The Sedona Conference Journal®

Volume 19 ❖ 2018 ❖ Number Two

Articles

The Sedona Conference®

Antitrust Law, Complex Litigation, and Intellectual Property Rights

The Sedona Conference Journal®

Volume 19

■

2018

Number 2

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complimentary basis to courthouses and public law libraries. Additionally, each issue is available for purchase ($45; $30 for Working Group Series members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. 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® designed by MargoBDesignLLC at www.margobdesign.com.

Cite items in this volume to "19 Sedona Conf. J. _____ (2018)."

Publisher's Note

Welcome to Volume 19, Number 2, 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, and intellectual property rights. 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 through advanced legal education for the bench and bar.

The various Working Groups in The Sedona Conference Working Group Series (WGS) 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 dialogue-based 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 19, Number 2, of the *Journal* contains two nonpartisan consensus commentaries from The Sedona Conference Working Group on Electronic Document Retention and Production (WG1), one nonpartisan consensus commentary from the Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6), and one nonpartisan consensus commentary from the Working Group on Data Security and Privacy Liability (WG11). Additionally, this issue contains two articles originally presented at our 2017 Inaugural Sedona Conference on Developing Best Practices for Trade Secret Issues, as well as two new articles, each addressing select evidentiary or procedural problems with electronically stored information. I hope you find these articles to be thought-provoking pieces that stimulate further dialogue and ultimately serve to move the law forward.

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

Craig Weinlein
Executive Director
The Sedona Conference
July 2018

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., Redgrave LLP, Washington, DC

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

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

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, Minneapolis, MN

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

The Hon. Craig B. Shaffer (ret.), Denver, CO

Daniel R. Shulman, Esq., Gray Plant Mooty, 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. Ira B. Warshawsky (ret.), Meyer, Suozzi, English & Klein, P.C., Garden City, NY

Table of Contents

THE SEDONA CONFERENCE DATA PRIVACY PRIMER

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

Author:

The Sedona Conference

Editor-in-Chief:

Corey M. Dennis

Senior Editors:

Elise Houlik

Peter B. Miller

Contributors:

Jay Edelson

Jennifer L. Hamilton

Roy E. Leonard

Dana L. Post

Matthew F. Prewitt

Caroline E. Reynolds

Joe Sremack

Staff Editors:

Susan McClain

Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views 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 belongs, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series and 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, *Data Privacy Primer*, 19 SEDONA CONF. J. 273 (2018).

PREFACE

Welcome to the final, January 2018 version of The Sedona Conference *Data Privacy Primer*, a project of The Sedona Conference Working Group Eleven 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 *Data Privacy Primer* will be of immediate and practical benefit to organizations, attorneys, and jurists.

The public comment version of the *Data Privacy Primer* was published in January 2017. After a 90-day public comment period, the editors reviewed the public comments received, and, where appropriate, incorporated them into this final version.

The Sedona Conference acknowledges the efforts of Editor-in-Chief Corey Dennis, who has moved this project forward through its various stages, and senior editors Elise Houlik and Peter Miller, who were key in bringing this publication to fruition. We also thank contributors Jay Edelson, Jennifer Hamilton, Roy Leonard, Dana Post, Matthew Prewitt, Caroline Reynolds, and Joe Sremack for their efforts and commitments in time and attention to this project. We also acknowledge the assistance of Indira Cameron-Banks and Colman McCarthy.

Finally, 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 2018

FOREWORD

Unquestionably, the law of privacy and data protection has rapidly evolved over the past several years. This complex regulatory framework has become both challenging and esoteric to many, including practitioners, legislators, regulators, and courts alike. Recognizing the need for a useful privacy law guide, we developed the *Data Privacy Primer* ("Primer").

This Primer is intended to provide a practical framework and guide to basic privacy issues in the United States and to identify key considerations and resources, including key privacy concepts in federal and state law, regulations, and guidance. It is not an exhaustive treatment of federal or state privacy law or of any particular privacy-related issue, but instead provides a point of entry to privacy issues. This Primer focuses on privacy laws in the United States, and as such, global privacy laws are outside the scope of its coverage, as is a comprehensive treatment of criminal laws relating to privacy and surveillance.

Discussions of privacy inevitably lead to discussions of definitions, principles, goals, and underlying intent. It is beyond the scope of a primer to resolve competing definitions of privacy, to harmonize the many policy and practical considerations required to apply privacy principles to day-to-day business activities, or to take a position about the wisdom (or lack thereof) of existing or planned privacy law. Instead, this Primer addresses privacy as it exists and attempts to provide background and context for understanding and interpreting current privacy laws and requirements.

TABLE OF CONTENTS

I. INTRODUCTION

This Primer begins with a Background and Overview to provide context for the current privacy issues addressed in the main section. That context is found in the common law development of privacy rights in the United States, the Fair Information Practice Principles and similar privacy-protecting frameworks, and in progressive attempts to determine what constitutes personal information that is entitled to privacy protection.

While discussions of "privacy" and "security" naturally go hand-in-hand, it is worthwhile to briefly distinguish between the two concepts. As discussed in more detail below, privacy entails the general right an individual has to determine how his or her personal information is or will be used. Data security, by contrast, entails the logical, physical, administrative, and technical controls that are employed by a party in possession of sensitive information, which can include personal information.

This Primer's focus is principally on providing foundational information concerning the U.S. civil privacy laws and regulations designed to protect an individual's right to control how his or her personal information is used, shared, or otherwise handled by parties in possession of such data. Although criminal law implications are addressed at various points in this Primer, a more systematic treatment of federal criminal law regarding privacy is outside the scope of this Primer.[1]

1. Recently, a number of federal criminal laws with privacy implications, including national security laws (such as the USA Patriot Act and the Foreign Intelligence Surveillance Act), the Computer Fraud and Abuse Act, and laws regarding access to personal communications and information about personal activities (such as the Communications Assistance for Law Enforcement Act and the Electronic Communications Privacy Act) have been the subject of extensive public and legislative scrutiny and debate as a result of the Edward Snowden disclosures and follow-on issues relating to transparency, access, and individual rights to privacy.

After laying that groundwork, the Primer is organized into substantive sections by broad privacy categories for ease of reference, with each such category describing key federal and state laws, policies, and considerations from both a compliance and a litigation perspective. Those categories include "Federal and State Governments," "General Consumer Protection," "Health," "Financial," "Workplace Privacy," and "Student Privacy."

II. BACKGROUND AND OVERVIEW

This background information provides context for the legal and practical requirements discussed in the substantive privacy categories that follow this section.

A. Common Law of Privacy

No serious written discussion of the concept of privacy begins without a reference to the article by Samuel Warren and Louis Brandeis, published in the Harvard Law Review in 1890, titled "The Right to Privacy."[2] The article stands as the most influential article to advocate for a legal right to privacy.[3]

The article was inspired by a rapidly expanding form of media, the printed newspaper, and by concerns about a revolutionary technology, "instantaneous photograph[y]."[4] Warren and Brandeis were concerned about the lack of "protection of the person," and "for securing to the individual" the right "to be let alone."[5] "Instantaneous photographs and newspaper enterprise," they wrote, "have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to

2. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

3. Over 100 years after it was published, the article was described as "brilliant" by the U.S. Court of Appeals for the Ninth Circuit in *Albert D. Seeno Constr. Co. v. Twin City Fire Ins. Co.*, 114 F.3d 1193 (9th Cir. 1997). Judge Richard Posner of the U.S. Court of Appeals for the Seventh Circuit commented in *Anderson v. Romero*, 72 F.3d 518 (7th Cir. 1995), that the "legal concept of privacy . . . originated in a famous article by Warren and Brandeis." *See id.* at 521; *see also* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1342–47.

4. Warren & Brandeis, *supra* note 2, at 195.

5. *Id*.

make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[6]

As explained by Dean Prosser, "[p]iecing together old decisions in which relief had been afforded on the basis of defamation, or the invasion of some property right, or a breach of confidence or an implied contract, the article concluded that such cases were in reality based upon a broader principle which was entitled to a separate recognition. This principle they called the right to privacy."[7]

The privacy right conceptualized by Warren and Brandeis did not receive immediate judicial acceptance. It wasn't until fifteen years after publication of "The Right to Privacy" that the first state supreme court adopted the invasion of privacy cause of action. In 1905, the Supreme Court of Georgia in *Pavesich v. New England Life Insurance Co.*[8] recognized a cause of action in tort nearly identical to the privacy action articulated by Warren and Brandeis.[9] The court found that the right to privacy is a right derived from natural law[10] and that a violation of the right of privacy is a direct invasion of a legal right of the individual.[11] Emphasizing that the invasion of privacy is a tort, the court described the damages to be recovered for its violation "are those for which the law authorizes a recovery in torts of that character; and if the law authorizes a recovery of damages for wounded

6. *Id*.

7. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 384 (1960).

8. 122 Ga. 190 (Ga. 1905).

9. *See* Benjamin E. Bratman, *Brandeis and Warren's "The Right to Privacy and the Birth of the Right to Privacy,"* 69 TENN. L. REV. 623 (2002).

10. *Pavesich*, 122 Ga. at 197.

11. *Id*. at 201–202.

feelings in other torts of a similar nature, such damages would be recoverable in an action for a violation of this right."[12]

The right to privacy concept proposed by Warren and Brandeis[13] is almost universally regarded as the origin of the law of privacy, which consists of four distinct kinds of invasion of four different privacy interests, and which is recognized in the vast majority of states today[14] as set forth in the Restatement (Second) of Torts. The privacy torts may be described as:

- intrusion upon seclusion;[15]
- appropriation of name or likeness;[16]
- public disclosure of private facts;[17] and

12. *Id*.

13. After becoming a Supreme Court Justice, Brandeis relied on the "right to be let alone—the most comprehensive of rights and the right most valued by civilized man" in arguing that the Fourth Amendment's protection against illegal searches and seizures and the Fifth Amendment's guarantee against self-incrimination implied a right to privacy, in his dissenting opinion in *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928), a government wiretapping case.

14. *See* Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998) ("Today, we join the majority of jurisdictions and recognize the tort of invasion of privacy.").

15. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

16. "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasions of his privacy." *Id.* § 652C.

17. "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." *Id.* § 652D.

- false light or "publicity."[18]

Intrusion upon seclusion is the tort claim most often associated with common law privacy liability in the context of data privacy. A privacy violation based on the common law tort of intrusion requires (1) that the defendant intentionally intrude into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy; and (2) the intrusion must occur in a manner highly offensive to a reasonable person.[19] As to the first element of the common law tort, the defendant must have "penetrated some zone of physical or sensory privacy . . . or obtained unwanted access to data" by electronic or other covert means, in violation of the law or social norms.[20] In either case, the expectation of privacy must be objectively reasonable.[21] The second element involves a "policy" determination as to whether the intrusion is highly offensive under the circumstances.[22] "Highly offensive" conduct is not, however, amenable to a precise definition and must be determined on a case-by-case basis.

18. "One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed." *Id.* § 652E.

19. Hernandez v. Hillside, 47 Cal. 4th 272, 286, 211 P.3d 1063, 1072 (Cal. 2009), citing Shulman v. Group W Productions, Inc., 18 Cal. 4th 200, 231 (Cal. 1998) (approving and following RESTATEMENT (SECOND) OF TORTS, § 652B).

20. 47 Cal. 4th at 286; *Shulman*, 18 Cal. 4th at 232.

21. *Id*.

22. *Id*.

B. Fair Information Practice Principles and Similar Privacy-Protecting Frameworks

The concept of a framework of privacy principles to protect personal information began to be formalized within the U.S. government in the early 1970s, as an initiative by the U.S. Department of Health Education and Welfare (now the U.S. Department of Health and Human Services (HHS)) that culminated in the privacy protections built into the Privacy Act of 1974 (5 U.S.C. § 552a). Similar efforts to develop privacy-protecting frameworks were underway outside the United States during that same time frame, including the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).[23]

23. *See* OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (1980), *available at* www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. The OECD Privacy Guidelines were updated for the first time in 2013. *See* 2013 OECD PRIVACY GUIDELINES, Organisation for Economic Co-operation and Development (2013), *available at* http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

Different names have been used for privacy-protecting frameworks in the United States, including the "Code of Fair Information Practice,"[24] "Fair Information Practices,"[25] "Fair Information Practice Principles (FIPPs),"[26] and "Generally Accepted Privacy Principles."[27] Although comparing and harmonizing frameworks and privacy-protection principles is beyond the scope of this Primer,[28] the importance of these frameworks and the accompanying principles is that all share the common goal

24. *See* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, OFFICE OF THE ASSISTANT SECRETARY FOR PLANNING AND EVALUATION, U.S. DEPT. OF HEALTH AND HUMAN SERVICES (1973), *available at* https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

25. For a thorough history of the evolution, application, and operative principles of Fair Information Practices and related frameworks, *see* ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (2017), *available at* https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

26. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (Dec. 29, 2008), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

27. *See* Am. Inst. of Certified Pub. Accountants, Inc. & Canadian Inst. of Chartered Accountants, *Generally Accepted Privacy Principles*, CIPP (2009), *available at* https://www.cippguide.org/2010/07/01/generally-accepted-privacy-principles-gapp/.

