place the protection of PCI on the back burner.

It is important for LSPs to update their risk assessments on a regular basis and alter policies or practices in response. Threats to security and privacy change constantly. The compliance landscape challenges organizations at every level, arising from industry-specific, provincial/territorial, and federal requirements, and obligations that affect the creation, management, transfer, or disposition of information in non-Canadian jurisdictions. These factors, coupled with constantly evolving technologies, require ongoing vigilance to ensure that the LSP's privacy and security policies and practices remain responsive to changing circumstances.

To be "reasonable and appropriate," security policies and practices should be current; and the best way to keep them current is to stay abreast of developments in the law, technology, and industry best practices. This creates a need to perform two tasks in tandem: (1) conduct *ad hoc* reassessments based on

active monitoring of the LSP's actual real-time or near real-time practices; and (2) undertake regularly scheduled (ideally annual) reviews of developments that may concern the LSP's current internal practices or supported programs.

II. SOURCES OF THE DUTY TO PROTECT PRIVATE AND CONFIDENTIAL INFORMATION[2]

The duty to protect privacy and confidentiality applies to all participants in the legal services industry. The duty is multifaceted and derives from a number of sources. The principal sources of the duty are: (1) the ethical rules applicable to lawyers and paralegals; (2) federal, provincial, and municipal statutes and bylaws regulating the collection, use, and disclosure of personal information; (3) foreign laws, where applicable; (4) statutory and common-law-based causes of action; and (5) agreements with and instructions by clients.

A. Ethical Rules Applicable to LSPs

The Federation of Law Societies of Canada ("Federation") has developed a Model Code of Professional Conduct ("Model Code") to synchronize professional conduct standards for the legal profession across Canada. The Model Code has been adopted by 12 of the 13 provincial and territorial law societies (in Québec, the Model Code is under review, although the *Code of Ethics of Advocates* is largely harmonized with the Model Code[3]).

This section provides an overview of obligations related to competency and confidentiality under the Model Code that may intersect with privacy considerations. It also provides an overview of applicable guidelines issued by various law societies and the Canadian Bar Association (CBA).

---

2. Unless otherwise expressly stated in this *Commentary*, the term "information" includes both electronically stored information (ESI) as well as information in paper or hard-copy form.

3. Federation of Law Societies of Canada, "Implementation of the Model Code," online: <http://flsc.ca/resources/implementation-of-the-model-code/>.

Although professional standards set out by the Federation and provincial law societies apply directly to lawyers and in some cases paralegals, they also apply indirectly to nonlawyer LSPs working under the supervision of, or employed by, lawyers. Supervising lawyers are responsible for ensuring that their employees and any third parties hired to assist with a specific matter adhere to the rules.

1. Technical Competency Under the Model Code

The duty of competence is set out under rules 3.1-1 and 3.1-2 of the Model Code. A competent lawyer must apply "relevant knowledge, skills and attributes in a manner appropriate to each matter undertaken on behalf of a client."[4]

For most LSPs, legal practice is highly integrated with technology. Although the implications of the proliferation of technology are not explicitly addressed by the Model Code, implicitly, the duty of competence requires lawyers to consider what technology may assist them to practice competently, and how to use it. For example, the use of technology may help lawyers meet their obligation to implement necessary skills competently, perform functions in a timely and cost-effective manner, manage their practices effectively, and adapt to changing professional requirements, standards, techniques, and practices. Additionally, the commentary to rule 3.1-2 stipulates that lawyers must recognize tasks that they may lack the competence to handle and take steps to ensure that the client's needs are appropriately addressed.[5]

The implied requirement to use technology may, however, be a double-edged sword, because LSPs' use of technology

4. Federation of Law Societies of Canada, *Model Code of Professional Conduct*, r 3.1-1 online: <http://flsc.ca/interactivecode/> [Model Code].

5. *Ibid,* r 3.1-2, commentaries 5, 6.

presents unique ethical challenges when it comes to preserving the confidential or personal information of clients and others. Computers may be accessed by unauthorized users, cellphones holding sensitive data may be lost, and even an email sent to the wrong recipient may involve inadvertent disclosure of PCI.

The Federation has recognized that technological competence—and the risks that may accompany the proliferation of technology in the provision of legal services—are burgeoning issues for legal regulators and lawyers. The Federation has suggested that lawyers should assess and mitigate risks flowing from the use of a particular type of technology.[6] Additionally, clients should be informed of any risks associated with the use of technology throughout the duration of the lawyer-client relationship.

2. Client Confidentiality Under the Model Code

Section 3.3 of the Model Code addresses a lawyer's handling of confidential information. Rule 3.3-1 imposes a general duty on lawyers to: "at all times . . . hold in strict confidence all information concerning the business and affairs of the client acquired in the course of the professional relationship and . . . not divulge any such information."[7]

The duty of confidentiality under the Model Code is broad. It covers all information obtained by a lawyer during the course of the retainer, whether directly from the client or from some other source. The source of the confidential information and the intended use attaching to the information are not relevant for determining whether information is confidential.[8] It is also implied that a lawyer may, unless the client directs otherwise,

6. *Ibid*., Preface.

7. *Ibid*, r 3.3-1.

8. *Ibid*, r 3.3-1, commentary 2.

disclose client information to partners and associates in the law firm and, to the extent necessary, to other LSPs, TPSPs, and administrative staff whose services are used by the lawyer.[9]

Lawyers who practice in association with other lawyers in cost- or space-sharing arrangements are particularly susceptible to confidentiality breaches and should institute systems and procedures to insulate their respective practices from the risk of inadvertent disclosure.[10]

The duty of confidentiality is owed to every current and former client, regardless of whether the lawyer-client relationship is ongoing.[11] The duty extends to prospective clients seeking advice, even if the lawyer is not ultimately retained.[12] For example, a lawyer generally cannot reveal that he or she has been retained by a client or consulted about a particular matter by a prospective client, unless information about the retainer is in the public domain or there is client authorization to disclose it.[13]

Safeguarding confidential client information presents one of the most challenging ethical responsibilities in the context of technology, particularly because of the wide scope and duration of lawyers' obligations under the Model Code. It is therefore imperative that lawyers specifically consider how to approach the duty in light of the types of technology implemented in their practices. Lawyers should take measures to safeguard client information in all modes of technology employed, including computers, mobile devices, networks, technology outsourcing, and cloud computing.

---

9. *Ibid*.
10. *Ibid*, r 3.3-1, commentary 7.
11. *Ibid*, r 3.3-1, commentary 3.
12. *Ibid*, r 3.3-1, commentary 4.
13. *Ibid*, r 3.3-1, commentary 5.

Rules 6.1-1 and 6.2-2 of the Model Code incorporate lawyers' duties to supervise the work of nonlawyers and law students under their supervision.[14] Lawyers are ultimately responsible if their employee discloses confidential information without authorization.[15] Lawyers should therefore properly vet and train the professionals, administrative staff, and service providers they hire and should have reasonable checks in place to ensure confidentiality is maintained.

3. Law Society Practice Guidelines

Several law societies across Canada have issued nonbinding guidelines intended to help lawyers navigate their professional obligations relating to the use of technology in practice. The Law Societies of British Columbia (LSBC), Alberta (LSA),[16] Manitoba (LSM),[17] Saskatchewan (LSS),[18] Ontario (LSO), New Brunswick

14. *Ibid*, rr 6.1-1–6.1-2.

15. *Ibid*.

16. Law Society of Alberta, *File Retention and Document Management*, online: <https://dvbat5idxh7ib.cloudfront.net/wp-content/uploads/2017/06/14230254/TAB2_3_File-Retention-and-Document-Management2.pdf> [Alberta File Retention and Document Management Guide]; Law Society of Alberta, *To File or Not to File*, online: <https://www.lawsociety.ab.ca/resource-centre/key-resources/practice-management/to-file-or-not-to-file/>.

17. Law Society of Manitoba, *Practice Direction 91-01: Destruction of Closed Client Files* (2004), online: <https://lawsociety.mb.ca/regulation/act-rules-code/practice-directions/91-01-destruction-of-closed-client-files/?hilite=%27Destruction%27%2C%27Closed%27%2C%27Client%27%2C%27Files%27>.

18. Law Society of Saskatchewan, *Retention, Storage and Disposition of Client Files*, online: <https://www.lawsociety.sk.ca/media/9995/fileretentionnov08.pdf>.

(LSNB),[19] Newfoundland and Labrador (LSNL),[20] and Northwest Territories (LSNWT),[21] the Nova Scotia Barristers' Society (NSBS),[22] and the Barreau du Québec ("Barreau")[23] all have guidelines for protecting client confidentiality when opening and maintaining client files,[24] as well as practices to follow when retaining and destroying closed files.[25]

Three guidance documents from the LSO are representative of the types of province- and territory-specific practice resources available:

---

19. The Law Society of New Brunswick has endorsed the Law Society of British Columbia's publication *Opening and Maintaining Client Files* (2006), online: <https://learnlsbc.ca/sites/default/files/LSBC_SF_FileManagement_ClientFiles.pdf>.

20. Law Society of Newfoundland and Labrador, *Practice Advisory—Concerning File Closure, Retention and Destruction* (2003), online: <http://www.lawsociety.nf.ca/wp-content/uploads/2012/11/Practice-Advisory.pdf>.

21. Law Society of the Northwest Territories, *Practice Advisory: Destruction of Closed Client Files*, online: <http://lawsociety.nt.ca/sites/default/files/documents/LSNT_PracticeAdvisory_DestructionofFiles.pdf>.

22. Nova Scotia Barristers' Society & the Law Office Management Standards Committee, *Law Office Management Standards*, online: <http://www.lians.ca/standards/law-office-management-standards>.

23. Barreau du Québec, *Retention, Destruction and Digitization of Records*, online: <https://www.barreau.qc.ca/en/ressources-avocats/services-avocats-outils-pratique/conservation-destruction-numerisation-dossiers/>.

24. Law Society of British Columbia, *Opening and Maintaining Client Files* (2006), online: <https://learnlsbc.ca/sites/default/files/LSBC_SF_FileManagement_ClientFiles.pdf>.

25. Law Society of British Columbia, *Closed Files—Retention and Disposition* (2017), online: <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/ClosedFiles.pdf> [British Columbia File Retention and Disposition Guide].

The *File Management Guideline*[26] sets out the essential features of technological and paper systems to: store information regarding clients and opposing parties; open and maintain active client files; close, retain, and dispose of closed files; and identify clients' property and place it in safekeeping. It also urges LSPs to train employees to understand the inherent risks of leaving storage media containing electronic client information unattended or unsecured.

The *Guide to File Retention and Destruction*[27] describes appropriate file handling after a client matter is closed, including regulatory requirements relating to privacy and confidentiality. Specifically, the Guide recommends that any documents retained for use as precedents should be stripped of personal client information. Long-term storage of documents with identifying information, whether it be on-site or off-site, physical or electronic, should be done in a manner that maintains confidentiality and protects the files from loss or damage (such as through use of encryption software).

The *Technology Guideline*[28] addresses confidentiality when using electronic means of communication. The LSNB,[29] the

26. Law Society of Ontario, *File Management Guideline*, online: <https://lso.ca/lawyers/practice-supports-and-resources/practice-management-guidelines/file-management>.

27. Law Society of Ontario, *File Retention and Destruction*, online: <https://lso.ca/lawyers/practice-supports-and-resources/topics/managing-files/file-retention-and-destruction>.

28. Law Society of Ontario, *Technology Guideline*, online: <https://lso.ca/lawyers/practice-supports-and-resources/practice-management-guidelines/technology>.

29. Law Society of New Brunswick, *Code of Professional Conduct, Appendix B—Guidelines on Ethics and the New Technology*, online: <https://lawsociety-barreau.nb.ca/uploads/forms/Code_of_Professional_Conduct.pdf>.