28. The American Law Institute is currently working on *Principles of the Law, Data Privacy* (formerly known as RESTATEMENT OF THE LAW, THIRD, INFORMATION PRIVACY PRINCIPLES). As explained in the Reporters' Memorandum regarding this project: "Information privacy law in the United States is currently a bewildering assortment of many types of law that differ from state to state and in federal statutes and regulations . . . . Information privacy law is, therefore, an area of law that requires the type of guidance that the ALI can bring." Paul M. Schwartz & Daniel J. Solove, *Reporters' Memorandum: Restatement Third of Information Privacy Principles, 2013 Preliminary Draft No. 1* ix (2013), *available at* http://scholarship.law.berkeley.edu/facpubs/2238.

of articulating key privacy protection principles that, when adopted and implemented, assist organizations, whether public sector or private, large or small, to manage the privacy risks associated with collecting, retaining, using, and disclosing personal information.

By way of example, the White House, in announcing its strategy for trusted identities in cyberspace, provided the following articulation of the FIPPs in 2011:

- Transparency—Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- Individual Participation and Access—Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- Purpose Specification—Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose(s) for which the PII is intended to be used.
- Data Minimization—Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- Use Limitation—Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purposes for which the PII was collected.

- Data Quality and Integrity—Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- Security—Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Accountability and Auditing—Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.[29]

Over time, these frameworks and their privacy-protecting principles, however articulated, have been incorporated into day-to-day business operations of a significant number of public- and private-sector entities, and they are reflected in much of the federal and state privacy law, enforcement, and guidance discussed in this Primer.

29. *See* THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE CHOICE, EFFICIENCY, SECURITY, AND PRIVACY, Appendix A (April 2011), *available at* https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf. The White House also articulated the Fair Information Practice Principles (FIPPs) in its Consumer Privacy Bill of Rights in 2012, along with a comparison between the Consumer Privacy Bill of Rights to other statements of the FIPPs. *See* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, Appendices A and B (2012), *available at* https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

C. Personal Information

One key step in managing privacy risks is to determine what constitutes "personal information" that requires protection. Unfortunately, there is no universal "one size fits all" definition of "personal information" under laws in the United States or a single applicable legal rule that applies in all circumstances. Instead, as will be discussed below, this definition depends upon the particular law that applies, the context in which it is used, and each organization's privacy policies and procedures.

As a general rule, the level of legal protections afforded under the law to the information varies based upon the sensitivity of the information and the risk that unauthorized access to it could cause injury to an individual. Thus, certain U.S. laws define "personal information" to include social security numbers and other government-issued identification numbers, financial account information, medical information, health insurance information, and identifiable information collected from children.

Although U.S. privacy laws typically apply only to individually identifiable personal information, adopting privacy practices solely based upon this narrow definition may be insufficient from the perspective of consumers, for instance where such information is used for data analytics purposes.[30] Moreover, the definition of "personal information" under the laws of

30. For example, in 2012, a predictive analytics program used by Target to analyze purchase patterns, identify behaviors, and provide focused advertising to individuals generated media controversy and consumer backlash when consumers discovered that Target sent pregnancy-related advertising materials to the home of a high-school student whose family was unaware of her pregnancy. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), *available at* www.nytimes.com/2012/02/19/magazine/shopping-habits.html; *see also* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59 (2014), *available at* http://digitalcommons.law.yale.edu/yjolt/vol16/iss1/2.

other countries, in particular those in the EU, is significantly broader than that under applicable U.S. laws.[31]

Further, in some circumstances, personal information that was thought to have been sufficiently de-identified or anonymized has been re-identified.[32] Opinions vary on the extent to which such re-identification is feasible and cost-effective from a practical perspective, and thus a risk that must be mitigated, but this risk should be considered when using or disclosing such information.[33]

---

31. For example, the EU Data Protection Directive (94/46/EC) defines "personal data" as "any information relating to an identified or identifiable natural person," which includes a broad set of information (e.g., date of birth, address, phone number), as well as identifiable images. *See Opinion of the Article 29 Data Protection Working Party on the "Concept of Personal Data,"* Opinion 4/2007 (June 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

32. For example, Netflix provided purportedly de-identified datasets of subscriber viewing information to participants in a $1 million contest to improve its algorithm for recommending movies based on movies previously viewed and enjoyed. By combining information from other sources with the datasets, researchers were able to re-identify a number of Netflix subscribers, and, after FTC intervention, Netflix decided not to proceed with a planned second contest. *See* FTC Closing Letter to Netflix (Mar. 12, 2010), *available at* www.ftc.gov/sites/default/files/documents/closing_letters/netflix-inc./100312netflixletter.pdf*; see also* Larry Hardesty, *Privacy Challenges*, MIT NEWS (Jan. 29, 2015), *available at* http://news.mit.edu/2015/identify-from-credit-card-metadata-0129.

33. *Compare, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010), *available at* http://www.uclalawreview.org/pdf/57-6-3.pdf, *with* NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, DE-IDENTIFICATION OF PERSONAL INFORMATION, NISTIR 8053 (2015), *available at* http://dx.doi.org/10.6028/NIST.IR.8053. For example, HIPAA provides both a Safe Harbor method and an Expert Determination method for sufficiently de-identifying protected health information to permit its use and disclosure.

As a result of these considerations, many organizations now take a broader view of what constitutes personal information, including taking into account the potentially identifying effect of combining information from several sources. For example, PII under federal government requirements for federal agencies is defined broadly to include "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[34] This approach requires a case-by-case assessment of the specific risk of identifying an individual to determine whether the information constitutes PII, recognizing that non-PII can become PII when combined with other available information.[35] Organizations should consider all of the above when developing policies and practices regarding privacy, data security, and the collection, use, and disclosure of personal information.

34. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM M-10-23, GUIDANCE FOR AGENCY USE OF THIRD-PARTY WEBSITES AND APPLICATIONS, at Appendix (2010), *available at* https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

35. *Id.*; *see also* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM M-07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION, at 1 n.1 (2007), *available at* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf.

D. Industry Standards

Industry standards have been cited at both the state[36] and federal[37] levels when determining the reasonableness of an organization's data security practices and potential liability. For example, the U.S. Federal Trade Commission (FTC) has brought a series of high-profile enforcement actions based upon the failure to implement policies and controls consistent with industry standards.[38] Industry standards typically provide guidance on privacy and data security best practices regarding policies, data use and retention, and information security, including encryption.

36. *See, e.g.*, Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS. CODE REGS. 17.00, 17.01(1) (2010), *available at* http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

37. The FTC has "urge[d] industry to accelerate the pace of its self-regulatory measures" and development of "sector-specific codes of conduct." FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at v–vi (2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

38. *See* PATRICIA BAILIN, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, STUDY: WHAT FTC ENFORCEMENT ACTIONS TEACH US ABOUT THE FEATURES OF REASONABLE PRIVACY AND DATA SECURITY PRACTICES (2014), *available at* https://privacyassociation.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf.

The applicability of industry standards is based on the size,[39] particular business practices,[40] or specific industry[41] of the subject organization. Although not always legally required, compliance with industry standards is becoming increasingly important to mitigate privacy and security risks.[42]

E. Contract-Based Privacy Rights

In the United States, privacy-related rights of individuals have not generally been seen as enforceable (or waivable) through the application of contract law principles. Accordingly, the trend thus far has not been to determine or limit individual privacy rights based on contract law or the terms of express or implied agreements, such as privacy policies, website terms of use, or end user license agreements.[43] However, companies do impose contractual privacy and data security requirements on service providers with which they do business to ensure that

---

39. *See, e.g.*, *Data Privacy for Small Businesses*, BETTER BUS. BUREAU, *available at* http://www.bbb.org/council/for-businesses/toolkits/data-privacy-for-small-businesses (last visited Jan. 1, 2017).

40. *See, e.g.*, PCI SEC. STANDARDS COUNCIL, DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES (2010), *available at* https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

41. *See Cyber Security: New American National Standard Provides Guidance for Industrial Automation and Control Systems*, ANSI (Jan. 16, 2008), *available at* https://www.ansi.org/news_publications/news_story?menuid=7&articleid=c4299bac-df0e-4ce3-9c2f-69a0db54e207.

42. *See* Jedidiah Bracy, *Will Industry Self-Regulation Be Privacy's Way Forward?*, THE PRIVACY ADVISOR (June 2014), https://iapp.org/news/a/will-industry-self-regulation-be-privacys-way-forward.

43. *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588–89, 595–97 and cases and materials cited therein (2014), *available at* http://columbialawreview.org/content/the-ftc-and-the-new-common-law-of-privacy/.

personal information is handled in compliance with applicable laws and best practices.[44]

SIDE BAR — BACKGROUND AND OVERVIEW

Privacy laws and industry standards have evolved over the past century. Today, a complex framework exists, which has evolved based upon common law, statutes, and the Fair Information Practice Principles (FIPPs).

Invasion of privacy tort claims are recognized under the vast majority of state laws. There are several theories of liability upon which such claims may be based (which vary by state), including: (1) an "intrusion upon seclusion" where an individual has a reasonable expectation of privacy; (2) an appropriation of one's name or likeness; (3) a public disclosure of private facts; or (4) false light or "publicity."

The FIPPs and related guidelines, which were developed in the 1970s, form the basis for several U.S. privacy laws, including the Privacy Act of 1974. The FIPPS incorporate a number of key privacy principles, including: access/individual participation, purpose specification, data minimization, use limitation, data quality/integration, security, and accountability/auditing.

Individual privacy rights and organizations' use of personal information today are governed by not only a complex patchwork of state and federal laws, but also industry standards and contractual requirements. Regulators often rely upon industry standards to determine whether an organization maintains reasonable privacy and information security practices.

44. For example, as discussed below, HIPAA covered entities must enter into business associate agreements with their business associates.

III. FEDERAL AND STATE GOVERNMENTS

The federal government has a number of statutory, regulatory, and other obligations (including Executive Orders, Office of Management and Budget (OMB) Memoranda, and National Institute of Standards and Technology (NIST) guidance) that impact its collection, handling, use, disclosure, and disposal of personal information.[45] This section of the Primer addresses key privacy obligations that govern federal agency collection, retention, use, and disclosure of personal information.

A. Federal Government

1. Privacy Act of 1974 (5 U.S.C. § 552a)

Against the backdrop of government surveillance of civil rights activities, the Watergate break-in, and increasing concern about the federal government's ability to compile information about individuals, the Privacy Act of 1974 (5 U.S.C. § 552a) ("Privacy Act")—which incorporated elements of the FIPPs—was enacted to establish requirements for federal agencies' collection, use, sharing, and disclosure of personal information. The Privacy Act generally applies to "any item, collection, or grouping of information about an individual" (i.e., the "record") that is compiled into a system operated by or on behalf of a federal agency (i.e., the "system of records"), but only if the agency

45. As noted above, "personally identifiable information" (PII) under federal government requirements for federal agencies is defined broadly to include "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual." OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM M-10-23, GUIDANCE FOR AGENCY USE OF THIRD-PARTY WEBSITES AND APPLICATIONS, Appendix (2010), *available at* https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

actually uses the individual's name or other personal identifier to access and retrieve personal information from the system.[46]

Under the Privacy Act, federal agencies must identify each of their Privacy Act system of records by publishing a System of Records Notice (SORN) in the Federal Register, and by regularly reviewing and updating agency SORNs as needed. In addition, agencies that collect information directly from individuals must provide them with a Privacy Act statement that identifies the legal authority for collecting the information, the purpose for collecting it, the uses of the information, whether provision of the information is voluntary or mandatory, and what, if any, consequences will result from not providing the information.