LSNWT,[30] the Barreau,[31] and the LSA[32] have similar guidance on how lawyers can protect confidential information when using electronic media. Lawyers can minimize the risk of loss or interception of confidential electronic communications by:

- discussing inherent security risks of particular technology (e.g., portable storage media carrying unencrypted data) with the client;
- using security software to protect information in transit and when stored;
- taking appropriate measures to secure confidential information when using cloud-based services; and
- developing office management practices that protect against inadvertent discovery or disclosure of electronic communications.

In addition, some law societies have resources regarding the use of TPSPs to electronically store or process client information. The LSBC has emphasized the need for the lawyer to ensure that the service provider's policies are in line with the lawyer's professional obligations.[33] This is especially the case where client

30. Law Society of the Northwest Territories, *Practice Advisory: Guidelines on Ethics and the New Technology*, online: <https://lawsociety.nt.ca/sites/default/files/documents/Practice%20Advisory%20-%20Internet%20and%20Technology.pdf>.

31. Barreau du Québec, *Guide on the Management of Technological Documents* (2005), online: <https://www.fondationdubarreau.qc.ca/wp-content/uploads/2016/10/Guidetech_allege_EN.pdf>.

32. Law Society of Alberta, *Computer/Network Security Checklist* (2014), online: <https://dvbat5idxh7ib.cloudfront.net/wp-content/uploads/2017/06/21224619/TAB2_4_Computer-Network-Security-Checklist.pdf>.

33. Law Society of British Columbia, *Cloud computing due diligence guidelines*, online: <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/guidelines-cloud.pdf>. See also Law Society of British

information will be stored electronically in another jurisdiction.[34] In such instances, the client should be fully informed.[35] The LSBC has adopted restrictions around lawyers' engagement of data storage services, in the form of amendments to the LSBC Rules.[36] Similar concerns may extend to servers physically located in Canada but subject to foreign ownership interests.

4. The Canadian Bar Association's *Legal Ethics in a Digital World*

The Canadian Bar Association has issued a guideline intended to help lawyers navigate their professional responsibilities in highly computerized practice settings.[37]

The CBA Guideline begins by suggesting that lawyers protect confidential client information through safeguards that ensure the integrity of the information, so that it is not exposed to

---

Columbia, *Cloud Computing Checklist v. 2.0* (2017), online: <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/checklist-cloud.pdf>. See also Law Society of Newfoundland and Labrador, *Loss Prevention Tip #15: Protecting Yourself from Cybercrime Dangers: Be Careful About Putting Your Firm Data in the Cloud*, online: <http://lsnl.ca/loss-prevention-tip-15/>.

34. Alberta File Retention and Document Management Guide, *supra* note 16, at 9.

35. British Columbia File Retention and Disposition Guide, *supra* note 25, at 19.

36. Law Society of British Columbia, *Law Society Rules 2015*, rr 10-3–10-4, online: <https://www.lawsociety.bc.ca/support-and-resources-for-lawyers/act-rules-and-code/law-society-rules/>.

37. Canadian Bar Association, *Legal Ethics in a Digital World*, online: <http://www.cba.org/getattachment/Sections/Ethics-and-Professional-Responsibility-Committee/Resources/Resources/2015/Legal-Ethics-in-a-Digital-World/guidelines-eng.pdf> [CBA Guideline].

accidental or malicious modification or alteration.[38] Backing up files is a necessary component of security policies.[39]

The CBA Guideline identifies three categories of security measures, drawn from federal privacy legislation: physical safeguards (like locked filing cabinets and restricted office access); organizational procedures (like security policies and training initiatives); and technological measures (including the use of passwords, encryption software, and firewalls).[40]

Special attention is paid to security measures that should be adopted when sensitive information is transported outside of the office, to prevent third-party access.[41] Encryption mechanisms should be used to secure the information during transport, and accessing the information via a secure Virtual Private Network (VPN) connection should be considered in lieu of carrying electronic files on a hard drive or USB key.[42] Use of unsecured wireless networks should be avoided.[43] Particular care must be given when traveling internationally, as electronic devices may be subject to search or seizure by border officials. The CBA Guideline recommends that steps be taken to minimize metadata (background information about electronic documents) or to remove it from files circulated electronically, due to the sensitive information metadata may convey.[44]

Cloud computing tied to servers located in foreign jurisdictions presents a particular concern to client confidentiality, as

38. *Ibid* at 4–5.
39. *Ibid* at 6.
40. *Ibid* at 1–2, 7–8.
41. *Ibid* at 8.
42. *Ibid* at 7–8.
43. *Ibid* at 7.
44. *Ibid* at 9–10.

some foreign governments have enacted legislation that allows them to access such information.[45]

B. Federal Statutory Obligations

The privacy law regime in Canada under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to every organization in the country that collects, uses, or discloses personal information in the course of commercial activities.[46] As organizations engaged in commercial activities, lawyers in private practice and other LSPs must comply with PIPEDA when dealing with personal information.

PIPEDA presumptively applies to all federally or provincially regulated entities, unless the organization is otherwise subject to provincial privacy legislation that has been declared to be "substantially similar" to PIPEDA.[47] The three provinces that have enacted "substantially similar" legislation are Alberta, British Columbia, and Québec. In such cases, the substantially similar provincial law applies instead of PIPEDA, although PIPEDA continues to apply to interprovincial or international transfers of personal information.[48]

---

45. *Ibid* at 10.

46. Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 4(1) [PIPEDA].

47. *Ibid* at s 26(2).

48. Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador have enacted privacy legislation as well, but only with respect to personal health information collected, used, or disclosed by health information custodians. LSPs should be aware of these provincial laws, particularly when representing clients who are custodians, as the provisions regarding agency may apply. LSPs should also be aware that some of the statutes contain specific provisions addressing exceptions that are applicable to lawyers and legal proceedings.

The term "personal information" under PIPEDA is broadly defined as "information about an identifiable individual." Information will be "about" an individual when it relates to or concerns the individual.[49] Individuals will be "identifiable" where there is a serious possibility that they could be identified through the use of that information, alone or in combination with other available information.[50]

PIPEDA stipulates that LSPs may collect, use, and disclose an individual's personal information only with the knowledge and express or implied consent of that individual, unless a legislative exemption applies. The level of consent required depends on the sensitivity of the information and the reasonable expectations of the individual. As an overarching principle, an organization may only collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

PIPEDA mandates protection for all personal information held by an organization. Unlike the duty of confidentiality, it applies to information regarding any individual. This means that PIPEDA may apply not only to information that LSPs collect, use, or disclose in relation to clients, but also to information about others, including adverse parties, third parties, lay witnesses, and expert witnesses. Lawyers should keep in mind that while their duties under PIPEDA overlap significantly with their professional duties, PIPEDA's application is broader and extends to nonclients.

The Office of the Privacy Commissioner of Canada (OPC) oversees compliance with PIPEDA. The OPC has created a

49. Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157 at paras 43, 59, 61, [2007] 1 FCR 203.

50. *Gordon v Canada (Health)*, 2008 FC 258 at para 33.

Privacy Handbook for lawyers, entitled *PIPEDA and Your Practice*.[51] The Handbook addresses how sole practitioners and law firms should approach their obligations under PIPEDA. The Canadian Bar Association has published ten guidelines to help law firms ensure that they are compliant with PIPEDA.[52] The comments that follow incorporate guidance from the OPC, CBA, and relevant case law.

1. Establishing Privacy Policies

For most legal practices, the starting point for compliance with PIPEDA will be an assessment of the law's administrative requirements, which include the appointment of an individual who will be accountable on behalf of the LSP for its obligations under PIPEDA (usually referred to as a "Chief Privacy Officer"). Sole practitioners will be required to assume this responsibility themselves.[53]

LSPs must understand how personal information is collected, used, and disclosed in the course of running the practice, and for what purposes. Privacy policies must address the various ways that personal information is handled, including obtaining consents as needed and developing procedures to handle complaints and requests for access to personal information under PIPEDA.[54] The Lawyers' Professional Indemnity Company ("LawPRO"), the professional liability insurer of Ontario lawyers, has developed a Sample Firm Privacy Policy that may

51. Office of the Privacy Commissioner of Canada, *PIPEDA and Your Practice: A Privacy Handbook for Lawyers*, online: <https://www.priv.gc.ca/media/2012/gd_phl_201106_e.pdf> [Handbook].

52. Canadian Bar Association, *Law Firm Privacy Compliance in 10 Steps* (2015), online: <http://www.cba.org/Publications-Resources/CBA-Practice-Link/Young-Lawyers/2014/Law-Firm-Privacy-Compliance-in-10-Steps>.

53. *Ibid*.

54. *Ibid*.

be used by LSPs as a precedent for developing procedures for dealing with personal information.[55]

Similarly, LSPs will need to establish (and train employees to apply) policies and practices that give effect to the requirements of PIPEDA. Privacy policies should be made publicly available by, for example, posting on a website.

The OPC has recommended that LSPs pay particular attention to the following objectives:[56]

- ensuring that third parties who conduct work on the LSP's behalf have in place a comparable level of protection while the information is being processed by the third party
- setting retention and destruction schedules for personal information the LSP holds
- establishing procedures to handle requests for access to personal information received by the LSP

2. Collection of Personal Information from Clients and Prospective Clients

LSPs often have to collect personal information from potential or existing clients throughout the retainer. For example, prior to commencing the client-solicitor relationship, a lawyer will likely have to conduct conflict checks and complete client identification in accordance with law society rules. Client consent for collection and use of this information, in the context of the specific purpose for which it is to be used, will have to be obtained. Consent may, however, be implied through a client's

55. Lawyers' Professional Indemnity Company, Sample Firm Privacy Policy, online: <https://www.practicepro.ca/wp-content/uploads/2003/07/2003-06-sample.pdf>.

56. *PIPEDA Case Summary No 377, Re*, (April 5, 2007) 2007 CarswellNat 5684.

act of providing the requested information to the LSP in order to secure the retainer.[57]

LSPs that seek to collect personal information about a client or prospective client from a third-party source, such as via a credit check, should obtain the express consent of the individual.[58] LSPs should, within the requirements of their professional obligations and conflict checking systems, minimize the amount of personal information they keep if the LSP is not retained by the client.

3. Collection of Personal Information from Nonclients

LSPs are often engaged in the collection, use, and disclosure of the personal information of nonclients, particularly in the litigation context. The Ontario Superior Court has commented that PIPEDA does not apply to individual litigants who collect information about an opposing party through a private investigator, because information collected in this context is for a personal purpose.[59] Similarly, the Federal Court of Canada has held that a party may collect, use, and disclose personal information about another party during the course of a civil action.[60] This qualifies as a noncommercial activity, and therefore remains exempt from PIPEDA. This is so even if third parties, such as LSPs or investigators, are retained to assist in the litigation.

Despite the above cases, the OPC is of the opinion that there may be instances where the collection, use, or disclosure of personal information in connection with litigation may engage

57. Handbook, *supra* note 51, at 6.

58. *PIPEDA Case Summary No 340, Re*, (May 2, 2006) 2006 CarswellNat 5567.

59. *Ferenczy v MCI Medical Clinics*, 70 OR (3d) 277, 2004 CanLII 12555 (ON SC).

60. State Farm Mutual Automobile Insurance v Privacy Commissioner of Canada, 2010 FC 736 at paras 98–100, 106–07.

PIPEDA. For example, litigation involving commercial organizations may be considered as part of their commercial activities and may be distinguished from claims involving individual litigants in their personal capacity. In a 2011 proceeding involving a commercial organization,[61] the OPC found that the organization's civil defence against a customer's claim regarding an incident that occurred on the organization's premises was sufficiently related to its regular course of business to constitute a commercial activity under PIPEDA. A decision of the Nova Scotia Supreme Court goes against this conclusion in the context of a dispute involving a large insurance company. The court in that case held that PIPEDA did not apply to information pertaining to litigation, because the relationship between the company and the other party arose in the litigation itself and was therefore not of a commercial nature. The court commented that "PIPEDA was not intended to apply to litigants in a legal proceeding."[62]

Given the unclear guidance provided by the case law, LSPs should consider their obligations, and those of their clients, under PIPEDA when engaging in litigation. Any personal information that is collected, used, or disclosed in connection with reasonably anticipated or actual litigation should be collected either with the express or implied consent of the involved parties, or under one of the exceptions provided under PIPEDA.

4. Exceptions to Consent

The exceptions to the knowledge and consent principle include collection and use for purposes related to investigating a breach of an agreement or a contravention of the law; disclosure to a lawyer (or notary in Qu. . .bec) who is representing the

61. *PIPEDA Case Summary No 2011-003, Re*, (March 25, 2011) 2011 CarswellNat 6886.

62. *Hatfield v Intact Insurance*, 2014 NSSC 232 at para 27.

organization; and disclosure to comply with a subpoena, warrant, court order, or rules of court relating to the production of records.[63]

The OPC has found that information collected by a client may be disclosed to its lawyer, under subsection 7(3)(a) of PIPEDA, if the lawyer or law firm is acting as the client's representative.[64]

PIPEDA also permits the nonconsensual collection, use, or disclosure of certain publicly available information from professional or business directories, statutorily created registries, or documents of a judicial or quasi-judicial body that are available to the public.

5. Use and Disclosure of Personal Client Information

LSPs that market their services using information about clients and prospective clients should be aware of how PIPEDA applies to this activity. Business contact information is outside the scope of PIPEDA only when it is collected, used, or disclosed for the purpose of communicating with an individual in relation to their business or profession.[65]

Additionally, LSPs may receive unsolicited personal information about individuals through referrals. LSPs should not assume that consent has been obtained from the prospective client until the prospective client has contacted the LSP.[66]

LSPs may sometimes find themselves subject to information requests from law enforcement authorities and regulatory

63. *PIPEDA*, *supra* note 46, at s 7.

64. *PIPEDA Case Summary No 218, Re*, (September 5, 2003) 2003 CarswellNat 5816; *PIPEDA Case Summary No 181, Re*, (July 10, 2003), 2003 CarswellNat 5891.

65. Handbook, *supra* note 51, at 7.

66. *Ibid* at 8.

agencies seeking information about their clients. Although PIPEDA permits organizations to disclose personal information about individuals without their consent upon the request of a government institution with the requisite authority, and as required by law, these exceptions have been narrowly interpreted by Canadian courts. Further, professional obligations of confidentiality may prevent this sort of disclosure.

6. Providing Access to Personal Information

Under subsection 8(3), PIPEDA allows individuals to access personal information about themselves held by an organization by submitting a written access request.[67] Upon receipt of a request, the LSP must inform the individual of the existence of their personal information and provide access to the information within thirty days.

Responding to access requests may pose a challenge for many LSPs. Because PIPEDA allows individuals to access their own personal information in the possession of an organization, LSPs and their clients may receive requests for access to personal information from individuals who are adverse to their client's interests. An LSP contemplating or engaged in litigation must still respond to and process access requests from such individuals.[68] That said, LSPs should also be aware that access requests are limited to information "about" the requestors themselves. For example, the OPC has found that it was not necessary for a lawyer to grant the bulk of an access request for information related to an estate under which the requestor claimed

67. PIPEDA, *supra* note 46, at principle 4.9.

68. PIPEDA *Case Summary No 352*, *Re*, (September 8, 2006) 2006 CarswellNat 5578.

to be a beneficiary. The requestor was only entitled to obtain information that was specifically about him.[69]

Further, PIPEDA provides a number of exceptions, such as where the information is protected by solicitor-client or litigation privilege; would reveal confidential commercial information; was collected in the course of an investigation into the breach of an agreement or of a law; or was generated in the course of a formal dispute resolution process.

With respect to privilege, the OPC has required that a party be able to prove the claims of privilege it asserts,[70] and information subject to litigation privilege may need to be provided to a requester once the underlying litigation has ended.[71]

7. Safeguarding Personal Information

The law society and CBA recommendations described above to protect confidential information are also applicable to meet the PIPEDA requirement to safeguard personal information. Limitations on access to files and retention of personal information, technological security measures, and ensuring that third-party vendors apply comparable protections are all central to remaining accountable for personal information in an LSP's control.

8. Retention of Personal Information

LSPs must reconcile their professional obligations regarding file retention with the requirements of PIPEDA. While PIPEDA

69. PIPEDA *Report of Findings No 2013-005, Re*, (October 2, 2013) 2013 CarswellNat 5605.

70. PIPEDA *Case Summary No*. 2008-397, *Re*, (December 18, 2008) 2008 CarswellNat 6817.

71. *Davidson and Williams LLP, Re*, 2011 CarswellAlta 2571, [2013] AWLD 399 at para 129.

requires organizations to retain personal information only as long as necessary for the purpose for which it was collected, professional regulators may require that information be retained as necessary to defend against any future proceedings or to conduct an assessment or review of the file. LSPs should nonetheless limit their retention of personal information to the minimum required in the circumstances.[72]

C. Provincial Statutory Obligations

The provincial privacy statutes in Québec,[73] Alberta,[74] and British Columbia[75] that have been deemed substantially similar to PIPEDA contain similar requirements and exceptions to PIPEDA. Although the provincial statutes and PIPEDA share common objectives and are based upon similar key principles, there are some distinct obligations imposed by the provincial statutes that exceed those imposed by PIPEDA.

The main area for uneven privacy law coverage between the federal and provincial statutes is in relation to employee personal information. PIPEDA only applies to information about employees of organizations that are federal works, undertakings, or businesses. In contrast, the privacy legislation in Québec, British Columbia, and Alberta applies to employee information held by provincially regulated organizations in these provinces. Therefore, LSPs that operate in one of these three provinces should be aware that their privacy obligations may extend to their employees.

---

72. Handbook, *supra* note 51, at 11–12.

73. Québec Act Respecting the Protection of Personal Information in the Private Sector, CQLR, c P-39.1.

74. Alberta Personal Information Protection Act, SA 2003, c P-6.5.

75. British Columbia Personal Information Protection Act, SBC 2003, c 63.

D. Foreign Statutory and Regulatory Requirements

International privacy is a dynamic area of the law in which consumers, private entities, and government actors seek to balance the considerable benefits of technological innovations with critical privacy concerns. The state of the law in the European Union (EU) has fundamentally changed since the implementation of the General Data Protection Regulation (GDPR) in 2018.[76] Among other things, the GDPR implements new protections concerning the transfer of EU citizens' information to non-EU countries.[77] Equally significant, stronger privacy rules have been developed in Latin America, Asia, and certain U.S. states. As a result, many multinational organizations are requesting confirmation that their Canadian legal counsel comply with these laws.

LSPs representing clients based outside Canada, or who are engaged in cross-border files, should consider the application of foreign privacy laws to the PCI they may handle in the course of an engagement. In some circumstances, it may be appropriate to seek foreign law advice before committing to receive or transmit data subject to international privacy laws.

---

76. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 [GDPR], online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents>. A specific Directive (680/2016) on data protection in policing and justice was adopted on May 5, 2016 and applicable as of May 6, 2018: European Data Protection Supervisor *Legislation*, online: <https://edps.europa.eu/data-protection/data-protection/legislation_en>.

77. The GDPR has extraterritorial applicability to cross-border data protection matters. Accordingly, the rights and safeguards provided under the Regulation apply with respect to data transferred outside of the EU: GDPR, *supra* note 76, Article 15.2.

E. Statutory and Common Law Causes of Action

LSPs should be aware of how security breaches or the collection, use, or disclosure of certain types of information may give rise to liability under statutory or common law privacy torts.

A number of provinces have enacted statutory privacy torts. Sections 35-37 of the *Civil Code* of Québec govern causes of action rooted in privacy rights that can be enforced in the courts. British Columbia,[78] Saskatchewan,[79] Manitoba,[80] and Newfoundland and Labrador[81] have similarly passed Privacy Acts that codify limited rights of action for the willful invasion of privacy. In Ontario, the courts have recognized common law torts of intrusion upon seclusion and publication of private facts.[82]

Additional sources of common law liability for data breaches may include: (1) legal malpractice; (2) breach of fiduciary duty; (3) breach of contract; and (4) general tort, including class action negligence claims. For example, an LSP that misuses a client's confidential information may not only be in breach of professional obligations but may also be subject to claims related to legal malpractice and breach of contractual duty to safeguard client information. Similarly, third parties that are injured following a data breach of an LSP's systems may seek legal redress for their injuries if the breach led to disclosure of sensitive personal information. One need only consider the class actions that have followed major data breaches to appreciate the business

78. *Privacy Act*, RSBC 1996 c 373.

79. *Privacy Act,* RSS 1978, c P-24.

80. *Privacy Act*, CCSM, c P125.

81. *Privacy Act*, RSNL 1990, c P-22.

82. *Jones v Tsige*, 2012 ONCA 32 [*Jones*]; *Doe 464533 v ND*, 2016 ONSC 541 [*Doe*].

case for taking adequate steps to secure sensitive information, no matter whose information it is.[83]

As this is a rapidly evolving area of law, LSPs responding to a breach of PCI should consider whether the circumstances of the incident may give rise to civil liability and whether their insurance policies provide coverage for such claims.

F. Client Requirements

A broad range of information security decisions may need to be client-specific, to allow for differences in the client's business judgment and assessment of security risks and costs. When counseling clients about security alternatives, the LSP should document any advice given and ensure that the client has access to technology experts. Upon request from the client, the LSP should clearly disclose the nature of the security measures and policies of the LSP and its vendors. Any decision by the client to forego security measures that the LSP recommends should be documented. In addition, the LSP should, when appropriate, counsel the client about potential liability insurance coverage issues and be mindful that in some situations (especially those that may expose the LSP to third-party lawsuits), the LSP should consider whether to decline to provide representation if a client is unwilling to accept recommended security measures.

83. See, e.g., Drew v Walmart Canada, 2017 ONSC 3308; Elkoby c Google and Google Canada, 2018 QCCS 2623; Lozanski v The Home Depot, 2016 ONSC 5447.

III. CONDUCTING A SECURITY RISK ASSESSMENT

The touchstone of a sound information privacy and security program is its careful tailoring and scaling to the LSP and its practice. This tailored approach begins with an assessment of risk, considering both the probability and the harm or damage that could be caused by an occurrence.[84] LSPs should determine what privacy and security solutions are appropriate to the circumstances using a risk-based analysis, and subsequently develop and implement a reasonable and appropriate information privacy and security program to mitigate risks. Conducting a security risk assessment is a complex task requiring specialized expertise. The information provided below is not intended to be a substitute for a comprehensive professional risk assessment. LSPs will often need to engage a security expert to design and conduct such security assessments.

To properly assess risk, an LSP must consider the importance of maintaining the confidentiality, integrity, and availability of the information it controls. Taken together, these terms mean that information held by an LSP should be protected from unauthorized or accidental alteration, copying, or deletion. Private or confidential information should be protected from those who do not need to use it. Those who must use it must be able to obtain it quickly whenever they need it.

In security terminology, the basic elements common to almost every risk assessment are:

- Asset Identification and Evaluation: LSPs should identify the types of information they handle (e.g., social insurance numbers, payment card

84. *See* National Institute of Standards in Technology Special Publication 800-30, *Guide for Conducting Risk Assessments* (2012), online: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.

numbers, patient records, designs, and human resources data) and the sources of that information, evaluate the sensitivity or relative importance of each type of information, and rank by priority which types require protection and how much protection they require.

- Risk Profiling and Assessment: Analyze the specific threats and vulnerabilities that pose the greatest risk to information assets, including physical loss or damage. The risk assessment process should also examine obligations already facing the LSP: security precautions for client information may already be addressed in retainer agreements—a salutary practice—particularly if client information is to be stored off-site, including in the cloud. Security for third-party information may often be governed by contract or court order.
- Risk Mitigation and Treatment: Once the sensitivity of information assets has been determined and the sources of risks and threats identified and ranked, an LSP can make informed decisions when developing reasonable, proportional responses to the threats and vulnerabilities identified. The practices discussed in Section IV of this *Commentary* provide a guide for such risk mitigation efforts.