As a general rule, federal agencies cannot disclose personal information from a Privacy Act system of records unless the agency has written consent from the individual or the disclosure falls within one of twelve statutory exceptions[47]:

1) "need to know" use by the agency that maintains the record;
2) required disclosure under the Freedom of Information Act (FOIA);[48]
3) "routine uses," i.e., uses that are consistent with the purpose for which the agency collected the information *and* that the agency has identified by publishing in the Federal Register;

---

46. *See* 5 U.S.C. § 552a(a). The Department of Justice oversees federal agency implementation, interpretation, and compliance with the Privacy Act. Its Office of Privacy and Civil Liberties maintains a website that contains resources and guidance and provides a "comprehensive treatise of existing Privacy Act case law." *See* U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974 (2015 ed.), *available at* https://www.justice.gov/opcl/privacy-act-1974.

47. 5 U.S.C. § 552a(b).

48. FOIA is discussed further below.

4) use by the Bureau of the Census;
5) use for statistical research;
6) transfer to the National Archives and Records Administration;
7) use for civil or criminal law enforcement;
8) compelling health or safety circumstances;
9) official use by Congress;
10) official use by the Government Accountability Office;
11) required disclosure by court order; or
12) reporting bad-debt information to a consumer reporting agency after due process.[49]

The Privacy Act gives individuals, with limited exceptions, the right to request an "accounting" that identifies the name, address, date, nature, and purpose of each disclosure of that person's record to any person or any agency.[50] Individuals also generally have the right to access, review, and request correction of records containing information about them, to have those corrections provided to other individuals and entities who have received copies of the information, and to request agency review of any decision not to amend.[51]

Individuals have the right to bring a civil action in federal district court if a federal agency fails to comply with its Privacy Act obligations, and may be entitled to relief that includes actual damages and recovery of reasonable attorney's fees and litigation costs. No private right of action exists against federal employees who violate the Privacy Act, but federal employees who willfully violate the Privacy Act are subject to criminal prosecution for a misdemeanor, as are individuals who obtain records from federal agencies under false pretenses. For purposes of the

49. 5 U.S.C. § 552a(b).

50. *Id.* at § 552a(c).

51. *Id.* at § 552a(d).

Privacy Act, federal contractors who operate a system of records by or on behalf of a federal agency are deemed to be federal employees.[52]

It should be noted that the Privacy Act requires federal and state entities that collect social security numbers (SSNs) directly from individuals to provide them, before collection, with a Privacy Act statement-like disclosure that explains whether their provision of the SSN is mandatory or voluntary, cites the statutory authority for the request, and describes the use of the SSN; and federal and state entities cannot deny benefits solely based on an individual's refusal to provide a SSN.[53] In addition, the Privacy Act limits the circumstances under which federal agencies can engage in "computer matching," in which an agency compares personal information from its systems of records with that from another agency and compiles shared information about individuals.

The Privacy Act has a number of significant carve-outs that limit its applicability. First, it applies only to U.S. citizens and lawfully admitted aliens, although the Judicial Redress Act granting EU citizens the right to legal redress for privacy violations against certain U.S. agencies in U.S. courts was recently passed.[54] Second, there are statutory exceptions that, for example, do the following: prevent individuals from accessing information relating to civil and criminal investigations, law enforcement activities, and national security matters; permit agencies engaged in criminal enforcement or intelligence activities to publicly designate systems of record as exempt from the Privacy

52. *Id.* at § 552a(m).

53. *Id.* at § 552a note.

54. *Id.* at § 552a(a); European Commission Statement by Commissioner Věra Jourová on the signature of the Judicial Redress Act by President Obama (Feb. 24, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-401_en.htm.

Act; and prevent the release of information relating to specified government personnel, promotion, and security activities.[55]

2. E-Government Act of 2002 (Public Law 107-347)

The E-Government Act of 2002 ("E-Gov Act"), applicable to federal government agencies, was enacted to "enhance the management and promotion of electronic Government services and processes" by, among other things, "establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services." This push toward a more modern electronic and digital federal government was accompanied by formal privacy and data security requirements to protect the data, websites, and information systems used by federal government agencies. Although this Primer focuses on the key privacy-related requirements of the E-Gov Act, Title III of the E-Gov Act also created government-wide information security requirements, the Federal Information Security Management Act of 2002 (FISMA).[56]

The OMB provides much of the guidance and interpretation relied on by federal agencies in implementing and complying with the E-Gov Act. OMB maintains a website, https://www.whitehouse.gov/omb/, with information about E-Gov Act initiatives, as well as links to relevant memoranda, reports, and other materials.

---

55. *Id.* at § 552a(d)(5), (j), (k).

56. *See* 44 U.S.C. § 3541–3549. FISMA interpretation and compliance relies heavily on OMB guidance and NIST publications regarding information security-related practices. FISMA 2002 was amended by the Federal Information Security Modernization Act of 2014 to reflect current thinking about information security, compliance, reporting, and oversight.

The privacy protections in Title II of the E-Gov Act[57] are intended to "ensur[e] sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government." The following three key privacy requirements imposed on most federal agencies by the E-Gov Act directly impact the public: conduct a "Privacy Impact Assessment" (PIA); post a privacy policy on federal agency web sites; and protect and limit the use of personal information that federal agencies collect for statistical purposes.

- PIA—Federal agencies must conduct a Privacy Impact Assessment before developing or procuring an IT system or initiating a project that collects, maintains, or disseminates information in an identifiable form from or about members of the public. With certain limited exceptions, completed PIAs must be posted on the agency's public-facing website. Each PIA must address what information is to be collected and why, the intended use of the information (including routine agency uses that may be common to multiple PIAs), who the information will be shared with, what notice or opportunities individuals have to decline to provide information, how the information will be secured (including risk mitigation), and whether the collection of information will create a system of records for purposes of the Privacy Act. In addition, agencies must regularly review and update their PIAs as needed to reflect changes in agency practices that impact privacy-related risks.[58]

57. Title II of the E-Gov Act is reproduced at 44 U.S.C. § 3501 note.

58. Other federal laws impact the content of federal agency PIAs, including the Federal Records Act, which imposes obligations to address retention, disposal, and labeling of information.

- Privacy Policy—Federal agency websites must post a privacy policy that, consistent with the Privacy Act, describes what information is being collected (including automatic collection) and why, how the information will be used and who it will be shared with, what notice and opportunity for consent individuals have with regard to collection and sharing of the information, how the information will be secured, and what rights the individuals have under the Privacy Act "and other laws relevant to the protection of the privacy of an individual." The privacy policy must be clearly labeled, written in plain language, and easy to access in terms of location, machine readability, and accessibility to persons with disabilities. Like PIAs, privacy policies must be reviewed and updated as needed to reflect changes in practices.
- Confidential Collection of Statistical Information—Title V of the E-Gov Act, enacted as the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA),[59] protects individuals and organizations who provide information to federal agencies for statistical purposes under a pledge of confidentiality by making sure that agencies secure the information, do not disclose it in identifiable form, and do not use it for non-statistical purposes. CIPSEA potentially applies, for example, to online and offline surveys conducted by federal agencies and their contractors if

59. Reproduced at 44 U.S.C. § 3501 note; *see also* Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), 72 Fed. Reg. 33,362 (June 15, 2007).

they are represented as being confidential and for statistical purposes. Disclosure of individually identifiable information covered by CIPSEA is a felony.

3. Freedom of Information Act (5 U.S.C. § 552)

The Freedom of Information Act (FOIA) generally requires federal agencies to "make available for public inspection and copying" certain categories of routine agency documents, as well as materials previously released under the FOIA that the agency believes are likely to be subject to multiple requests.[60] In addition, agencies, with certain limitations, must "make records promptly available" to any person who submits a "request for records which reasonably describes such records."[61] Federal agencies can only withhold records or portions of records that fit within one of the nine exemptions at 5 U.S.C. §§ 552(b)(1)–(9). The Department of Justice's (DOJ) Office of Information Policy oversees federal agency compliance with the FOIA and maintains a website that contains current FOIA interpretation and guidance including the comprehensive *Department of Justice Guide to the Freedom of Information Act* ("DOJ Guide").[62]

Although much of the FOIA implicates issues that are beyond the scope of this Primer, two FOIA exemptions specifically protect privacy interests. Exemption 6 protects "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[63] Exemption 7(C) protects "records or information compiled for law enforcement purposes, but only to the extent that

60. 5 U.S.C. § 552(a)(2).

61. *Id.* at § 552(a)(3)(A).

62. *See* OFFICE OF INFO. POLICY, U.S. DEP'T OF JUSTICE, OIP GUIDANCE (2016), *available at* www.justice.gov/oip/oip-guidance.

63. 5 U.S.C. § 552(b)(6).

the production of such law enforcement records or information (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy."[64] As stated in the DOJ Guide, "under both personal privacy exemptions of the FOIA, the concept of privacy not only encompasses that which is inherently private, but also includes an 'individual's control of information concerning his or her person.'"[65]

Under Exemption 6, interest balancing is required, but "[s]ubstantial privacy interests cognizable under the FOIA are generally found to exist in such personally identifying information as a person's name, address, image, computer user ID, phone number, date of birth, criminal history, medical history, and social security number."[66] In contrast, the DOJ Guide asserts that:

> Exemption 7(C) can be applied on a categorical basis. In *DOJ v. Reporters Committee for Freedom of the Press*, the Supreme Court found that a third party's request for law enforcement records pertaining to a private citizen categorically invades that citizen's privacy, and that where a request seeks no official information about a government agency, the privacy invasion is unwarranted. Indeed, the Court of Appeals for the District of Columbia Circuit held in *SafeCard Services v. SEC* that, based upon the traditional recognition of the

64. DOJ Guide, Exemption (7)(C), *available at* www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption7c.pdf.

65. DOJ Guide, Exemption 6 at 1 (citing DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989)), *available at* www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption6.pdf.

66. *Id*. at 10.

> strong privacy interests inherent in law enforcement records, and the logical ramifications of *Reporters Committee*, the categorical withholding of information that identifies third parties in law enforcement records will ordinarily be appropriate under Exemption 7(C).[67]

As a result, notwithstanding that the FOIA is intended to promote openness and transparency and provide ready access to information collected and created by federal agencies, the protections for personal information are relatively strong and well established.

4. The Fourth Amendment

The Fourth Amendment to the U.S. Constitution protects citizens from unreasonable/warrantless searches or seizures by government actors. Evolving technologies make the collection and interpretation of data more readily accessible to federal agencies and law enforcement, placing those parties in the position of justifying their data collection practices over the potential loss of privacy rights of individuals. What constitutes an unreasonable search/seizure of personal information was at the heart of the recent debate concerning the National Security Agency's (NSA) telephone metadata bulk collection practices, ultimately leading to the shut-down of that aspect of the agency's program.[68]

---

67. DOJ Guide, Exemption 7(C) at 1–2 (citations omitted), *available at* www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption7c.pdf.

68. Pete Williams, *Massive NSA Phone Data Collection to Cease*, NBCNEWS.COM (Nov. 27, 2015), *available at* http://www.nbcnews.com/news/us-news/massive-nsa-phone-data-collection-cease-n470521; *see also* Charlie Savage, *Judge Deals a Blow to N.S.A. Data Collection Program*, N.Y. TIMES (Nov. 9, 2015), *available at* http://www.nytimes.com/2015/11/10/us/politics/judge-deals-a-blow-to-nsa-phone-surveillance-program.html.

While traditionally the Fourth Amendment has been most frequently leveraged as a right to suppress evidence in criminal prosecutions, it can also apply in purely civil cases. The use of unreasonably seized information in violation of the Fourth Amendment's privacy protections and causing an injury to a party may give rise to a civil rights claim under 42 U.S.C. § 1983. Further, if a non-government party is acting under color of law with the government, that private party may be subject to the § 1983 claim as well.[69]

These same Fourth Amendment limitations could apply to any other data gathering by the government that is deemed a "search," and what constitutes a reasonable search is an unresolved issue that has evolved over time consistent with technological changes. This has most recently been brought to light when The Federal Bureau of Investigations (FBI) issued a search warrant to Apple compelling the company to assist the FBI in by-passing the encryption technology built into an iPhone device that formerly belonged to terror suspect, Syed Rizwan Farook, who was involved in a mass-shooting in San Bernardino, California. Among the constitutional issues raised by Apple in response to the warrant was the suggestion that while the FBI's search warrant may be technically valid, the method of execution requested to enforce the warrant would be unreasonable under the Fourth Amendment.[70] The FBI later unlocked the

69. *Cf.* Soldal v. Cook County, 506 U.S. 56 (1992) (holding that a police-assisted seizure of a mobile home for eviction purposes raised a claim under the Fourth Amendment, and was a proper § 1983 claim against both the police and the landlord); *see also* Jack M. Beerman, *Why Do Plaintiffs Sue Private Parties Under Section 1983?*, 26 CARDOZO L. REV. 9 (2004), *available at* http://www.nlg-npap.org/sites/default/files/Beermann.pdf.

70. *See* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistance at 35, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate

phone using a third party tool and the DOJ withdrew the case, but the controversy regarding the balance between individual privacy rights and the government's need to conduct law enforcement investigations and ensure national security persists.[71]

5. Federal Criminal Law Enforcement

Federal criminal law prohibits, among other conduct, that which constitutes wire fraud, identity theft, unauthorized access of a computer (including through hacking and/or password trafficking), phishing, accessing and/or disclosing stored communications, and cyberstalking.[72] The Federal Bureau of Investigations (FBI) and United States Secret Service (USSS), and

---

35KGD203, ED No. CM 16-10 (SP) (E.D. Cal. Feb. 25, 2016), *available at* https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf. Seventeen amicus briefs and four letters to the court were submitted in support of Apple's position. *See Amicus Briefs in Support of Apple*, APPLE INC., http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html (last visited Jan. 5, 2017).

71. *See* Mark Skilton & Irene Ng, *What the Apple versus FBI Debacle Taught Us*, SCI. AM. GUEST BLOG (May 20, 2016), http://blogs.scientificamerican.com/guest-blog/what-the-apple-versus-fbi-debacle-taught-us.

72. *See* 18 U.S.C. §§ 1028–1030, 1343, 2261A, 2511, & 2701. There are additional federal criminal statutes prohibiting conduct that impacts privacy in the context of computer or cyber crimes. The January 2015 DOJ Computer Crime and Intellectual Property Section Criminal Division publication, *Prosecuting Computer Crimes*, discusses some of the statutes referenced herein, as well as others; and can be found at http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf. Additionally, discussion about the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*., and the Stored Communications Act, 18 U.S.C. § 2701 *et seq*., can be found in the U.S. Attorneys' Manual at sections 9-48.000, 9-7.000, and 9-60.200, and the U.S. Attorneys' Criminal Resource Manual at sections 1021, 1040, and 1061. *See* http://www.justice.gov/usam/usam-9-7000-electronic-surveillance; http://www.justice.gov/usam/usam-9-48000-computer-fraud; https://www.justice.gov/usam/usam-9-60000-protection-individual;

other sections of the U.S. Department of Homeland Security (DHS), have dedicated units that investigate privacy-related conduct that could constitute computer and/or cyber crimes.[73]

FBI accepts computer and cyber complaints via the FBI Internet Crime Complaint Center (IC3), found at https://www.ic3.gov/default.aspx. The DOJ prosecutes criminal conduct that impacts privacy pursuant to federal criminal statutes.[74]

B. State Governments

Like the federal government, of course, state governments collect substantial amounts of data from and about their own citizens as well as non-residents who pass through their borders. States have adopted laws in several key areas to ensure that government entities properly handle that information.

---

http://www.justice.gov/usam/criminal-resource-manual-1021-18-usc-1030-post-october-1996; http://www.justice.gov/usam/criminal-resource-manual-1040-introduction-criminal-sanctions-illegal-electronic-surveillance; http://www.justice.gov/usam/criminal-resource-manual-1061-unlawful-access-stored-communications-18-usc-2701.

73. *See* https://www.fbi.gov/about-us/investigate/cyber for discussion of the FBI's cyber crime priorities; *see also* http://www.secretservice.gov/investigation/; http://www.dhs.gov/cybersecurity-overview. Federal law enforcement works together as part of a National Cyber Investigative Joint Task Force. *See* https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

74. Such cases are investigated and brought by the DOJ Criminal Division as well as U.S. Attorney's Offices throughout the country. The Criminal Division has a dedicated Computer Crime and Intellectual Property Section (CCIPS), https://www.justice.gov/criminal-ccips, which includes a cybersecurity unit, http://www.justice.gov/criminal-ccips/cybersecurity-unit. In April 2015, CCIPS provided guidance on *Best Practices for Victim Response and Reporting Cyber Incidents*, which can be found at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

1. State Constitutional Privacy Protections

Ten state constitutions reference a right to privacy: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington.[75] More than half these provisions enshrine a general right to privacy that, at least in theory, applies in all contexts. The California Constitution, for example, makes "pursuing and obtaining" privacy an inalienable right, on par with "enjoying and defending life and liberty."[76] The Florida Constitution goes almost as far, but leaves room for some governmental invasions of privacy by declaring that "[e]very natural person has the right to be let alone and free from governmental intrusion into the person's private life *except as otherwise provided herein*."[77] Arizona and Washington also allow for at least some governmental intrusions, providing that "[n]o person shall be disturbed in his private affairs . . . without authority of law."[78] Hawaii and Montana are more restrictive, requiring "the showing of a compelling state interest" to justify any infringement of a person's right to privacy.[79] Alaska, on the other hand, does not even include that limited exception; in Alaska, "[t]he right of the people to privacy . . . shall not be infringed."[80]

In several of the state constitutions that address privacy, the state analogue to the Fourth Amendment explicitly provides

---

75. For a hyperlinked list of the state constitutional provisions referenced here, *see* the National Conference of State Legislatures (NCSL) website at http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

76. *See* CAL. CONST. art. I, § 1.

77. FLA. CONST. art. I, § 23 (emphasis added).

78. ARIZ. CONST. art. II, § 8; WASH. CONST. art. I, § 7.

79. HAW. CONST. art. I, § 6; MONT. CONST. art. II, § 10.

80. ALASKA CONST. art. I, § 22.

that invasions of privacy are prohibited as unreasonable searches and seizures. For example, the Illinois Constitution ensures the peoples' right to be secure "against unreasonable searches, seizures, *invasions of privacy or interceptions of communications by eavesdropping devices or other means*."[81] The Florida Constitution, in somewhat more limited fashion, specifies that "[t]he right of the people to be secure . . . against the *unreasonable interception of private communications by any means*, shall not be violated."[82]

2. Public Records Statutes

Every state—including those whose constitutions provide explicit rights to privacy—has enacted a "public records" law that allows members of the public to obtain documents from state and local government agencies.[83] At the same time, many

---

81. ILL. CONST. art. I, § 6 (emphasis added); *see also* HAW. CONST. art. I, § 7 ("The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and *invasions of privacy* shall not be violated[.]") (emphasis added); LA. CONST. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or *invasions of privacy*.") (emphasis added); S.C. CONST. art. I, § 10 ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and *unreasonable invasions of privacy* shall not be violated[.]") (emphasis added).

82. FLA. CONST. art. I, § 12 (emphasis added). Although the Missouri Constitution does not explicitly refer to "privacy," a 2014 amendment explicitly protects "electronic communications or data, such as that found on cell phones and other electronic devices" against unreasonable searches and seizures. MO. CONST. art. I, § 15.

83. *See, e.g., State Public Record Laws*, FOIADVOCATES, http://www.foiadvocates.com/records.html (hyperlinked list of 50 state laws on access to government records) (last visited Jan. 6, 2017). *See also Privacy/Public Access to Court Records*, NAT'L CENTER FOR STATE COURTS, http://www.ncsc.org/Topics/Access-and-Fairness/Privacy-Public-Access-to-Court-Records/State-

of these states have also passed laws designed to protect certain PII that may be contained in those government records. For example, notwithstanding its public records statute, California law requires the courts in each county, along with the district attorney, to establish procedures to protect victims' confidential personal information that may be contained in various court filings.[84] California also prohibits the disclosure of the names or addresses of victims of certain sex-related crimes in any documents produced in response to requests for records (such as under the Public Records Act).[85] California has also enacted several statutes requiring specified court and other government records to truncate social security numbers in any documents released to the public.[86]

3. Surveillance and Other Data Collection

A number of states have enacted laws designed either to limit the state government's authority to collect certain information about state residents, or to specify whether and how the government can use or disclose that information. This section touches on just a few categories of state-collected information.

Links.aspx?cat=Rules%20on%20Bulk%20Data (hyperlinked list of 38 state laws on access to court records). California even enshrined the right of public access into its constitution. The "Sunshine Amendment," which voters approved in 2004, provides that "[t]he people have the right of access to information concerning the conduct of the people's business, and, therefore, the meetings of public bodies and the writings of public officials and agencies shall be open to public scrutiny." CAL. CONST. art. I, § 3(b)(1).

84. CAL. PENAL CODE § 964.

85. CAL. GOV'T CODE § 6254, CAL. PENAL CODE § 293.

86. *See* CAL. CIV. CODE § 1798.89; CAL. COM. CODE § 9526.5; CAL. EDUC. CODE § 66018.55; CAL. GOV'T CODE § 27300.

(a) Motor Vehicle Records

The federal Drivers Privacy Protection Act (DPPA), 18 U.S. Code § 2721 *et seq*., requires states to provide a minimum baseline of protection to drivers' motor vehicle records, but it does not prohibit states from enacting more stringent provisions. A number of states have done so.[87]

(b) License Plate Readers

Automated license plate readers (ALPRs) employ specialized image-processing technology to identify vehicles by their license plates. ALPRs may be mounted on police cars or fixed structures, like bridges or signs, and can capture images of hundreds of license plates per minute. The technology can assist law enforcement in locating stolen vehicles or wanted individuals. On the other hand, some have expressed concerns about how the data collected by ALPRs is used, pooled, analyzed, and retained.[88]

A minority of states have enacted statutes limiting the use of data collected by ALPRs.[89] While most of those laws limit the use of ALPR technology to law enforcement or other narrowly

87. *See, e.g.*, CAL. VEH. CODE §§ 1808–1821.

88. *See You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/feature/you-are-being-tracked (last visited Jan. 6, 2017). Additionally, use of data collected by these devices may raise Fourth Amendment concerns under the U.S. Constitution. *See* Jessica Gutierrez-Alm, *The Privacies of Life: Automatic License Plate Recognition is Unconstitutional Under the Mosaic Theory of Fourth Amendment Privacy Law*, 38 HAMLINE L. REV. 127 (2015), *available at* https://digitalcommons.hamline.edu/hlr/vol38/iss1/5/.

89. *See Automated Plate Readers: State Statutes Regulating Their Use*, NAT'L CONFERENCE OF STATE LEGIS. (April 13, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plade-readers-alpr-or-alpr-data.aspx.

prescribed purposes, the other standards embodied in the statutes vary widely. For example, there is little consensus on the length of time the data may be retained. On the shorter end, Maine only permits ALPR data to be stored for a mere 21 days.[90] California permits its highway patrol to retain the data for no more than 60 days (unless the data is being used as evidence in a felony case).[91] The rule in Tennessee is 90 days, unless the data are part of an ongoing investigation.[92] Colorado, on the other hand, allows governmental entities to retain images for up to three years.[93]

The states also vary in the extent to which they afford special privacy protection to ALPR data. The Florida statute specifies that ALPR images and data containing personal information are confidential and exempts them from the state's public records law.[94] Maine contains a similar provision.[95] The California statute prohibits selling the data or making it available to non-law-enforcement agencies.[96]

---

90. ME. REV. STAT. ANN. tit. 29-A, § 2117-A(2).

91. CAL. VEH. CODE § 2413.

92. S.B. 1664, 108th Gen. Assemb. (Tenn. 2014) (enacted at TENN. CODE ANN. § 55-10-302 (West)).

93. COLO. REV. STAT. § 24-72-113. After the first year, the custodian of the data may only access it if there has been a claim or a specific incident that may cause the record to become evidence in a civil, labor, administrative, or felony criminal proceeding. *Id*.

94. FLA. STAT. § 316.0777.

95. ME. REV. STAT. ANN. tit. 29-A, § 2117-A(2) (providing that ALPR data is confidential and may be used only for law enforcement purposes).

96. *Id*.

(c) Event Data Recorders

An event data recorder (EDR), sometimes called a "black box," is a device stored in some motor vehicles that records information specifically related to crashes, including "pre-crash vehicle dynamics and system status" and whether or not the vehicle's occupants were wearing seatbelts.[97] About 17 states have passed statutes covering EDRs.[98] Those states uniformly prohibit data collected by the EDR from being downloaded without the owner's consent, except in limited circumstances.[99] The statutes also generally require disclosure to the consumer that the motor vehicle contains an EDR, often in or along with the owner's manual.[100]

97. *See Welcome to the NHTSA Event Data Recorder Research Web Site*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., http://nhthqnlas187.nhtsa.dot.gov/Research/Event+Data+Recorder+%28EDR%29/Welcome+to+the+NHTSA+Event+Data+Recorder+Research+Web+site.