All LSPs should consider scaling and prioritizing their information security practices to fit their particular circumstances as they are known at the time. The focus should always be on what is reasonable and appropriate. To determine that, an LSP should first evaluate the type of information it has, who uses the information, and how they use it. The LSP should also consider

which of its employees should have access to information, when they should have it, and whether they have put in place effective measures to prevent unauthorized access. All providers have challenges ensuring security for PCI, but ultimately all need to scale their security programs to meet their own and their clients' needs.

IV. GUIDELINES FOR POLICIES AND PRACTICES THAT ADDRESS PRIVACY AND INFORMATION SECURITY

Information security policies and practices should be scaled to the circumstances of the LSP and the needs of its clients. They may be simple or complex. This Section of the *Commentary* sets out a multifaceted and layered approach to information security.

Not everything set out in this Section can or should be adopted by everyone. Providers should consider cost, business needs, and strategy, but ultimately the reasonableness of the solution is derived from the results of the LSP's risk assessment described in Section III.

This Section identifies a variety of policies and practices that might be used to meet the needs of LSPs and clients. In particular, it addresses the means by which members of the legal services industry may:

- consider the sources of the sensitive information they maintain and the nature of that information;
- identify those within the organization with a bona fide need for access to information, and limit access to those people;
- address information security policies in three subparts: (1) information security in the office and on the network, (2) information security for information that travels outside the office or the network, and (3) information security for information that is shared with experts, consultants, other service providers, and adversaries (either in negotiations or discovery exchanges);
- plan for the disposition of information after it is no longer needed;

- institute a training program that reaches everyone and incentivizes their compliance; and
- anticipate potential breaches by developing plans for prevention, improving detection and response to incidents, preparing to notify affected parties if the information is jeopardized, and adopting contingencies for promptly resolving any problems.

<table>
<tr><th colspan="2">Illustrative Narrative</th></tr>
<tr><td colspan="2">Throughout this section are gray boxes, which contain two sides of a running fictional narrative. It is a depiction of a series of standard cyberattacks, and the simple mitigations that can defeat them. Its intent is to show that while many common attacks are not complicated, a small firm can maintain a reasonable (read, proportional) level of security without undue hardship.

The infrastructure system used in this example is Office 365, but the techniques described (both those used by the attacker, and the defensive measures used by Alex and the firm) can be implemented across many different systems.</td></tr>
<tr><th colspan="2">Introduction to the two players</th></tr>
<tr><td>Alex is a partner at Lawyer, Barrister & Solicitor LLP (LBS LLP), a three-partner law firm which handles the personal legal affairs of several high-profile celebrities.

One Friday, Alex received a phone call from a longtime friend and client, Bryce Bayne, a high-profile, high-</td><td>Haxor3k is the anonymous online username of a malicious hacker that prefers the shadows. It operates internationally, using technical know-how and an ability to manipulate people over the phone and over the internet to extort money or favours from those who fall victim to</td></tr>
</table>

net-worth actor who had recently been in the news following a messy breakup: Bryce's partner was alleging misconduct and threatened to take Bryce to court. Bryce believes that there are messages on his cellphone that prove he was in the right but is concerned that disclosing any of the contents of his phone could be damaging: as an intensely private person, Bryce is sensitive about giving up the phone, even if it will prove his case.	its schemes. Haxor3k noticed the recent news of Bryce Bayne's messy breakup and decided this was an opportunity to extort the celebrity, get some additional leverage for future extortions on other targets, and toy with someone from the shadows.

A. Step 1: Identify the Types and Sources of Information That Must Be Protected

To launch any privacy and information security program, an LSP should first evaluate the type of information it has and collects as well as how it uses that information (discussed in Section III).

Illustration #1: Determining and Gathering Personally Identifiable Information	
Alex speaks to his friend Bryce, cognizant of the intensely personal relationship between a person and one's cellphone in the modern era. As a portal to the	Haxor3k has decided on a target, so now it shifts to reconnaissance. The job now is to gather as much Personally Identifying Information about Bryce as it can, connect

web, a cellphone contains photos, messages, idle musings, and internet search history, which most would rather keep to themselves. Alex argues, however, that these messages should be used to defend Bryce from the unfounded accusations being leveled at him in public and private. For Alex's client, this Personally Identifiable Information is anything that could be tied back to Bryce, be it cellphone call logs (to connect Bryce to a phone number, and those of his closest friends), or a photograph of Bryce at his cottage. Bryce's cottage is remote and thus far undiscovered by paparazzi, and Bryce would prefer to keep it that way. If that cottage photograph were to get out, the background signage, layout of the bay, and architecture of the building could be used to connect the address back to Bryce, destroying his personal privacy.	it together, and determine the best way to move on with its attack. Looking at the last three years of press releases, Haxor3k determines that Lawyer, Barrister & Solicitor LLP often represents Bryce in legal dealings: contract negotiations and publicity agreements. Alex Lawyer was mentioned in a recent news article related to Bryce's messy breakup as a close friend close who lent Bryce support as he retreated from the public eye. Alex looks like a good target: access to intensely personal information, likely communications in writing or over the phone, maybe even in possession of a computer or phone with some juicy extortable material on it. Alex also has a small team so isn't likely to have sophisticated defences in play, and more people means more potential targets. Perfect. Shifting focus to Alex Lawyer and LBS LLP, Haxor3k goes to LBSLLP.ca and copies

	all of the contact information it can find: names, addresses, personal bios of all lawyers and staff on the team. Any cited cases on the website are fair game: it compiles a list of past clients, particularly those that have been a party to multiple newsworthy cases on the LBSLLP.ca website, because these are likely repeat customers. Haxor3k wants to impersonate one of these important customers to gain a level of trust, so it goes to the websites of the discovered clients, pulling the information of likely C-suite accountants or ranking members of the legal department who may be in regular contact with LBS LLP's team. It also runs some online queries and determines that Office 365 is the main back-office communication and storage system used by LBS LLP, and by downloading some PDFs from its website, Haxor3k can guess at the type of PDF editor used on LBS LLP systems.

B. *Step 2: Determine Those Who Need Access*

The LSP should determine who among its members and employees needs to have access to what information and under what circumstances should they have it—keeping in mind that all security breaches and leaks come from one of three possible sources: (1) employees (whether intentionally or inadvertently);[85] (2) lost or stolen media; and (3) intrusions from the outside. The governing information management principle should be "need to know." Only those employees with a specific business purpose requiring access to a particular type of information should have access. Policies should be drafted with this guiding principle in mind.

C. *Step 3: Develop Specifically Tailored Information Security Policies and Practices*

This section addresses information security policies and practices in three distinctly different contexts: security in the office and on the network; security for information outside the office or network; and security for information when it is provided to others. In each of these three situations, a fully adequate information security and privacy program can be scaled to meet the specific needs of the LSP and its clients.

---

85. One article identifies four types of employees who pose risks: the "security softie," who does things he or she should not do; the "gadget geek," who adds devices or software to the system that do not belong there; the "squatter," who uses IT resources inappropriately; and the "saboteur," who hacks into areas where he or she does not belong. The article further notes that "insider threats come from many sources: maliciousness, disgruntled employees, rogue technology, lost devices, untrained staff and simple carelessness." *See* Mark Hansen, *4 types of employees who put your cybersecurity at risk, and 10 things you can do to stop them* (28 March 2014), online: ABA Journal <http://www.abajournal.com/news/article/war_stories_of_insider_threats_posed_by_unapproved_data_services_and_device>.

1. Security in the Office and on Firm-Controlled Systems

(a) Require User Authentication and Permissions

LSPs can protect PCI that is stored on networks or devices by requiring those who seek access to the information to show they have authorization to access it. This means that access to information stored on a network, a computer, or a mobile device should require user authentication through biometric means or passwords or, in the case of multifactor authentication, a password combined with a token or security question. Similarly, where the provider determines (see Step 2 above) that employee and partner access to certain information should be restricted, then users' access should be limited through permissions for designated levels of sensitive information. For example, an LSP might implement role-based access controls, by which its employees' access to information is determined by the type of information and the employee's role in the organization. Such a system might grant varying rights depending on whether a person is a partner, associate, law clerk, administrative assistant, and so forth.[86]

86. For an overview of the subject, see Computer Security Resource Center, *Attribute Based Access Control – Project Overview* (28 March 2018), online: National Institute of Standards and Technology <http://csrc.nist.gov/projects/abac>. For a more detailed review of the topic, see David F. Ferraiolo & D. Richard Kuhn, *Role-Based Access Controls*, 15th National Computer Security Conference (1992), pp. 554–63, online: <https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf>. An alternative, more complicated, system for limited access controls is the attribute-based access control. For an overview of this method, *see Attribute Based Access Control – Project Overview*.

(b) Require Sufficient Password Complexity

Illustration #2: Phishing for Passwords	
Alex started using a Password Manager two years ago, and while the transition took some time, it now saves a lot of time and headache. Alex used to use a password based on the name of his hometown, but eventually it got too hard to remember how many exclamation points were stuck to the end for his bank password, or the number of threes Alex added for the movie theater password. Better yet, with the Password Manager, each password is completely different: there's no guessable pattern to them at all.	Haxor3k knows all of the business email addresses for members of the firm, so it reaches out to contacts on the firm's website, searching for any known passwords associated with these accounts and any account credentials that were exposed during the last decade of data breaches. Finding two accounts and passwords for Alex Lawyer, it tries to log in with these credentials, with no success. It looks as if the old passwords are both based on the name of Alex's hometown, which Haxor3k found on Alex's LinkedIn profile, through Alex's high school. Haxor3k assigns one of its computers to attempt a few thousand variations on this name over the next two days. But still no luck. Since guessing passwords is hard, maybe Alex will simply give them up. Armed with its previous research, Haxor3k decides to go spear phishing.

No matter how the LSP grants or limits access to particular types of information, access to network areas and devices containing confidential information should be protected by "strong" passwords at least. The strength of a password is related to its length and its randomness properties.[87] Length is the greatest contributor to password complexity.[88] However, the complexity of a password alone does not ensure that it is immune from attack. If a password is reused on multiple accounts, through no user action, one website breach can cause a cascade of compromised online accounts.[89]

Password Managers allow users to easily save, store, and retrieve a unique password that is both complex and long for every account they control.

As a potential single source of failure, however, Password Managers must be strongly protected with a unique, long password and additional security measures, such as Two-Step Authentication and conditional-access rules, explained below.

Illustration #3: Alex accidentally reveals a password	
Alex receives a sharing link from his biggest client, Dr. Seo of Seo Inc., who asks for	Haxor3k knows from its PII research that Seo Inc. is a major client of LBS LLP. It

87. *See* Meltem Sönmez Turan et. al., NIST Special Publication 800–132, *Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, Appendix A.1* (2010 December), online: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf>.

88. *See* Paul A. Grassi et. al., NIST Special Publication 800–63-3, *Digital Identity Guidelines* (2020 March), online: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>.

89. This is known as a "credential stuffing" attack, where known usernames and password combinations are tried against other online services. Data breaches are an unfortunate regular occurrence, and these losses often include usernames and passwords for users of the breached service.

a review of a draft contract that needs to be signed by the end of the day. Alex notes that this is an unusual request, but Seo Inc. is important enough to the firm that it always gets what it asks for. Alex replies to Dr. Seo, then clicks the link and is prompted to log in to an Office 365 account so he can review the document. Alex opens the Password Manager, which usually automatically fills in these passwords, and pastes in the password.	also knows that Seo Inc. uses SharePoint. It sets up a fake website (www.office.com.login.downloadshared.fake) that impersonates Microsoft's login page, stealing the credentials of any account that tries to log in. Hakor3k sets up a free Gmail account, using the name Dr. Falsi Seo, the CEO of Seo Inc., and sends an email to Alex Lawyer, inviting Alex to log in and download a draft contract. Haxor3k smiles as Alex enters the password. "We're in."