98. *See Privacy of Data From Event Data Records: State Statutes*, NAT'L CONFERENCE OF STATE LEGIS. (Dec. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

99. *See, e.g.*, CAL. VEH. CODE § 9951 (data may also be downloaded by court order, for vehicle safety research, or for servicing of the vehicle).

100. *See, e.g.*, CAL. VEH. CODE § 9951; COLO. REV. STAT. § 12-6-401; ME. REV. STAT. ANN. tit. 29-A, § 1971; NEV. REV. STAT. § 484D.485; N.H. REV. STAT. § 357-G:1; N.Y. VEH. & TRAF. § 416-b.

(d) 911 Call Recordings

Some states have statutes that specifically address whether recordings or transcripts of 911 calls are confidential.[101] More often, those recordings and transcripts fall under the state's public records law.

States that expressly address 911 calls often provide strong protection for the audio recording of the call. For example, in Alabama, audio recordings of 911 calls may not be released (other than to law enforcement) without a court order explicitly finding that the "right of the public to the release of the recording outweighs the privacy interests of the individual who made the 911 call or any person involved."[102] That rule is subject to only a narrow exception providing access for the caller or his or her estate.[103] Pennsylvania, likewise, exempts recordings of 911 calls from public disclosure unless "the agency or a court determines that the public disclosure outweighs the interest in nondisclosure."[104] Mississippi also generally protects the confidentiality of recordings of calls.[105]

Several states distinguish between the audio recording and a written transcript, providing different protection to each form of record. Maine makes *audio recordings* of 911 calls confidential and prohibits their disclosure except in limited circumstances.[106] On the other hand, *transcripts* of the calls are public and must be

---

101. *See State 9-1-1 Legislation Tracking Database*, NAT'L CONFERENCE OF STATE LEGIS. (Jan. 3, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-9-1-1-legislation-tracking-database.aspx.

102. ALA. CODE § 11-98-12.

103. *Id*.

104. 65 PA. CONS. STAT. § 67.708.

105. MISS. CODE ANN. § 19-5-319(2).

106. ME. REV. STAT. ANN. tit 25, § 2929(4).

disclosed in most cases.[107] Minnesota, North Carolina, and North Dakota take essentially the same approach.[108] North Carolina, however, also permits the release of an "altered voice reproduction" of the call.[109]

Other states err on the side of disclosure. In Georgia, for example, 911 calls are public records, and the caller's PII may only be redacted from the records "if necessary to prevent the disclosure of the identity of a confidential source, to prevent disclosure of material which would endanger the life or physical safety of any person or persons, or to prevent the disclosure of the existence of a confidential surveillance or investigation."[110] In Wyoming, the custodian of any information obtained through a 911 call "shall allow any person the right of inspection" of the records unless contrary to law, prohibited by court order, or contrary to the public interest.[111] Similarly, 911 records are presumed open under Virginia law, although personal, medical, or financial information in those records may be withheld if the safety or privacy of any person is jeopardized.[112]

---

107. *Id*.

108. *See* MINN. STAT. § 13.82, subd. 4; N.C. GEN. STAT. § 132-1.4(c), N.D. CENT. CODE § 57-40.6-07.

109. N.C. GEN. STAT. § 132-1.4(c)(4). In North Carolina and North Dakota, the caller's PII is exempt from the public records laws and may always be redacted. *See* N.C. GEN. STAT. § 132-1.4(c); N.D. CENT. CODE § 57-40.6-07 (3).

110. GA. CODE ANN. § 50-18-72(a)(26). In keeping with states' tendency to give more protection to audio recordings, Georgia does exempt from disclosure audio recordings that capture the voices of minors or the cries "in extremis" of any person who died during the call. GA. CODE ANN. § 50-18-72 (26.1). Other audio recordings, however, are not protected by the Georgia statute.

111. WYO. STAT. ANN. § 16-4-203.

112. VA. CODE ANN. § 2.2-3706g.

4. Privacy Policies

About one-third of states have passed laws requiring government agencies to maintain and publicize a privacy policy.[113] California, for example, requires state agencies to adopt a privacy policy and to appoint an employee to be responsible for the policy.[114] A Connecticut statute requires anyone who collects social security numbers in the course of business to create a privacy policy, which must be posted on a publicly-available web page.[115] The policy must limit access to the numbers and prohibit their unlawful disclosures.[116]

States are increasingly adopting legislation to criminalize a wide variety of conduct relating to privacy. The most important categories of state laws relate to computer crimes of various forms, identity theft, and online threats and harassment.

5. State Criminal Statutes

(a) Computer Crimes

State laws criminalize a wide variety of conduct concerning computers, computer systems, networks, and the like.[117] Nearly

113. DEL. CODE ANN. tit. 6, § 1206C. For a hyperlinked list of 17 such state laws, *see State Laws Related to Internet Privacy*, NAT'L CONFERENCE OF STATE LEGIS. (Jan. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

114. CAL. GOV'T CODE § 11019.9; *see also* CAL. STS. & HY. CODE § 31490 (explicitly requiring transportation agency that uses electronic toll collection systems to establish and conspicuously post a privacy policy).

115. CONN. GEN. STAT. ANN. § 42-471.

116. *Id*.

117. *See, e.g., Computer Crime Statutes*, NAT'L CONFERENCE OF STATE LEGIS. (Dec. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx; *State Hacking/Computer Security Laws*, IRONGEEK.COM, http://www.iron

every state makes it a crime to obtain unauthorized access to a computer or system, whether that conduct is described generally as any access obtained without consent[118] or more specifically as hacking,[119] trespass,[120] or tampering.[121] Unauthorized access is often a misdemeanor, but many states provide that aggravating factors, such as accessing a computer in order to further a scheme to defraud or to steal intellectual property, may make the crime a felony. For example, in Oregon, unauthorized access is a misdemeanor, but the crime becomes a felony if the access or attempted access was for the purpose of:

a) devising or executing any scheme or artifice to defraud;
b) obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or
c) committing theft, including, but not limited to, theft of proprietary information.[122]

In at least twelve states, it is a crime to introduce a virus or other "contaminant" into a computer.[123] Just under half the

---

geek.com/i.php?page=computerlaws/state-hacking-laws (last visited Jan. 6, 2017).

118. *See generally* IRONGEEK.COM, *supra* note 117.

119. Only a small handful of states expressly outlaw "hacking." *See, e.g.*, OHIO REV. CODE ANN. § 2909.07(A)(6)(a); S.C. CODE ANN. §§ 16-16-10(j), 16-16-20(4).

120. A number of states have criminalized "trespass" into a computer or computer system. *See, e.g.*, ARK. CODE ANN. § 5-41-104; N.Y. PENAL LAW § 156.10; VA. CODE ANN. § 18.2-152.4.

121. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-2316; 720 ILL. COMP. STAT. ANN. 5/17-51, 5/17-52; MO. ANN. STAT. § 569.095.

122. OR. REV. STAT. § 164.377(2)–(5).

123. *See, e.g.*, FLA. STAT. § 815.04(1); *id*. at § 815.03(3) (defining "computer contaminant" to include viruses and worms).

states have outlawed "spyware" or "adware," which is software that performs certain behaviors on a person's computer without first obtaining their consent, such as advertising and collecting personal information.[124] Similarly, about half of the states have passed statutes specifically criminalizing "phishing," which refers to internet schemes in which a fraudster poses as a legitimate sender in order to dupe the recipient into providing personal information.[125]

State penalties for computer crimes range widely from small fines for misdemeanor offenses to lengthy prison sentences and substantial fines for felonies.[126] Some states also provide for civil remedies for certain computer crimes.[127]

(b) Identity Theft

All 50 states and the District of Columbia criminalize identity theft or impersonation.[128] A slight majority of those statutes

---

124. *See State Spyware Laws*, NAT'L. CONFERENCE OF STATE LEGIS. (Dec. 3, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/state-spyware-laws.aspx.

125. *See, e.g.*, *Phishing*, FED. TRADE COMM'N (Sep. 2011), http://www.consumer.ftc.gov/articles/0003-phishing.

126. For example, in Missouri, "computer tampering" is a Class A misdemeanor subject to a fine not to exceed $1,000. MO. ANN. STAT. §§ 560.016, 569.095. If the tampering was for the purpose of any scheme to defraud, however, the crime is a Class D felony punishable by imprisonment for up to four years, as well as a fine of up to $5,000. MO. ANN. STAT. §§ 558.011, 560.011. In Connecticut, the offense of "computer crime in the first degree" is a class B felony, which could be punished by imprisonment up to twenty years. *See* CONN. GEN. STAT. ANN. §§ 53a-35a, 53a-252.

127. *See, e.g.*, MO. ANN. STAT. § 537.525 (providing for civil action for compensatory damages against anyone who commits computer tampering).

128. *Identify Theft*, NAT'L. CONFERENCE OF STATE LEGIS., http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx (last visited Jan. 6, 2017).

include restitution provisions.[129] In some states, stealing the identity of an elderly person is an aggravating factor leading to stiffer penalties.[130]

One possible method of collecting information for identity theft purposes—scanning or "skimming" of radio frequency identification (RFID) tags—has received particular scrutiny and is the subject of specific legislation in many states. As the National Conference of State Legislatures explains, an RFID tag "consists of a microchip and antenna that, when stimulated by a remote reader, sends back information via radio waves."[131] RFID technology may be used in a number of consumer contexts, from race time trackers to public transit passes to no-swipe tickets at amusement parks—and most notably, in credit cards and even drivers' licenses or ID cards. Although it is not clear whether remote "skimming" of RFID chips is a serious or frequent threat, some states have enacted criminal laws addressing particular RFID applications.[132] In California, for example, it is a crime to remotely read another person's RFID identification document without that person's knowledge or consent.[133]

---

129. *Id*.

130. *See, e.g.*, CONN. GEN. STAT. ANN. § 53a-129b (lower dollar value threshold for class B felony if victim is over sixty years of age).

131. *Radio Frequency Identification (RFID) Privacy Laws*, NAT'L. CONFERENCE OF STATE LEGIS. (Oct. 29, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/radio-frequency-identification-rfid-privacy-laws.aspx.

132. *Id*.

133. *See, e.g.*, CAL. CIV. CODE § 1798.79 (conduct is a misdemeanor, punishable by up to a year in jail and/or a find up to $1,500).

(c) Threats and Harassment

(1) Cyber-Stalking

All 50 states and the District of Columbia have enacted laws criminalizing stalking. A substantial majority of them have now amended their statutes to include language that expressly applies to cyber-stalking, or stalking that occurs online or uses electronic communications.[134] As one cyber-stalking expert has explained,

> cyber-stalking can include threats of violence (often sexual), spreading lies asserted as facts (like a person has herpes, a criminal record, or is a sexual predator), posting sensitive information online (whether that's nude or compromising photos or social security numbers), and technological attacks (falsely shutting down a person's social-media account).[135]

The specific conduct these statutes outlaw varies from state to state. For example, in Alaska, "nonconsensual contact" for purposes of criminal stalking may include "sending mail or electronic communications" to the victim or a family member.[136] In Arizona, on the other hand, felony stalking does not include sending emails, but does cover, "[u]sing any electronic, digital

---

134. *Working to Halt Online Abuse*, http://www.haltabuse.org/resources/laws/ (last visited Jan. 13, 2017).

135. Marlisse Silver Sweeney, *What the Law Can (and Can't) Do About Online Harassment*, THE ATLANTIC (Nov. 12, 2014), http://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/ (quoting Danielle Citron, a professor at the University of Maryland's Francis King Carey School of Law).

136. ALASKA STAT. § 11.41.270(b)(3)(F).

or global positioning system device to surveil a specific person" for twelve hours or on two or more occasions.[137]

(2) Revenge Porn

Following a few high-profile cases that made clear there were gaps in the law, states have recently begun criminalizing "revenge porn," which refers to the publication (usually online) of sexually explicit photographs or videos of a person without their consent. In many cases, the victim's name and address is included along with the images. The practice became known as "[r]evenge porn" because images may be posted by the victim's former partner after a romantic relationship has ended, but in a large number of cases (such as hacking incidents), the perpetrator does not even know the victim. About sixteen states now outlaw revenge porn.[138]

The Illinois statute, passed at the end of 2014, is a particularly powerful example.[139] Unlike some other state laws, the Illinois ban applies to unauthorized publication of "selfies," or photos taken by the victim, as well as photos taken by someone else.[140] The Illinois law is not limited to nude photos, and it also applies to individuals who received the photos secondhand.[141] In Illinois, publishing revenge porn is a Class 4 felony punishable by one to three years in prison, a possible $25,000 fine, and restitution to victims for costs incurred.

---

137. ARIZ. REV. STAT. § 13-2923(C)(1)(a)(ii).

138. Barbara Herman, *Illinois Passes Revenge Porn Law with Teeth*, INT'L BUS. TIMES (Jan. 6, 2015), http://www.ibtimes.com/illinois-passes-revenge-porn-law-teeth-other-states-should-copy-says-privacy-lawyer-1774974.

139. *See* 720 ILL. COMP. STAT. ANN. 5/11-23.5.

140. *Id*.

141. *Id*.

Some states have law enforcement authorities that specifically investigate privacy-related criminal conduct.[142] Oftentimes the state law enforcement agency refers complainants to the FBI's IC3 at https://www.ic3.gov/default.aspx or the FTC's Complaint Assistant at https://www.ftccomplaintassistant.gov/#crnt&panel1-1.

142. State law enforcement efforts vary between states. In order to identify whether a specific state has dedicated law enforcement addressing privacy-related criminal conduct, one should contact the state attorney general's office. For example, California has an "eCrime Unit" that is "tasked with investigating and prosecuting large scale identity theft and technology crimes with actual losses in excess of $50,000." *See Ecrime Unit*, STATE OF CAL. DEP'T OF JUSTICE, https://oag.ca.gov/ecrime (last visited Jan. 6, 2017). Kentucky has a "Cyber Crimes Unit" to "concentrate . . . efforts on cases of online solicitation, scams and identity theft." *See Cyber Crimes Unit*, KY.GOV, https://ag.ky.gov/criminal/dci/cybercrimes/Pages/default.aspx (last visited Jan. 6, 2017).

SIDE BAR — FEDERAL AND STATE GOVERNMENTS

The existing privacy laws governing the collection, use, and safeguards applied to personal information by state and federal governments, as well as the privacy rights of individuals with respect to such governments, are complex and varied.

The Privacy Act of 1974 imposes significant compliance obligations upon federal agencies that maintain a "system of records" that is used to access personal information, as well as government contractors that maintain such a system on behalf of federal agencies. The Privacy Act restricts disclosure of personal information by such agencies, grants individuals a right to access and seek amendment to such information, and generally requires agencies to comply with the FIPPs.

The Fourth Amendment protects citizens from unreasonable/warrantless searches or seizures by government actors, and has been interpreted to provide a right to privacy, including regarding access to electronic data and communications by government actors. Government agencies should consider these restrictions where personal information is accessed without fully transparent consent by the individual.

Many state laws exist that govern the collection, use, disclosure, and access to personal information by state governments and agencies, including laws applicable to motor vehicle records, 911 recordings, and license plate readers. In addition, many state constitutions include a general right to privacy that applies in a wide variety of contexts.

IV. GENERAL CONSUMER PROTECTION

A. Federal Privacy Statutes of General Applicability

1. Federal Trade Commission Act (FTC) Act

In its 2015 privacy and data security update, the FTC reported that, since inception, its privacy and data security enforcement program had been responsible for "over 130 spam and spyware cases and more than 50 general privacy lawsuits" as well as "almost 60 cases against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk."[143] A large number of those matters were brought under Section 5 of the FTC Act, 15 U.S.C. § 45(a), which generally authorizes FTC consumer protection activities to prevent "persons, partnerships, or corporations" subject to FTC jurisdiction from engaging in "unfair or deceptive acts and practices" (UDAP) "in and affecting commerce."[144] The FTC uses its Section 5 authority to bring enforcement actions against entities that fail to protect consumer privacy and fail to properly

143. *Privacy & Data Security Update*, FED. TRADE COMM'N (2015), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2015.

144. The FTC lacks jurisdiction over a number of categories of entities, including non-profit organizations, insurance and financial institutions, and providers of federally regulated transportation and telecommunication services. *See* 15 U.S.C. § 45(a)(2). Other federal agencies have general statutory authority to protect consumers with regard to privacy and data security in areas where the FTC lacks jurisdiction, including, as discussed below, the Federal Communications Commission for issues relating to telecommunications and telemarketing, and the Consumer Financial Protection Bureau with regard to financial institutions. In addition, as discussed in the subject matter sections below, specific privacy and data security statutes vest regulatory and enforcement authority in the FTC and other federal agencies.

secure personal information, as well as to engage in a wide variety of policy, educational, and other activities relating to consumer privacy and data security.[145]

From the FTC's perspective, using Section 5 as a basis for privacy and data security activities is consistent with well-established FTC consumer protection and UDAP principles. As Bureau of Consumer Protection Director Jessica Rich made clear in 2014,

> [T]his is the same Section 5 that we have used for decades to challenge practices involving deceptive advertising and fraud; and the same Section 5 that has been litigated and developed in the courts. There is no separate privacy and data security jurisprudence, but simply application of a tried and true Section 5 standard . . . just as the law has been applied to pyramid schemes, business opportunity scams, weight loss products, cramming, and many other areas of consumer protection.[146]

---

145. Information about the FTC's privacy and data security activities, including cases and educational materials, are available on the FTC website, including at www.consumer.ftc.gov/topics/privacy-identity (consumers), www.ftc.gov/tips-advice/business-center/privacy-and-security (businesses), and www.ftc.gov/datasecurity. In addition, the International Association of Privacy Professionals (IAPP) maintains an online "FTC Casebook," a "full-text searchable, tagged, indexed and annotated" collection of FTC privacy and data security cases, https://iapp.org/resources/ftc-casebook (IAPP membership required).

146. Jessica Rich, *The FTC's Privacy and Data Security Program: Where It Came From, Where It's Going*, Remarks to the International Association of Privacy Professionals Global Privacy Summit (Mar. 6, 2014), *available at* www.ftc.gov/system/files/documents/public_statements/293641/140306iappremarks.pdf.

Businesses and other entities have questioned the FTC's authority to apply Section 5 UDAP standards to privacy and data security matters, particularly given the existence of other more specific statutes that authorize the FTC to regulate and enforce privacy and data security issues for specific categories of activities. Until 2015, however, the FTC's authority to bring privacy and data security enforcement actions under Section 5 of the FTC Act had not been challenged in and substantively reviewed by a federal court of appeals, because the administrative and federal court complaints filed by the FTC in privacy and data security enforcement actions had, with several exceptions, been resolved by settlement agreements. Through what Professors Daniel Solove and Woodrow Hartzog describe as an FTC-developed "common law of privacy":

> the FTC has risen to act as a kind of data protection authority in the United States. Despite having limited jurisdiction and limited resources, the FTC has created a body of common law doctrines through complaints, consent decrees, and various reports and other materials. The FTC's jurisprudence has developed in some classic common law patterns, evolving from general to more specific standards, gradually incorporating more qualitative judgments, imposing certain default standards, and broadening liability by recognizing contributory liability.[147]

In several cases to be litigated to decision rather than resolved by settlements, the FTC's use of Section 5 authority and its failure to provide concrete guidance about specific data security practices have been hotly contested. For example, in its administrative complaint against LabMD, the FTC alleged that

147. Solove & Hartzog, *supra* note 43, at 676.

the medical testing laboratory had unfairly failed to secure personal information.[148] In that matter, the Administrative Law Judge (ALJ) dismissed the FTC's complaint, but the FTC overturned the ALJ's decision and entered an Order finding that LabMD had violated Section 5.[149] LabMD's Petition to Vacate the FTC's Order is currently pending before the U.S. Court of Appeals for the Eleventh Circuit.[150] In its complaint in federal court against a number of Wyndham hotel entities,[151] the FTC alleged that the hotels had deceptively asserted that they protected personal information and unfairly failed to secure that personal information. In August 2015, the U.S. Court of Appeals for the Third Circuit upheld the FTC's authority to "regulate cybersecurity under the unfairness prong of [15 U.S.C.] § 45(a)" in the FTC's action against Wyndham Worldwide.[152] And in *FTC v. D-Link Systems*, the U.S. District Court for the Northern District of California agreed with the Third Circuit that data security falls within the ambit of the unfairness prong of Section 5 as a general matter, but nevertheless dismissed an FTC claim that defendant supplied consumers with insecure Internet routers and cameras

148. *In re* LabMD, FTC Matter No. 102 3099, Docket No. 9357, *available at* www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

149. *In re* LabMD, FTC Matter No. 102 3099, Docket No. 9357 (Commission opinion July 29, 2017), *available at* https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf.

150. *See* LabMD, Inc. v. FTC, No. 16-16270, slip op. at 5, 13 (11th Cir. Nov. 10, 2016) (staying FTC Order pending resolution of LabMD's petition to the Court of Appeals).

151. FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-JAD (D.N.J.), some documents *available at* https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation.

152. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

because it concluded the FTC failed to allege an essential element of an unfairness claim, namely, actual or likely substantial consumer injury.[153]

Under Section 5, the FTC defines deceptive conduct to be "a misrepresentation, omission, or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment."[154] In its privacy and data security enforcement actions, typical FTC deception counts focus on an entity's failure to "do what it says and say what it does" with regard to its privacy and data security practices. For example, in August 2015, the FTC announced settlements with 13 companies that claimed to be current participants in the now defunct EU-U.S. Safe Harbor Framework but whose certifications had either lapsed or never been submitted.[155] Similarly, in March 2015, the FTC announced a settlement with TRUSTe, a company that provided "Certified Privacy Seals" to client websites and mobile applications that complied with privacy program requirements that TRUSTe administered, including the Children's Online Privacy Protection Act and the EU-U.S. Safe Harbor Framework. The FTC complaint alleged that TRUSTe's claim that it recertified its clients annually was deceptive because "from 2006 until January 2013, Respondent did not conduct annual recertifications for all companies holding TRUSTe Certified Privacy Seals.

153. FTC v. D-Link Sys., Inc., No. 3:17-cv-00039-JD, slip op. at 6–10 (N.D. Cal. Sept. 19, 2017).

154. *See also FTC Policy Statement on Deception*, FED. TRADE COMM'N (Oct. 10, 1983), *available at* www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

155. *See* case materials linked to *Thirteen Companies Agree to Settle FTC Charges They Falsely Claimed To Comply With International Safe Harbor Framework*, FED. TRADE COMM'N (Aug. 17, 2015), *available at* www.ftc.gov/news-events/press-releases/2015/08/thirteen-companies-agree-settle-ftc-charges-they-falsely-claimed.

In over 1,000 instances, TRUSTe conducted no annual review of the company's compliance with applicable Program Requirements."[156]

The FTC defines an unfair practice under Section 5 as conduct that satisfies the three prongs of Section 5(n) of the FTC Act, which prohibits the FTC from declaring a practice unfair unless it "[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition."[157] In privacy and data security enforcement actions, typical FTC unfairness counts involve an entity that fails to properly handle and safeguard personal information. For example, the FTC announced settlements with two debt brokers who were trying to sell debt portfolios in an online marketplace and posted information in an unencrypted spreadsheet. The FTC's complaint contained an unfairness count alleging that the would-be sellers:

---

156. *See* case materials linked to *TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program*, FED. TRADE COMM'N (Nov. 17, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its.

157. 15 U.S.C. § 45(n). *See also* Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, U.S. Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (December 17, 1980), reprinted in *In re* Int'l Harvester Co., 104 F.T.C. 949, 1070, 1074 n.3 (1984) ("Unfairness Policy Statement"). Litigants have questioned whether meeting Section 5(n)'s test is *sufficient* to establish unfairness (as the FTC contends) or rather is merely *necessary* for such a finding, with an additional culpability element also being required to be met. This issue was left open by the Third Circuit in *Wyndham*, 799 F.3d at 259 ("The three requirements in § 45(n) may be necessary rather than sufficient conditions of an unfair practice, but we are not persuaded that any other requirements proposed by Wyndham pose a serious challenge to the FTC's claim here."), and currently is before the Eleventh Circuit in LabMD, *see* Brief of Petitioner LabMD, at 26–27 (11th Cir. filed Dec. 27, 2016).