(c) Impose Conditional Access Rules

Although at times inconvenient for the user, a network ideally would lock out a user who has not revised a password within a prescribed interval, or who has failed to enter a correct password after several incorrect attempts. Other conditional access rules—for example, preventing new logins from non-North-American locations—can further protect systems.

Illustration #4: Haxor3k tries to login as Alex
Haxor3k opens a web browser and enters Alex's email address and the password just phished using the fake Dr. Falsi Seo email account and fake login page. Haxor3k is immediately blocked: it used the right password, but at the moment, it seems that LBS LLP users are not

allowed to log in from outside of North America. Irritated, Haxor3k sets up a virtual environment in a data center in Virginia and tries to log in again from there.

(d) Use Two-Step Authentication

A Two-Step Authentication system (e.g., a notification appearing on a user's token or cellphone, requesting validation before a new device is allowed access to network resources) should, when available, be used to ensure that even in the case of a lost password, a user is notified of login attempts he or she did not initiate. Combined with a Mobile Device Management solution (discussed in Section 2(a) below), these authentication systems allow the LSP to control the flow of information at the borders of its network and beyond.

Illustration #5: Alex receives an unusual alert	
Alex receives a prompt on his phone: there was a request to log in to Alex's account from a computer in Virginia, down in the United States. That's unexpected; Alex hasn't used a new computer, and the last time the login screen appeared there wasn't a Two-Factor prompt. Alex isn't anywhere near Virginia. Denying the login request, Alex now knows about the attack but isn't too worried—he is already changing the main account password, and the unknown	Haxor3k tries to log in from the Virginia computer system, using Alex's username and password. Blocked again! This time it wants Alex to open his phone and authorize the new login. Haxor3k worries for the success of the attack, since Alex might now be aware that something phishy is going on. It's time to get more aggressive and exploit any opportunities available to turn this fiasco into a money-making venture. Haxor3k has invested time

login was already blocked. Alex is relieved that what could have been a serious breach in client trust was immediately averted.	and effort into the reconnaissance phase, so even if this targeted attack (spear phishing) failed, it's not yet time to give up.

(e) Protect Against Malware and Active Threats

Policies should consider which of the LSP's systems are regularly exposed to unknown files and applications, either through user action (downloading a new tool from a sharing website) or incoming communications (spam email). Policies should direct that antivirus software be deployed to mitigate the risk of infection and configured to automatically update and actively monitor systems to ensure that emerging threats are blocked.

Illustration #6: Alex blocks a virus	
Alex appears to be logged into the sharing site and downloads the PDF sent by Dr. Seo, but the firm's antivirus protection immediately quarantines the file: it scanned and detected a malicious file that would have taken over Alex's system. Alex is glad that the firm's antivirus is constantly updating definitions and actively monitoring activity on the network but is worried that Seo Inc. is infected or	Before it launched its phishing attack, Haxor3k set up a website to download a PDF with content that looked like a draft agreement but also contained a nasty surprise: since Haxor3k's research indicated that LBS LLP used an outdated PDF reader with known security issues, it created a malicious file that could break the program and infect the computer system. If the file succeeds, Haxor3k's virus will connect back to Haxor3k's

fell victim to a phishing attack.	systems asking for further instructions, and Haxor3k will be into the firm's infrastructure.

(f) Require Mandatory Reporting

The LSP should consider a requirement for staff to report any suspicious activity noticed on its computer systems, internal or external communications, or any observed attempts to compromise its credentials (for example, an unexpected Two-Step Authentication notification or a pop-up notification encountered by the staff member). Encourage transparency and caution: the sooner the organization is aware of a security incident, the lower its impact. Disincentivizing reporting will hinder your firm's security response.

Illustration #7: Alex notices the attack	
Reviewing the incoming email, Alex is unsure whether the virus originated with the legitimate Dr. Seo but realizes that the Gmail address is not the one Dr. Seo usually uses and isn't associated with Seo Inc. Alex forwards the email to the firm's IT support team, which was selected because of its demonstrable experience and certifications with information security. Alex is worried that the account password may have been	Haxor3k knows that the attack will be more successful if it flies under the radar. By creating a PDF with some somewhat sensible content, it hopes to delay any kind of alarm while Alex reads over the document.

compromised, so Alex also alerts the office manager and then changes the password. Alex acknowledges that there will be some hassle, but thanks to Two-Step Authentication, all of Alex's existing devices already enrolled with device-specific credentials will not need to be changed, since they were not compromised, and the devices are trusted.	

(g) Ensure Physical Security of the Office

Policies should provide for physical security of the LSP's office, including when doors should be locked and who has access to main entrances, offices, conference rooms, storage rooms, and other office locations. For example, a policy might specify that office locations that contain confidential information, whether desk drawers, file cabinets, or file rooms, be locked when not in use, and access should be limited to people who need access. Data on workstations and servers should be encrypted at rest to protect against physical theft.[90] Servers, which typically contain a high concentration of confidential information, should be in a dedicated storage room (or at least a locked cabinet that is physically secured in place in a nonpublic and locked office area). A slightly more elaborate plan may require that all access to areas containing confidential information should be tracked, perhaps through sign-in sheets or, more elaborately, through electronic

90. All major operating systems have built-in support for whole-disk encryption: BitLocker (Windows) and FileVault 2 (Mac) in particular.

verification such as keycards. An even greater level of security might require that servers or records storage areas should have especially limited employee access, perhaps deploying security cameras inside and outside these areas, or an intrusion alert system.[91] Biometric checkpoints may be warranted in some special circumstances.

(h) Restrict the Use of External Media

While there might be valid reasons to use external media such as flash drives, transferring information to portable media can compromise security. The media could introduce viruses or malware to the network. Information copied onto peripheral media can create an additional risk point because the media can easily be transported, lost, or stolen.

Thus, policies should restrict the use of unencrypted external media. LSPs should consider policies that specify when any external media may be used, who may use it, to what devices it may be connected, and how it is to be stored, erased, reused, transferred, and designated for disposal. Such policies can take several forms, from written directives to technical measures that preclude transferring or copying information. LSPs should encrypt portable media to restrict unintended access. As discussed in Section 2(a) below, Mobile Device Management is one method for enforcing these LSP policies.

91. If the office stores Payment Card Information, there is a higher set of requirements. Consider the firm's operational processes and whether there is a legitimate need to store Payment Card Information on the firm's systems. A PCI-DSS certified payment-processing partner is likely an appropriate alternative with less risk.

Illustration #8: "Was this our lost USB?"	
The next day, Alex comes into the office and is greeted by one of the clerks, who was hit by ransomware the previous day. The clerk found an LBS LLP USB stick in front of the building last lunch hour and couldn't get it to work on the office machines, but when plugged into a computer at home, the computer started issuing threats and demanding payment to decrypt personal files. Alex reminds the clerk about the firm's acceptable-use policy and hardware-use policy, which, in a nutshell, states that firm data should stay on firm devices—if the USB was thought to be a firm device, it shouldn't be connected to a personal computer. Further, Alex reminds the clerk that USB storage devices have been disabled on office computers—data should enter the firm either through email or the file sharing service.	Haxor3k decides that the office is the best attack vector, since all other avenues in have failed. It prepares 50 8GB USB sticks with a piece of malware, which will attempt to install itself on any computer that the sticks are connected to, then connect back to one of Haxor3k's command and control servers for further instructions. Haxor3k orders USB sticks with LBS LLP's logo printed on the side to increase the likelihood that they would be connected to a work machine, then drops them on the ground outside of the LBS LLP office and throughout the parking lot. Haxor3k gets five successful connections, all simply to consumer computers and none associated with an LBS LLP work station. Dejected, it makes the most of it by installing a standard ransomware package in an attempt to extort payment.

(i) Protect Network Security

Once an LSP has a single computer connected to a server, Wi-Fi router, or other network-enabled device, it has established a network. At a minimum, that network should then be protected against failure, and if it is connected at all to the outside world, it should be protected against intrusion. Network security requires developing secure infrastructure either in accordance with a client's specific security needs or according to a standard industry benchmark.[92] While the level of security is certainly scalable to fit the circumstances, once a provider moves beyond the most basic level, it will likely need to determine who will monitor the LSP's network for security breaches, how that monitoring will be accomplished, and how the monitors will be monitored. This will generally include an Intrusion

92. Industry certifications can represent a useful benchmark, but LSPs should generally not consider certification, or lack of it, to define the level of security. In addition, providers relying on these or other industry standards to determine third-party security should inquire as to exactly which parts of the third party's business are certified and which are not certified.

International Standards Organization (ISO) is the largest developer of standards in the world. Its membership is drawn from the National Standards Bodies of multiple countries. The International Electrotechnical Commission oversees the development of electrical and electronic standards for participating countries. The 27000 series has been reserved specifically for information security matters. ISO 27001 is a standard describing the best practices for an Information Security Management System (ISMS). An ISMS is "part of the overall management system, based on a business risk approach, to establish, implement, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, processes and resources." ISO/IEC 27000: 2012.

SSAE-16 (Statement on Standards for Attestation Engagements No. 16) is also a commonly used security standard for data centers, as set forth by the Auditing Standards Board of the American Institute of Certified Public Accountants.

Detection/Prevention System to watch for ongoing threats on the network and alert support staff (and potentially block the activity). Policies should describe procedures for regularly monitoring and analyzing network logs and events, and for identifying and addressing potential security breaches.

LSPs that offer Wi-Fi access in their office should ensure that the network is protected through over-the-air authentication and encryption, and their policies should provide protocols for managing and monitoring the Wi-Fi network. Logging features should be enabled so that there is a record of everything that is copied, in the event that data is wrongfully accessed. Wireless networks should be encrypted, and LSPs should not overlook the security of their wireless network. (Currently, Wi-Fi Protected Access II (WPA2) provides the highest level of router protection.) This includes a program for regular network device patching to mitigate newly discovered threats.

Patching network devices, and information technology systems in general, is difficult. Nevertheless, organizations should enable automatic patching where available or establish comprehensive vulnerability and patch management programs.[93] This means that IT partners should be engaged to monitor patches and apply them on a regular basis. In general, maintenance and patching overhead can be managed by simplifying IT systems, when appropriate. Request regular automated patch reports to ensure that the IT partner is dutifully updating systems, and discuss the risks of delayed patching with your IT partner.

Guest Wi-Fi should be provided through a separate network, with no ability to access the rest of the network.

---

93. *See* Canadian Centre for Cyber Security, *Baseline Cyber Security Controls for Small and Medium Organizations* (Retrieved April 2020) online <https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>.

Illustration #9: The virus doesn't spread to office computers

The Clerk who found the USB brought a personal computer into the office to ask the firm's IT staff about the computer.

Alex is alarmed that the infected device was brought to the office, since if the computer had been connected to the standard office network the ransomware could have spread to other systems at the office. However, the firm has an isolated guest network separate from the rest of its resources, so the virus is contained.

(j) Provide for Secure Backup and Disaster Recovery

Information security policies should provide for secure backup of provider information and include disaster/recovery plans, including procedures for restoration. LSPs should consider off-site storage of encrypted backup media, and if they back up client information separately from their own information, these backup processes should also have disaster/recovery plans. Such plans would ideally include specific procedures for backup and restoration that are understood, agreed upon, and maintained in compliance with a written agreement among the clients, providers, and third parties (as appropriate). Conducting regular test restores is highly recommended.

Illustration #10: Backup

Unfortunately, the clerk didn't have a proper backup for her home computer and is wondering what to do. Alex can't offer any suggestions except that sometimes ransomware is cracked and the decryption keys are released for free.

Alex decides to check the firm's backups, ensuring that they are working properly and saved to a separate storage device, which is protected from the rest of the devices on the

office: no users can edit or delete them except for the allowed backup user.

(k) Limit Remote Access to Firm Network

Many LSPs permit employees to access their network from locations outside the office. This access may be through encrypted connections such as a Virtual Private Network or remote access programs in order to maintain privacy and security. Remote access with authentication via Two-Step Authentication and deployment of access controls through role-based access control or attribute-based access control should ensure that those with permission to access certain information are the only people who can access it.[94]

(l) Avoid Use of Third-Party Computers or Networks

LSPs should train employees to avoid publicly available computer systems, such as computers at hotels, when accessing the LSP's network. Once the firm's computer system is accessed from an untrusted computer system controlled by an outside party, any restrictions on further use and dissemination become problematic, and accountability for the information is compromised. Even if the employee is trustworthy and loyal, the LSP should consider whether the employee should be allowed to use the devices of friends and family members to access the provider network or use public networks in locations such as cafes or airports. LSPs should set guidelines regarding the circumstances, if any, when an employee may use public Wi-Fi to transmit client information. Unencrypted client information sent through public Wi-Fi, including paid or free hotspots, can be easily compromised. Therefore, LSPs should clearly specify when use of

94. *See* Turan, *supra* note 87, and accompanying text.

public Wi-Fi is and is not permitted and what additional protections are required.[95]

(m) Provide for Adequate Monitoring and Audits

Oversight is appropriate to ensure that policies are executed correctly to identify remaining areas of risk and to quickly identify breaches. Policies should address who is responsible for audits and how and when audits will be conducted and reported. Monitoring should include all areas of the LSP's business and all processes involving confidential information, although all need not take place at the same time. Checklists can serve as a useful guide to ensure thoroughness of past and future audits.

In addition, real-time tracking and accounting of client information is necessary to identify breaches quickly and help mitigate problems caused by data loss. Immediate notification of appropriate LSP partners and affected clients, as well as any third parties, such as law enforcement authorities or insurers involved in the transport or loss of information, is essential.

LSPs should also require periodic data inventories, e.g., determining what information the LSP has and where it resides. Regular checks on data logs and data inventories provide quality assurance of information security.

(n) Track the Receipt and Creation of Confidential Information

Although sometimes difficult to achieve in practice, LSPs should consider implementing detailed procedures to track client information from receipt until destruction. Such procedures

95. Options for additional protections may include use of virtual private networks, which route data through a private connection. When possible, encrypted connections are also preferred through use of secure "https" addresses instead of "http" for websites and use of a Secure Sockets Layer (SSL) security protocol for applications.

might establish a central point for receiving and tracking client or case-related information and implement a process for logging information received from the client, no matter whether it arrives on an electronic device or external media, through an online transmission (email, FTP site, web file-sharing service, etc.), or in hard copy. Logging the date, sender, recipient, and contents of received information facilitates managing the information. Attaching a label with a unique ID to each piece of any media, device, or hard-copy file received may also help manage them throughout the representation. Logging confidential information allows LSPs to begin a chain of custody that reflects access, copying, transfer, and deletion of the files.

LSPs should also consider whether there is a need to distinguish between client-created information that is sent to them and work product that is generated by the LSP. Although LSPs should treat both types of information as confidential, the LSP may find it easier to create distinct life cycles for provider-created information and client-created information for the purpose of chain of custody and work management, as well as disposition at the end of a matter.

The flow of information into the LSP may also pose a threat: the LSP should consider inserting banners onto messages received from outside of the firm or known to be from other trusted senders, to prevent impersonation or fraud.

Illustration #11: Alex is impersonated over email	
The next day, Alex decides to work from a favourite café, down the street from the LBS LLP office. When Alex drops by the office before heading out, Gray Monie, the firm's	Haxor3k decides to go after the law firm's bank accounts: perhaps it can trick the firm's administrator to wire some funds from the firm's trust account. Creating another fraudulent

administrator, stops Alex for a moment and asks about an unusual email that just came in, purportedly from someone at the firm. Gray noticed the unusual nature of the request: LBS LLP has a standard process for moving trust account balances and doesn't move large sums of money without proper authorization from a partner. Gray also notes that the firm's email system had added a red banner to the bottom of the incoming email: "**Be careful with this message, it was sent from an external source.**"	email, this time impersonating Alex Lawyer, Haxor3k crafts an email to Gray Monie, LBS LLP's office manager. The email uses LBS LLP's standard email signature (which was copied from Alex's reply to the earlier spear-phishing attempt) and a name of a prominent LBS LLP client with simple instructions: "Real Estate Agent LLC has moved one of their files to another firm: transfer the remainder of their trust account to bank routing number 012345678, account 0123456." Haxor3k is again disappointed: it never receives a response from the office administrator.

2. Security Outside the Office and Network

Whenever information moves, it is vulnerable to being diverted, damaged, lost, stolen, or altered. This is true whether a move entails a ride in a cab to the courthouse or a trip around the globe for a meeting. Information security programs should address the movement of information and the potential risks. Where information is subject to special requirements, the LSP should set forth a mechanism for alerting the relevant personnel to those requirements.

Illustration #12: A stolen laptop	
Alex arrives at a favourite coffee shop, setting a bag and phone down at a table to secure a prime spot. Returning from the counter, Alex is alarmed when both are missing. Alex knows that the phone has a password and fingerprint reader, so at least it is secure. The laptop, too. It was automatically encrypted right after it was purchased: as soon as Alex logged into the system with LBS LLP account credentials, LBS's Mobile Device Management policy configured device encryption and auto-lock requirements. Alex checks at the counter, but no one in the busy shop saw who took the bag. Alex returns to the office and asks that the lost phone and laptop be remotely wiped. The phone can't be located, but the wipe command is issued: the next time the phone comes online, the	Haxor3k is now emotionally invested in the attack. Haxor3k flies to Alex's city to physically monitor the front of LBS LLP's office and observes as Alex arrives and then immediately departs the office, heading for a coffee shop. Reviewing Alex's public social media accounts, Haxor3k identifies three Instagram photos tagged with the name of a coffee shop near LBS LLP's office, the same shop Alex just entered and set down a bag at an empty table. Haxor3k wanders into the coffee shop and brushes past the unoccupied table, surreptitiously picking up the bag and cellphone. It walks back to its car, opens the laptop and tries the password phished from Alex the previous day. No luck. The laptop remains locked. Turning to the cellphone, it is again frustrated by a password on the phone. Haxor3k turns off the laptop and extracts its storage drive,

contents of the device will be securely erased.	connecting it to another computer. Unfortunately, the device is encrypted and thus unreadable. Attempting to evade capture, Haxor3k turns on Airplane mode on the cellphone before its location is traced.

(a) Provide for Remote Management of Mobile Devices

Mobile devices, such as laptops, phones, tablets, and PDAs (personal digital assistants) are a practical necessity for LSPs. However, their portability and access to information also make them a target for information theft, even when they are "safely" located within an office environment. The primary tools for protecting the devices from theft and intrusion consist of strong passwords, encryption, auto-locking defaults, device-tracing applications, and applications that allow the devices to be wiped remotely.

Through Mobile Device Management, the LSP can also remotely monitor and update devices (phones, tablets, and laptops). Mobile Device Management technologies can assist with the upkeep of asset inventories and the application of LSP-wide security policies. These systems maintain a list of trusted devices, associated with their primary user, and can enforce strong passwords, encryption, and other information transmission limits. It can thus install remote applications, configure settings, ensure security by updating and running malware detection software at predetermined times (or on demand), enable device firewalls, disable public file sharing, avoid automatic connections to public Wi-Fi, and even track and wipe lost or stolen devices. They can also facilitate a secure Bring Your Own Device

(BYOD) program by separating LSP and client data from the user's personal information.

Centrally managing trusted devices facilitates other advanced security initiatives, such as transparent external storage device encryption (all firm machines may be permitted read or write access to USB media encrypted by the firm, but not to unencrypted external media) or document-level digital rights management, which transparently decrypts a document's contents only when an authorized user on an authorized device attempts to open the file and logs that access to a central monitoring service. These technologies dramatically improve the security of information and the accountability of those with access to it, but they can impede access—they should be deployed only if the results will align with the LSP's security needs or those of its clients, and perhaps only for a subset of files.

Policies should instruct employees to notify the LSP immediately if a mobile device is lost or stolen so the LSP can wipe or disable the device, as appropriate.

Consider the LSP's Hardware Acceptable-Use policies: what is a user's expectation of privacy on a BYOD system, and is a user obligated to permit capture and discovery of the device?

Illustration #13: Remote access, denied and destroyed	
Alex is having a bad 24 hours, so he heads to a local bar with some friends after work.	Haxor3k continues to monitor Alex's movements: after returning, dejected, to the office and completing the rest of the work day, Alex heads to a local bar to relax. Haxor3k follows Alex in, impersonates a server and takes away Alex's empty glass, hoping to extract a

	fingerprint. Using the fingerprint from the glass, it gains access to Alex's phone: unfortunately, it is still in Airplane mode, and there is little actionable content on the phone itself, independent of the firm's network resources. Disabling Airplane mode in an attempt to connect to the firm's files, the phone immediately wipes itself. Another attack foiled.

(b) Encrypt Transferred Data

LSP policies should generally require encryption when private or confidential information is transferred. Unless email is encrypted, LSPs may wish to consider alternative ways to transfer particularly sensitive PCI. Encryption is more than a useful and convenient information security tool. It is critical for protecting client information, especially when the information is stored on mobile devices, transmitted, or stored remotely. Typically, encryption applies an algorithm to convert data to an unreadable code unless it is decrypted using a password. Provided only the sender and recipient of data know a password, the data will be protected against third parties even if the data is lost or intercepted. Encryption keys should be stored separately from the encrypted devices or media to ensure security.

Many operating systems and their supporting hardware can be configured to use encryption for all files or for files selected

by the user.[96] Several different products are available to provide various levels of encryption capabilities. LSPs need to be knowledgeable enough about the different encryption capabilities available to select the appropriate options for their needs. Third-party software for encryption is also readily available. Email applications can be set up to encrypt and automatically decrypt emails. Users simply need to exchange public keys and have their private key applied to decrypt messages; however, this key exchange process is burdensome within most standardized email environments and may lead to inconsistent application. There are third-party services that provide additional capabilities that make key exchange transparent and much easier to use. Mobile devices have encryption options—which can be managed through the device settings—that protect information when the device is locked.

Once information has been encrypted, it may then be securely transmitted through Secure File Transfer Protocol (SFTP), email, or cloud document management services. If information must be transmitted physically, the delivery method should reflect the sensitivity of the information. Highly sensitive information may need to be carried by a private courier or an LSP employee. The method of transport should be considered in avoiding unintended access due to the media being confiscated, lost, or stolen. If information is mailed, it should be sent in a

96. Encrypting files is a critical practice in many circumstances. LSPs should be mindful, however, that in some circumstances encryption may mask the introduction of malware into the network or obscure the theft of information. See Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown Publish Group 2014), ch 14; see also Karen Scarfone et. al., *Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices* (2007 November), online: National Institute of Standards and Technology, Computer Security Research Center <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf>.

manner so that it can be tracked at all times. Unencrypted sensitive information should never be placed in the mail or turned over to a courier for delivery. All too frequently, packages are lost, opened, or stolen in transit.

(c) Educate Regarding External Use Security Considerations

When working outside controlled environments, employees should be instructed to use screen guards to prevent laptop screens from being viewed by the public, and to avoid discussing sensitive information in public. Employees also should be made aware of the vulnerabilities of bluetooth technology and the potential for eavesdropping.