> publicly disclosed consumers' sensitive personal information without the consumers' knowledge or consent, including, consumers' first or last names, addresses, telephone numbers, email addresses, dates of birth, driver's license numbers, credit card numbers, full bank account and bank routing numbers, employers' names and contact information, the consumers' status as purported debtors, and the amount of each consumer's purported debt.[158]

Similarly, the FTC entered a settlement with a medical transcription company that primarily worked online with contract transcribers. The FTC complaint included an unfairness count alleging that the defendants "failed to employ reasonable and appropriate measures to prevent unauthorized access to personal information in audio and transcript files" and that, as a result of that failure, the defendants did not know that the contractor they worked with:

> used a File Transfer Protocol ("FTP") application to both store medical audio and transcript files on its computer network and transmit the files between the network and its typists. The application stored and transmitted files in clear readable text and was configured so that the files could be accessed online by anyone without authentication. A major search engine therefore was able to

158. Fed. Trade Comm'n v. Cornerstone and Co., et al., Case No. 1:14-cv-1479-RC, Dkt. No. 3 at 6–7 (D.D.C. Aug. 27, 2014); *see also Debt Brokers Settle FTC Charges They Exposed Consumers' Information Online*, FED. TRADE COMM'N (April 13, 2015), *available at* www.ftc.gov/news-events/press-releases/2015/04/debt-brokers-settle-ftc-charges-they-exposed-consumers.

> reach . . . and index thousands of medical transcript files . . . .[159]

The FTC has the same range of equitable remedies available to it in privacy and data security enforcement actions that it has for its other Section 5 consumer protection actions. Thus, among other forms of relief, the FTC may seek an ex parte temporary restraining order (including asset freezes and appointment of a receiver, in appropriate cases, to preserve assets and information) and temporary and permanent injunctions to stop the unlawful UDAP conduct and to impose additional "fencing-in" obligations on future conduct. FTC settlements in privacy and data security cases under Section 5 also typically include provisions requiring entities to implement effective privacy and/or data security programs, obtain regular third-party audits of the program(s), and comply with records-retention, compliance, and reporting requirements, usually for a 20-year period. The FTC retains enforcement authority over resolved cases and can bring contempt actions for violation of privacy and data protection orders.

2. Children's Online Privacy Protection Act (COPPA; 15 U.S.C. §§ 6501–6505)

In 1998, Congress enacted the Children's Online Privacy Protection Act (COPPA), which protects personal information of individuals under the age of 13.[160] In general, COPPA prohibits

159. *See* case materials linked to *Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information*, FED. TRADE COMM'N (Jan. 31, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

160. 15 U.S.C. § 6501(1).

operators of commercial[161] websites and online services (including mobile apps) from collecting, using, or disclosing personal information from children except in compliance with COPPA implementing regulations issued by the FTC,[162] or in compliance with a self-regulatory "safe harbor" program that has been reviewed and approved by the FTC.[163] COPPA applies not only to operators of sites and services that are specifically "directed to children," but also to any operator "who has actual knowledge that it is collecting personal information from a child."[164]

As regulator and primary enforcer of COPPA, the FTC maintains COPPA-related information online for businesses and consumers, including educational materials for businesses and consumers, agency guidance and recommendations, FTC policy and enforcement activities, and information about approved safe harbor programs and approved methods for verifying parental consent.[165]

The FTC's COPPA Rule, 16 C.F.R. Part 312, took effect in April 2000, and was last amended effective July 2013. As amended, the COPPA Rule defines personal information to be

---

161. COPPA does not alter the FTC's lack of jurisdiction over non-profit entities.

162. 15 U.S.C. § 6502(a).

163. *Id.* at § 6503.

164. *Id*.

165. *See Children's Online Privacy Protection Rule ("COPPA")*, FED. TRADE COMM'N, www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule; *Children's Privacy*, FED. TRADE COMM'N, www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy (businesses); *Protecting Your Child's Privacy Online*, FED. TRADE COMM'N, www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online (consumers). The FTC also maintains a "COPPA Hotline" for questions not covered by its existing materials, *available at* COPPAHotLine@ftc.gov.

"individually identifiable information about an individual" that is "collected online," including:

a) a first and last name;
b) a home or other physical address including street name and name of a city or town;
c) an e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address, that permits direct contact with a person online;
d) a telephone number;
e) a social security number;
f) a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or
g) information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.[166]

The FTC defines "collection" broadly to include not only directly asking children to submit personal information online, but also providing services that allow children to make their personal information publicly available online (for example, through instant messaging, chat rooms, or bulletin boards), and passively tracking children while they are online (for example, by using cookies or other unique online identifiers).[167]

166. 16 C.F.R. § 312.2.

167. *Id*.

The COPPA Rule identifies a number of factors to be considered when determining whether a website or online service is "directed to children," and thus subject to COPPA, including:

- specific characteristics of the site or service, including subject matter, visual or audio content, age of models, language or other characteristics or online service, and use of animated characters and/or child-oriented activities and incentives;
- extent to which advertising "promoting or appearing" on the website or online service is directed to children; and
- evidence about the intended and actual audience.[168]

To comply with COPPA, operators of websites and online services that collect, use, or disclose personal information from children must:

- provide a privacy notice that is "clearly and understandably written," complete, and contains "no unrelated, confusing, or contradictory materials";[169]
- with limited exceptions, obtain "verifiable parental consent," to the collection of personal information from children;[170]
- provide parents with the ability to review personal information collected from their child and prevent further use or maintenance of that collected information;[171]
- limit the personal information that children must disclose to participate in a game, prize offering, or other

168. *Id.* at § 312.2.

169. *Id*. at §§ 312.3(a), 312.4(a)–(b).

170. *Id*. at §§ 312.3(b), 312.5.

171. *Id.* at §§ 312.3(c), 312.6.

activity to the information than is reasonably necessary to that activity;[172] and

- use "reasonable procedures" to protect the confidentiality, security, and integrity of personal information collected from children.[173]

The requirements for entities that wish to operate self-regulatory programs under COPPA's safe harbor program, and for COPPA-covered operators who wish to use the COPPA safe harbor to be "deemed to be in compliance with" the COPPA Rule, are set forth at 16 C.F.R. § 312.10.

The FTC has primary COPPA enforcement authority to the extent that an entity is subject to FTC Act jurisdiction, and COPPA violations are subject to civil penalties as well as the equitable relief and remedies that are available under the FTC Act.[174] In addition, to the extent the FTC lacks jurisdiction over certain entities (e.g., common carriers, insurance, and financial institutions), the federal agencies with jurisdiction over those entities have COPPA enforcement authority.[175] State attorneys general also have COPPA enforcement authority with regard to conduct affecting their state residents, but that authority must be exercised in consultation with the FTC.[176]

3. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act; 15 U.S.C. §§ 7701–13)

The CAN-SPAM Act addresses concerns about "commercial electronic mail messages," which are defined as "any electronic

172. *Id.* at §§ 312.3(d), 312.7.

173. *Id*. at §§ 312.3(e), 312.8.

174. 15 U.S.C. §§ 6505(a), (d); 16 C.F.R. § 312.9.

175. 15 U.S.C. § 6505(b).

176. *Id*. at § 6504.

mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."[177] Congress noted "the extremely rapid growth in the volume of unsolicited commercial electronic mail," most of which "is fraudulent or deceptive in one or more respects."[178] In general, CAN-SPAM prohibits marketers from using deceptive header information that conceals the identity of the sender and deceptive subject lines that conceal the nature of the communication.[179] It also requires all marketing emails to include a return email address or similar method to opt out of future messages, and requires marketers to honor all such requests.[180]

The CAN-SPAM Act prohibits "aggravated" commercial email activity, which includes automated collection of email addresses from online locations, automated generation of possible email addresses from patterns, automated creation of multiple accounts to send commercial email from, and unauthorized access to and use of a network to send commercial email messages.[181] The FTC implemented the CAN-SPAM Act in its CAN-SPAM Rule, 16 C.F.R. Part 316.

As regulator and primary enforcer of the CAN-SPAM Act and Rule, the FTC maintains CAN-SPAM-related information online, including educational materials, agency guidance and recommendations, and policy and enforcement activities.[182]

---

177. *Id*. at § 7702(2)(a).

178. *Id*. at § 7701(a)(2).

179. *Id*. at §§ 7704(a)(1), (2).

180. *Id*. at §§ 7704(a)(3)–(5).

181. *Id.* at § 7704(b).

182. *See CAN-SPAM Rule*, FED. TRADE COMM'N, www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/can-spam-rule; *CAN-SPAM Act: A Compliance Guide for Business*, FED. TRADE COMM'N, www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

The Rule specifies that the CAN-SPAM Act applies when the "primary purpose" of an email message is commercial.[183] For email messages that contain commercial advertising or promotion blended with other content, the CAN-SPAM Rule provides that the primary purpose will be determined based on the nature of the other content and the manner in which it is presented:

- If the blended content is "transactional or relationship content" that relates to a prior or current business transaction or that provides information about the recipient's ongoing relationship with the business (e.g., warranties, recalls, changes in policies and features), the primary purpose of the email message is commercial if a recipient would reasonably interpret the subject line as relating to advertising or promotion, or if the bulk of the transactional or relationship content does not appear at the beginning of the message.[184]
- If the blended content is something other than transactional or relationship content, the primary purpose of the email message is commercial if a recipient would reasonably interpret the subject line as relating to advertising or promotion or would reasonably interpret the primary purpose of the body of the message—based on factors such as appearance, emphasis, and location of the content in the message—to be advertising or promotion.[185]

For email messages containing sexually oriented material, the first 19 characters on the subject line must be, in all caps and as depicted "SEXUALLY-EXPLICIT:" and that same phrase must also appear when the email is opened, along with the other

183. 16 C.F.R. § 316.3.

184. *Id.* at §§ 316.3(a)(2), (c).

185. *Id*. at § 316.3(a)(3).

required CAN-SPAM elements.[186] Finally, the CAN-SPAM Rule prohibits marketers from charging a fee, collecting information other than email address and opt-out preferences, or otherwise complicating a recipient's ability to opt out of future marketing messages.[187]

The CAN-SPAM Act applies not only to those who directly engage in prohibited conduct, but also to businesses that knowingly allow themselves to be marketed in ways that violate the act (unless they take steps to prevent the violation or notify the FTC), and, under certain circumstances, to third parties working with those businesses.[188]

The FTC has primary CAN-SPAM enforcement authority to the extent an entity is subject to FTC Act jurisdiction, and CAN-SPAM violations are subject to civil penalties, and to the other relief and remedies available under the FTC Act.[189] In addition, to the extent the FTC lacks jurisdiction over certain entities (e.g., common carriers, insurance, and financial institutions), the federal agencies with jurisdiction over those entities have CAN-SPAM enforcement authority.[190] State attorneys general also have CAN-SPAM enforcement authority with regard to conduct affecting their state residents, but that authority must be exercised in consultation with the FTC.[191] Finally, internet service providers who have been adversely affected by CAN-SPAM Act

186. *Id.* at §§ 316.4(a)(1), (2), unless the email recipient has previously provided affirmative consent, as defined in 15 U.S.C. § 7702.

187. 16 C.F.R. § 316.5.

188. 15 U.S.C. §§ 7705(a), (b).

189. *Id.* at §§ 7706(a), (d).

190. *Id.* at § 7706(b).

191. *Id*. at § 7706(f).

violations can seek injunctive relief and damages in federal district court.[192]

In addition to actual damages, treble damages are available in certain instances for "knowing and willful violations" of the CAN-SPAM Act and for the aggravated violations defined in § 7704(b). Note that, when seeking cease-and-desist orders and other forms of injunctive relief, the FTC, the Federal Communications Commission, and state enforcement entities are exempt from CAN-SPAM Act requirements to allege and prove a particular state of mind.[193]

Although the primary relief and remedies under the CAN-SPAM Act are civil, the act provides for criminal liability in certain circumstances. Congress noted that "[s]ome commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature."[194] As a result, failure to comply with the requirement that messages containing sexually oriented material be identified in the subject line and that the explicit material not be displayed upon opening but instead provide a link or similar mechanism,[195] can give rise to criminal liability.[196] Similarly, because "spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems," Congress instructed the U.S. Sentencing Commission to "review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate penalties for . . . offenses that may

192. *Id*. at § 7706(g).

193. *Id*. at §§ 7706(e), (f)(2).

194. *Id*. at § 7701(a)(5).

195. *Id*. at § 7704(d).

196. *Id*. at § 7704(d)(5).

be facilitated by the sending of large quantities of unsolicited electronic mail."[197]

4. Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"; 15 U.S.C. §§ 6101–6108)

The Telemarketing Act is the FTC equivalent of the Federal Communication Commission's (FCC) Telephone Consumer Protection Act of 1991 (TCPA; 47 U.S.C. § 227), although the FCC's TCPA jurisdiction is broader than the FTC's Telemarketing Act jurisdiction. Given the overlapping authority over telemarketing activity and the joint coordination regarding the National Do Not Call Registry, the FTC and the FCC coordinate many of their telemarketing policy and enforcement activities.