(d) Implement BYOD and Personal Device Policies and Practices

Losing a client's business information, trade secrets, or privileged information can get an LSP in trouble with its client and perhaps with the law society as well. Losing sensitive client information that is subject to special regulatory restrictions, such as health related information, may generate regulatory involvement. Personal devices present one of the most significant risks to client information. These devices include home computers as well as mobile devices such as laptops, smartphones, and tablets. The best defence against the loss or theft of trade secrets, business information, privileged materials, and other sensitive information may be a strong and strictly enforced policy banning the use of personal devices to transact business or store such information. If an LSP permits its employees to use their personal devices to access private or confidential information, the LSP should consider taking the following steps to lessen the risk of using such devices:

- Allowing the use of *only* those devices that are specifically approved by the LSP's security professionals.
- Requiring strong password and encryption policies.
- Limiting the employee's ability to create or store LSP or client information directly on the device, by providing access only through secured portals to provider-protected networks. LSPs may also consider "sandboxing" mobile device applications that contain confidential information to shield provider applications from access by other applications or malware on the device.[97]
- Designating types of client information that should not be accessed, transmitted, or stored on a personal device. This may include information that is subject to specific statutory protections, information that is otherwise highly sensitive, and information that clients have requested not be accessed by BYOD devices.
- Addressing employee home Wi-Fi networks and devices used to create personal hotspots by requiring that these networks be secured with strong passwords that are not shared and are changed regularly.

(e) Limit Carriage of PCI when Traveling Abroad

LSP personnel should avoid traveling across borders with client information or devices capable of accessing the LSP's IT

97. Sandboxing effectively allows a device to host applications or data from multiple sources while blocking the flow of information or data from one part of the device to another.

systems, unless appropriate precautions and safeguards have been taken to account for increased security risks. Because this is a specialized area, LSPs might consider consulting or hiring third parties with expertise in network security involving traveling and transporting data outside the country.

LSPs should specifically address travel to high-risk geographic regions. It may not be possible or advisable for employees to directly access firm systems from high-risk areas. It also may not be advisable to allow employees to carry their normal devices or media with them into high-risk areas, lest they be used to infiltrate the provider's systems. LSPs may also consider requiring employees to travel only with devices that do not contain sensitive information and adjusting default device settings on those devices. In addition, LSPs should consider whether Wi-Fi connections are especially risky and adopt a policy of wiping devices both before traveling through foreign customs and before reconnecting them to the provider's network when they return home.

3. Security Among Third-Party Service Providers

The best information security program in the world can be nullified if the information is vested in the hands of another service provider that does not have adequate safeguards in place. For that reason alone, LSPs have a strong incentive to make sure the information they share with their experts, consultants, litigation support specialists, and other providers is well protected.

LSPs, like their clients and other businesses, increasingly rely on Third-Party Service Providers to process, store, and manage information and IT systems. These TPSPs can include cloud storage providers, online human resource management companies, paper storage and destruction companies, eDiscovery service providers, enterprise-class online productivity services, Software as a Service (SaaS) cloud providers, and providers of

outsourced IT staffing and services. Regardless of the TPSP or type of service offered, LSPs should consider following a set of best practices when engaging the services of such a TPSP on its own or on behalf of a client. Key privacy and information security requirements should always be reflected in the contract between the LSP and the TPSP.

(a) Understand the Type of Information the TPSP Will Handle

Before entering into an agreement with a TPSP, LSPs should carefully consider the type(s) of information that the TPSP will handle. For example, the following questions should be asked about the information to be accessed, processed, or stored by a TPSP:

- Will the TPSP handle client information, or only information belonging to the LSP itself, such as its own human resources information?
- Will the TPSP handle PII, sensitive financial information, trade secrets, or privileged communications and materials?
- Are there any legal or regulatory restrictions imposed on the handling of the information?
- Are there any contractual obligations related to the information?

(b) Ensure Compliance with Applicable Legal and Regulatory Requirements

LSPs should understand the legal and regulatory requirements applicable to the type of information that will be accessed, processed, or stored by the TPSP, and ensure that the TPSP is not only capable of meeting these requirements, but also is contractually obligated to do so.

(c) Understand Geographic and Technical Risks Associated with the TPSP

LSPs should understand where their information will be stored and whether their information will be commingled with information belonging to other customers of the TPSP. TPSPs may store information in a variety of geographic locations, including overseas. The physical location of its information can subject LSPs to litigation and regulatory oversight in the jurisdiction where information is stored. LSPs must therefore understand and approve where its information will be stored. TPSPs may also commingle the information of their other customers. This is generally not a recommended arrangement for LSPs, because their information will be too sensitive to make the risks attendant with commingling acceptable. Thus, LSPs should avoid any arrangement in which information transferred to a TPSP will be commingled.

(d) Conduct Due Diligence

A TPSP's viability is critical, and LSPs should therefore obtain information about the TPSP's potential conflicts and its financial stability. LSPs should also know the scope and policy limits of the TPSP's insurance coverage and ensure that the TPSP performs background checks on its employees and requires employees to sign confidentiality agreements.

(e) Review and Approve the TPSP's Own Information Privacy and Security Policies Prior to Executing a Contract

No TPSP should be retained unless it has an appropriate information security and privacy policy. The TPSP's level of security and privacy protections should generally match or exceed those of the LSP. As a general matter, TPSPs should be retained only if they agree to meet an established standard, such as ISO

27001 and 27002. At a minimum, the LSP retaining a TPSP should consider contractually mandating each of the following:

(i) Physical Security Controls

TPSPs must ensure the physical security of facilities housing sensitive information or from which such information can be accessed, including offices, off-site facilities, and locations of servers. Access to these facilities should be logged. These same recommendations apply to TPSPs that access, process, or store information belonging to the LSP or its clients.

(ii) Information Access Controls

TPSPs need to have appropriate preventative controls on accessing information, including, but not limited to, multifactor authentication utilizing complex passwords, compartmentalization of information on the TPSP's systems, and access restricted to "need to know" individuals.

(iii) Intrusion Detection Systems

If the information provided to the TPSP is highly sensitive and contains significant private or confidential information, LSPs should consider requiring the TPSP to employ an intrusion detection and monitoring system.

(iv) Encryption Procedures

Information sent to a TPSP should be encrypted while in transit to and from the TPSP. LSPs should also consider whether the sensitivity of the information warrants a requirement to encrypt information while it is stored ("at rest") by the TPSP.

(v) Secure Disposition of Information

If the TPSP will store information for the LSP, it should agree that it will only use secure methods for disposing of that

information or any hardware or media on which that information was stored.

(f) Review and Approve the TPSP's Employee Training Program for Information Privacy and Security Prior to Executing a Contract

For both LSPs and TPSPs, proper employee and contractor training programs are essential to maintain information security and privacy. Before entering into an agreement with a TPSP, the LSP should inquire about the TPSP's employee and contractor training programs related to information security and privacy to ensure they are adequate. If the TPSP's training program is inadequate, the LSP should consider mandating the necessary improvements in its contract with the TPSP or finding another TPSP.

(g) Ensure Appropriate Safeguards for Intellectual Property

Contracts with TPSPs should protect the intellectual property rights of the LSP and those of its clients. Use of a TPSP should not alter or adversely affect intellectual property rights.

(h) Require Records Management Compliance

If a TPSP will store any information belonging to the LSP or its clients, the LSP should consider requiring the TPSP to adhere to the relevant existing records management and retention policies.

(i) Mandate Appropriate Information Disposition Upon Termination of the Relationship

The TPSP contract should require the TPSP to adhere to the records policies of the client and to securely dispose of, or return, all the LSP's information in a useable form, in a timely

manner, and upon termination of the relationship. Contractual clauses in which nonpayment on the part of the LSP or its client justify refusal or delay in returning or providing access to information are generally not acceptable.

(j) Consider Bankruptcy Protection

Careful consideration should be given to what will happen if the TPSP becomes insolvent or enters into bankruptcy. This scenario can be specifically addressed in the contract to ensure there is no dispute regarding ownership of the information or the media holding the information. Indeed, in certain situations, LSPs may wish to consider purchasing the physical media on which its information will be stored at the outset of the relationship, so there can be no question regarding the right or ability of the LSP to recover media containing PCI.

(k) Conduct Due Diligence on Information Backup, Disaster Recovery, Access Continuity, and Incident Response

Before sending information to a TPSP, the LSP should be satisfied that the TPSP has adequate plans and equipment for disaster recovery, backup of the LSP's information, and response to incidents such as data breaches. The LSP should also ensure that the TPSP is contractually obligated to provide access to its information without excessive down time and will have an appropriate level of technical support available when needed.

(l) Require Assistance in Discovery

In the event that information under the control of the LSP is in the possession or custody of the TPSP and becomes subject to a litigation hold or discovery obligation, a TPSP should be contractually required to render timely assistance in preserving and collecting information, as appropriate. Accordingly, the TPSP contract should include a clear benchmark for "timeliness" to

avoid confusion regarding the degree of delay acceptable in implementing a litigation hold and preserving and collecting the needed information. Similarly, the agreement should clearly set forth procedures to be followed by the TPSP if it directly receives a warrant, subpoena, or other civil or law enforcement request for the LSP's information. In most circumstances, the TPSP should be required to immediately notify the LSP and cooperate fully with it in responding.[98]

(m) Limit Subcontracting and Onward Transfers

A TPSP generally should not be permitted to allow a subcontractor or other third party to access, process, or store the LSP's information without express prior approval for using the particular subcontractor(s) or allowing the onward transfer(s) of information. Likewise, LSPs should not approve any such arrangements without first confirming that the subcontractor(s) will be legally bound to comply with the same contractual provisions as the original TPSP.

(n) Encourage Accountability Through Shared Liability

The contract between the LSP and the TPSP should consider proper incentives for compliance by imposing some form of liability on the TPSP for harm resulting from any failure to comply with its obligations under the agreement. LSPs should also consider requiring some form of indemnification of the LSP by the TPSP in the event of a data breach or other contract violation that exposes the LSP to liability. It can be challenging to negotiate such provisions because the value of the contract to the TPSP may be far lower than the potential cost of a data breach or other privacy violation. It is common for TPSPs to seek limitations on liability that are closely tied to the fees paid by the LSP, but LSPs

98. In some situations involving requests from law enforcement authorities, immediate notification may be prohibited.

may need to negotiate higher limitations (such as multiples of fees paid) or carve-outs from general limitations of liability in order to protect sufficiently against the security risk and create appropriate incentives to TPSPs to strictly adhere to their obligations. There is also the option of cybersecurity insurance for both the TPSP and the LSP where the potential costs of a breach would far exceed the contractual liability negotiated.

(o) Provide for Inspection and Monitoring

The contract should also give the LSP a right to audit the TPSP's compliance with its information, privacy, and security obligations, or to receive copies of the reports of an independent auditor. If the TPSP is concerned about giving the LSP access to its facilities or systems to test it for conflicts and security concerns, the agreement should allow for use of a mutually acceptable third-party auditor. It is also critical that at least one thorough inspection actually be performed, and not merely permitted in theory. Additionally, parties should negotiate terms that contemplate updates to information privacy and security obligations as related technology and processes evolve.

(p) Ensure Appropriate Access Controls for TPSP Personnel Given Access to LSP IT Systems

Where the contract calls for TPSP's personnel to have access of any sort to the LSP's own IT system, the LSP must make sure that it has appropriate safeguards in place. At a minimum, TPSP personnel who will have the ability to access the LSP's IT system should be subject to a background check, monitoring, and logging for unusual activity, and should have access to only the systems necessary to facilitate the purpose for which the TPSP was engaged. The contract should also address the TPSP's responsibility and role with respect to providing notice and remediation in the event of any loss, theft, or breach of information caused by TPSP personnel.

D. Step 4: Establish Processes for Timely Disposition of Records and Information

LSPs should consider establishing policies, procedures, methods, and technologies suitable for deletion and destruction of client and third-party PCI. Deletion of client information is necessary when directed by a client or triggered by the LSP's information retention policy. In general, information should be deleted when it is no longer needed. This means that LSPs should also ensure timely and thorough deletion of confidential information on devices of departing employees and on retired drives and devices during technology upgrades.

To ensure deletion policies are clearly understood by clients, LSPs should consider, when appropriate, including a standard addendum to engagement letters that addresses the retention and disposition of client and third-party information. Such attachments should address standard policies and practices for the LSP handling the deletion of client information at the end of a matter and provide instructions for the client to communicate its express wishes for the disposition of its information. Mid-matter deletion of certain unneeded documents may also be advisable, if a matter involves particularly sensitive information and is not subject to a preservation obligation. If the provider plans to retain work product containing confidential client information after a matter has closed because it has precedential value, the provider should clearly disclose its intention and obtain client consent. Standard policies and practices shared with clients about deletion of the client's files may address:

- whether the provider holds unique copies of documents potentially subject to a legal hold in other matters and whether the client would benefit from the LSP's retention of certain files from the closed matter;

- the level of sensitivity of the client's information held by the LSP;
- whether the client requires the LSP to retain certain documents, and whether other unnecessary files can be segregated and deleted;
- whether the client wants the LSP to send it a copy of the files to be deleted; and
- whether the client wants the LSP to keep copies of certain documents for safekeeping, and, if so, how those files will be stored.

The client engagement letter, or a related addendum, should also address the disposition of information if a client becomes unavailable after the close of a matter. In that circumstance, the agreement might allow the client's information to be disposed of following a designated waiting period and in compliance with the LSP's applicable legal and ethical obligations.

The waiting period should be set forth in the LSP's policies and made available to the client in the engagement letter. The addendum and a notice of the commencement of the applicable waiting period should be sent to the client after the matter closes. At the end of the applicable waiting period, the LSP should direct that the client's information be disposed of in accordance with the LSP's legal and ethical obligations, unless the LSP becomes aware of a reason to continue to hold the information, e.g., it becomes potentially relevant to other proceedings involving the client. Policies should set forth procedures for a legal hold of the LSP's information in the event the LSP has an expectation that the files may be relevant in future litigation.

LSP policies should account for whether the LSP may have any legal or other obligation to retain files after a client's matter concludes and whether it may need to retain a copy of any files as a record of the work it did for the client. LSPs may therefore wish to create a deletion schedule where the LSP's work product

is held for a longer period than client-created or client-provided information. If the LSP determines it should keep its work product longer than its retention time, it should hold onto the work product for only a reasonable period.

In instances where a client does not consent to retention of its confidential information after the close of a matter, the client file retained by the LSP may still contain work product that the LSP wishes to keep as precedent, form, or history (such as legal memoranda, pleading drafts, or case notes). Under these circumstances, the LSP should "sanitize" those documents, removing PCI before storing the documents in the LSP's precedent bank or file repository.

Deletion of a client's PCI should be comprehensive and involve all locations where the information resides.[99] Deletion will likely require efforts by the LSP's IT personnel and by the employees who accessed client information. To the extent feasible, the LSP should confirm deletion from all potential locations, including document management systems, shared and private network storage, employee email, employee computers, electronic devices, external storage, backup files, and cloud servers.

---

99. "Deletion" methods and underlying hardware can differ in degrees of information recoverability. Physical shredding of the storage media is the most secure deletion of information but may be impractical. Therefore, more commonly acceptable standards of deletion include secure overwrite methods. Most drive electronics have built-in secure erase commands that can be activated with software and thoroughly erase the drive. LSPs may also consider using crypto-deletion where overwrite methods are insufficient or impractical, e.g., cloud services. Crypto-deletion involves encrypting information and destroying the encryption key rather than the information, rendering the information unusable. Deletion policies need to account not only for the LSP's technology infrastructure, but also regulations and requirements for specific types of information. For example, crypto-deletion may not be a valid solution if there is a strict requirement that the information must be scrubbed.

The LSP should also direct that the same steps be taken by any parties to whom they delivered client information, including opposing parties and TPSPs, as well as other LSPs. LSPs should deliver written confirmation to clients of having exercised reasonable diligence in the deletion of PCI.

E. Step 5: Implement Training Program

People have unfortunate tendencies to lose things, speak at inopportune times, open strange emails, visit inappropriate websites, and so forth. Accordingly, LSPs need to train their owners and employees. Begin with teaching people about written information security and privacy policies that document and standardize the provider's practices for maintaining information security and confidentiality. Training should cover client information generally and identify categories of information that may require additional protection, identify applicable federal and provincial or territorial laws, and explain the nature of the client information held and any contractual obligations applicable to it.

Information security and privacy policies clearly apply to all personnel who might handle PCI. This includes the LSP's most senior people, its owners, managers, employees, contract staff, and other parties engaged by the LSP who can access private or confidential information.

Annual training that meets the above criteria is no less important for solo practitioners and their staff than for large law firms. However, it may be impractical for a solo practitioner or small law office to create an internal training program. Instead, such LSPs should consider using an accredited third-party organization; for example, by attending a conference, arranging for an in-house presentation, or employing a web-based solution.

Illustration #14: The training paid off

Considering the impersonation attack that the firm's email banner just warded off, Alex is relieved that the training the firm's administrator took was worthwhile. Alex knows that LBS LLP holds $35,000 in trust for Real Estate Agent LLC and is glad that the firm's annual cybersecurity training—new hires are required to complete cybersecurity training, which the firm outsources to an online provider, and all staff have to renew it with a two-hour review once every two years—has prevented such a sizable potential loss.

The following elements are features that an LSP should consider including in its training program:

1. Make Training Mandatory for All Personnel

An LSP should consider making security training mandatory for all lawyers, paralegals, assistants, law clerks, contract staff, records staff, IT staff, and other personnel, regardless of whether such staff members will have access to sensitive information. Universal mandatory training is beneficial because the nature of IT systems and legal practice makes it highly likely that all employees will encounter private or confidential information at some point during their employment, and even those who do not could still be the source of a security breach that spreads beyond their own computers or office. It takes only one employee holding a door open for someone he or she does not recognize, or clicking on a link in an email message, to compromise an LSP's entire network.

2. Provide for Annual or Biannual Frequency

The nature of security threats and tactics used by hackers and social engineers is constantly changing, as is the underlying technology. Accordingly, LSPs should consider sponsoring training on an annual basis. In addition to formal training on at

least an annual basis, periodic reminders or updates might also be sent to all personnel reminding them of best practices and updating them on emerging threats. Besides keeping personnel informed, such regular reminders show that the LSP takes information privacy and security seriously and expects its employees to do the same. Privacy and security training should also be mandatory for all new hires.

3. Provide for Accountability

There should be clear and meaningful consequences for personnel who fail to successfully complete training or abide by the LSP's privacy and security policies. For example, LSPs that pay bonuses might want to consider reducing bonus compensation for employees who fail to complete training in a specified time frame. Alternatively, they may wish to consider denying such employees access to the LSP's network until training is completed.

4. Include Core Content

An ideal training program may include the following content:

(a) General Background and a Clear Statement of Importance

Training programs should include a general overview or primer that provides a context for addressing information security and privacy issues. This primer should give examples that demonstrate the significance of these issues and the serious consequences that may result when information is inappropriately handled. These examples should reinforce the direct connection between the LSP's adherence to information security and privacy principles and the LSP's reputation and success. This primer will therefore reinforce the serious damages the LSP may likely suffer if it—or its employees—violate laws surrounding

information privacy/security or cause data breaches. These are both group and personal efforts, and training should convey that each employee is personally responsible for maintaining the LSP's standards for privacy and security.

(b) LSP Policies

Training should include all aspects of the LSP's information privacy and security policies, including policies regarding the use of social media and mobile devices.

(c) General Practices

In addition to explaining the LSP's own information privacy and security policies, training programs can include reasonable practices to maintain information security and privacy, such as those set forth in this *Commentary*.

(d) Applicable Ethical, Legal, and Regulatory Rules

Training programs should cover ethical, legal, and regulatory rules applicable to the information held by the LSP.

(e) Applicable Contractual Restrictions

If the LSP has access to information that is covered by contractual obligations, such as where a client has imposed additional information privacy or security restrictions on its information through a business associate agreement, training should cover and highlight those additional requirements.

(f) Role-Specific Requirements

In larger organizations where some employees, such as human resources staff, may be exposed to a large amount of highly sensitive information covered by detailed regulatory requirements, additional role-specific training may be warranted for such employees.

(g) Interactivity and Real-World Scenarios

LSPs may wish to consider implementing training programs that present "real-world" scenarios and prompt participants to indicate how they would respond under similar conditions. For example, such training programs might provide examples of methods successfully employed in the past by hackers and social engineers to bypass security controls and obtain access to private or confidential information. In this way, the trainee can learn from past mistakes made by others and hopefully avoid repeating them.

5. Conduct Testing

In order to facilitate accountability and ensure mastery of the training material, the LSP's training might also include a test that would be scored.[100] Failure to achieve a minimum score would require the individual to continue or repeat the training until a satisfactory score was achieved.

6. Consider Additional Messaging and Reminders

Larger organizations should consider supplementing formal training with posters, screen-saver messages, desk toys, and other aids to remind people on a regular basis of the importance of maintaining privacy and security over the LSP's information.

F. Step 6: Prepare for the Worst

An information security program is not complete unless it includes provisions for the worst possible scenario. Technical problems and human mistakes are inevitable: a device will almost inevitably be lost or stolen, a critical server will irreparably crash, a social engineer will send a phishing email that someone

100. This approach is similar to that already used in many training programs about sexual harassment and other human resources issues.

will click on, or an intruder will breach the firewall and either damage the IT system or steal something, or both. An LSP should prepare and test a data-breach response plan that anticipates common incidents.

This plan might consist of the following:

- Training all personnel to follow procedures for reporting and responding to potential information security breaches, including loss of devices or media, inadvertent transmission of information, or the interception or theft of information.
- Identifying a person or a team to direct the LSP's response to a breach incident.
- Creating a process for conducting a prompt investigation of a suspected breach, including assessing how and when the breach occurred, as well as what information sources have been compromised and what information is contained in those sources. (If an investigation would likely require third-party forensic or IT experts, they should be identified beforehand and listed in the LSP's policy.)
- Depending on the risk profile of the LSP, running periodic "fire drills" or "tabletop" exercises to test the plan under various scenarios. (This will allow for the potential absence of employees who would ordinarily be critical to the successful implementation of the plan.)
- Developing procedures to mitigate damage when a breach is ongoing, bearing in mind that unplugging the affected computer may not necessarily be the best approach to defeat a sophisticated attack or to preserve important evidence.

(Indeed, in some instances the "obvious" source of the intrusion may be a decoy meant to distract the security team from the real assault on the LSP's systems.)

- Establishing contingency plans for providing notice to the owners of compromised information, including clients and other interested parties after a breach or loss is confirmed.
- Developing procedures to revise and adjust policies after an unauthorized disclosure, loss, theft, or other data breach to avoid future occurrences.
- Implementing a system to receive news and updates of reported breaches outside of the LSP, which may affect the LSP's information security.
- Notifying appropriate law enforcement authorities and insurers.
- Abiding by applicable breach notification regulations.

Illustration #15: Back to the cottage	
Alex was under attack. But the firm's simple defences were enough to ward off the attacks and prevent loss of funds and sensitive client information. The firm's processes for dealing with an attack, in this case resetting passwords, wiping devices, and calling in suitable experts, was enough to ensure	Finally tired of this string of failures, Haxor3k decides to move on to easier prey and abandons the attack on LBS LLP, but it saves the research, email accounts, and passwords for potential later use.

that no sensitive data was lost. Contented, Alex calls Bryce, who is still relaxing in the privacy of his secluded cottage, and continues to counsel a dear friend through a difficult time.	

V. CONCLUSION

LSPs have the responsibility to take reasonable steps to protect PCI, a responsibility that is grounded in the ethics rules applicable to LSPs as well as in federal, provincial, and common law rules. In some situations, a duty may also arise under the laws of foreign nations. The nature of the risk, and significance of the potential consequences, must not be underestimated. This *Commentary* is intended to help LSPs assess security risks and provides guidelines for implementing privacy and information security policies. Where appropriate, reliance on third parties for risk identification, assessment, and mitigation measures will be necessary.

Moving the Law Forward in a Reasoned & Just Way