The Telemarketing Act addresses widespread concerns about, among other things, the dramatic increase in telemarketing fraud "and other forms of telemarketing deception and abuse," and the difficulties of bringing law enforcement actions against highly mobile and often out-of-state telemarketers.[198] Accordingly, Congress instructed the FTC to promulgate regulations to:

- define and prohibit deceptive telemarketing acts or practices, including "fraudulent charitable solicitations";
- prohibit "a pattern of unsolicited telephone calls" that "the reasonable consumer would consider coercive or abusive of such consumer's right to privacy";
- restrict "the hours of the day and night when unsolicited telephone calls may be made to consumers"; and

197. *Id*. at §§ 7703(b)(1), (c)(3).

198. *Id*. at § 6101.

- require telemarketers to "promptly and clearly disclose" that "the purpose of the call is to sell goods or services" or "to solicit charitable contributions, donations, or gifts or money of any other thing of value" and to make "other disclosures as the [FTC] deems appropriate."[199]

Congress also authorized the FTC, at its discretion, to address conduct by entities that "assist or facilitate" deceptive telemarketing practices, "including credit card laundering."[200] The FTC implemented the act in its Telemarketing Sales Rule (TSR), 16 C.F.R. Part 310.

As regulator and primary enforcer of the Telemarketing Act and the TSR, the FTC maintains telemarketing-related information online, including educational materials, agency guidance and recommendations, and enforcement activities.[201]

The TSR, like the Telemarketing Act, defines, with limited exceptions, telemarketing as "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call."[202] The portion of the TSR prohibiting deceptive conduct, 16 C.F.R. § 310.3, is focused on conduct involving disclosures, billing practices, and misrepresentations that are generally beyond the scope of this Primer.

---

199. *Id*. at § 6102.

200. *Id*.

201. *See Telemarketing*, FED. TRADE COMM'N, www.ftc.gov/tips-advice/business-center/advertising-and-marketing/telemarketing (last visited Jan. 6, 2017) (businesses); *Limiting Unwanted Calls & Emails*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/topics/limiting-unwanted-calls-emails (last visited Jan. 6, 2017) (consumers).

202. 15 U.S.C § 6106; 16 C.F.R. § 310.2.

The portion of the TSR addressing abusive telemarketing practices, however, protects consumer privacy interests by, among other things, prohibiting the following telemarketing conduct:

- "threats, intimidation, or the use of profane or obscene language";
- calls intended to "annoy, abuse, or harass";
- calling persons who have previously indicated that they do not wish to be contacted by telemarketers;
- failing to connect the person who answers a telemarketing call with a live telemarketer within 2 seconds ("abandoned" call);
- use of prerecorded messages, including "robocalls," with very limited exceptions; or
- calling persons before 8:00 a.m. or after 9:00 p.m. at their local time without prior consent.[203]

When promulgating the TSR, the FTC also implemented company-specific and national "do not call" (DNC) lists for individuals who did not wish to be contacted by telemarketers. The FTC maintains, in collaboration with the FCC, a national DNC Registry for consumers who wish to avoid telemarketing calls, www.donotcall.gov. With certain exceptions, the TSR prohibits telemarketers from:

- calling numbers on the company-specific and national DNC list;[204]
- "denying or interfering" with an individual's right to be placed on a company-specific or national DNC list;[205] and

203. 16 C.F.R. § 310.4.

204. *Id.* at § 310.4(b)(iii).

205. *Id*. at § 310.4(b)(ii).

- "sell[ing], rent[ing], leas[ing], purchas[ing], or us[ing]" a company-specific or national DNC list for any purpose other than preventing phone calls to listed numbers.[206]

Shortly after the FTC promulgated the TSR, Congress authorized the FTC's National DNC Registry, ratified the TSR concept of DNC lists, and authorized the FTC to "assess and collect an annual fee . . . to implement and enforce" the National DNC Registry.[207]

The FTC has primary Telemarketing Act and TSR enforcement authority over entities within its FTC Act jurisdiction, and can use all powers and obtain all remedies and relief available to it under the FTC Act.[208] With regard to entities beyond the FTC's jurisdiction, Congress instructed the Securities and Exchange Commission (SEC) to review and, as appropriate, promulgate "rules substantially similar to" the TSR.[209] A later Telemarketing Act amendment provides that a violation of the TSR by an entity subject to the jurisdiction of the Consumer Financial Protection Bureau (CFPB) is deemed to be a violation of the CFPB's rules prohibiting unfair, deceptive, or abusive acts or practices.[210] Finally, Congress directed the FCC to "issue a final [DNC] rule pursuant to the rulemaking proceeding that it began on September 18, 2002, under the Telephone Consumer Protection Act (47 U.S.C. 227 *et seq*.)."[211]

206. *Id.* at § 310.4(b)(iii).

207. 15 U.S.C. §§ 6151–6152.

208. *Id.* at § 6105.

209. *Id.* at § 6102(d).

210. *Id.* at § 6102(c)(2).

211. *Id.* at § 6153.

State attorneys general have enforcement authority with regard to conduct that violates the TSR and affects their state residents, but that authority must be exercised with notification to the FTC, and states cannot bring enforcement actions in federal court if either the FTC or the CFPB have pending enforcement actions.[212] Similarly, private individuals have enforcement authority for conduct that violates the TSR "if the amount in controversy exceeds the sum or value of $50,000 in actual damages for each person adversely affected by such telemarketing," but they must also notify the FTC of any such action and defer to any pending FTC and CFPB enforcement actions.[213]

5. Communications Act of 1934 (47 U.S.C. §§ 151 *et seq*.)

The FCC's authorizing statute, the Communications Act of 1934 (47 U.S.C. §§ 151 *et seq.*), imposes affirmative privacy and data security obligations on telecommunications carriers in the form of the "duty to protect the confidentiality of proprietary information of, and relating to other telecommunication carriers, equipment manufacturers, and customers."[214] The Communications Act defines the personal information that carriers must protect as "Consumer Proprietary Network Information" (CPNI), which consists of:

- information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by

212. *Id*.

213. 15 U.S.C. § 6154.

214. 47 U.S.C. § 222(a). This statutory requirement for entities subject to FCC jurisdiction to protect proprietary information, including the personal information of customers, provides the FCC with a direct statutory hook for its privacy and data security enforcement activities, unlike the FTC's use of its broader and more general "unfair or deceptive acts or practices" authority for privacy and data security activities under Section 5 of the FTC Act.

any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

- information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier,

but not "subscriber list information," which is information about the names, numbers, and addresses of subscribers if that information has or will be published by the carrier.[215] In a Declaratory Ruling, the FCC also determined that the definition of CPNI and the related obligations also applied "to information that telecommunications carriers cause to be stored on their customers' [mobile] devices when carriers or their designees have access to or control over that information."[216]

In February 2015, as part of its hotly contested "Open Internet" initiative, a divided FCC issued an Order that reclassified "broadband Internet access service"—internet services provided by cable, phone, and wireless internet service providers (ISPs)—as telecommunications services and thus made ISPs "common carriers."[217] That Order, which is currently on appeal before the U.S. Court of Appeals for the District of Columbia

215. 47 U.S.C. §§ 222(h)(1), (3).

216. *In re* Implementation of the Telecommc'ns Act of 1996: Telecommc'ns Carriers' Use of Customer Proprietary Network Info. and Other Customer Info., FCC 13-89, CC Docket No. 96-115, Declaratory Ruling (June 27, 2013), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-89A1.pdf.

217. *In re* Protecting and Promoting the Open Internet, Order, FCC 15-24, Report and Order on Remand, Declaratory Ruling, and Order (Feb. 26, 2015), 30 FCC Rcd. 5601 (2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

Circuit,[218] shifts jurisdiction over ISPs from the FTC to the FCC, and imposes on ISPs the statutory privacy and data security protections discussed in this section.

With limited exceptions, carriers can only use or disclose CPNI to the extent necessary to provide telecommunications services; carriers may also disclose CPNI in response to an "affirmative written request by the customer, to any person designated by the customer."[219] The FCC implemented 47 U.S.C. § 222 in its regulations at 47 C.F.R. §§ 64.2001–.2011.

The FCC maintains Communications Act-related information online, including educational materials, agency guidance, and enforcement activities.[220] The FCC regulations provide additional detail about the limited circumstances in which CPNI can be used without customer approval,[221] and place the burden on the carrier to demonstrate that customer approval has been obtained.[222]

Even more important in terms of the FCC's privacy and data security enforcement activities, the FCC regulations impose obligations on carriers with regard to obtaining customer approval, using and securing CPNI, and verifying compliance.

---

218. United States Telecom Ass'n, et al. v. FCC and U.S.A, No. 15-1063 (D.C. Cir. 2015).

219. *See* 47 U.S.C. § 222(c).

220. *See, e.g., Protecting Proprietary Information Including Customer Proprietary Network Information (CPNI)*, FED. COMMC'NS COMM'N, http://transition.fcc.gov/eb/CPNI/; *Enforcement Primer*, FED. COMMC'NS COMM'N, https://www.fcc.gov/encyclopedia/enforcement-primer; *Consumer Guides*, FED. COMMC'NS COMM'N, www.fcc.gov/encyclopedia/consumer-publications-library#Privacy; *Protecting Your Telephone Calling Records*, FED. COMMC'NS COMM'N, www.fcc.gov/guides/protecting-your-telephone-calling-records.

221. 47 C.F.R. § 64.2005.

222. *Id.* at § 64.2007.

When soliciting approval, carriers must first notify customers of "their right to restrict use of, disclosure of, and access to" CPNI, and do so in a way that permits the customer to make an informed decision, including the carrier's identification of what CPNI is, who will receive it and why, and the customer's right to revoke approval.[223] Carriers must maintain safeguards to make sure that CPNI is used appropriately, including training, a supervisory review process, retention of compliance records, and annual certification of the carrier's compliance with the CPNI rules.[224] The FCC also requires carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI," including "properly authenticat[ing]" customers who request disclosure of their CPNI, using methods other than "readily available biographical or account information" to authenticate customers with "lost or forgotten passwords," and "notify[ing] customers immediately" about account changes.[225]

Finally, the regulations impose specific incident notification and response requirements in addition to any requirements that might be imposed by states. The regulations define a breach as a circumstance in which "a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[226] Carriers must notify the USSS and the FBI "as soon as practicable" but "no later than seven (7) business days" after "reasonable determination of a breach," and then wait another 7 days before notifying its customers or the public about the breach, unless earlier notification is necessary to avoid "irreparable harm" or delayed notification is required to avoid

223. *Id.* at § 64.2008.

224. *Id.* at § 64.2009.

225. *Id.* at § 64.2010.

226. *Id.* at § 64.2011(e).

"imped[ing] or compromis[ing] a criminal investigation or national security."[227] The carrier has no discretion in terms of breach notification: it "shall notify its customers" about a breach of their CPNI.[228]

From the FCC's perspective, the failure to reasonably secure customers' personal information violates a carrier's statutory duty under 47 U.S.C. § 222 and constitutes an "unjust and unreasonable practice" that is unlawful under 47 U.S.C. § 201 and subject to civil penalties and injunctive relief. In April 2015, the FCC obtained a $25 million civil penalty from AT&T Services, Inc. to resolve an FCC investigation into AT&T's failure "to properly protect the confidentiality of almost 280,000 customers' proprietary information, including sensitive personal information such as customers' names and at least the last four digits of their Social Security numbers, as well as account-related data known as customer proprietary network information (CPNI), in connection with data breaches at AT&T call centers in Mexico, Columbia, and the Philippines."[229] The breaches involved unauthorized access to and sales of CPNI to third parties, and the consent decree required AT&T to:

> develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into AT&T's business practices to protect consumers against similar data breaches in the future. In particular, AT&T will be required to improve its privacy and data security practices by appointing a senior compliance manager who is

227. *Id.* at §§ 64.2011(a), (b).

228. *Id.* at § 64.2011(c).

229. *In re* AT&T Servs., Inc., DA 15-399, File No.: EB-TCD-14-00016243, Order (April 8, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-15-399A1.pdf.

> privacy certified, conducting a privacy risk assessment, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company's privacy policies and the applicable privacy legal authorities.[230]

Similarly, in September 2014, the FCC obtained a $7,400,000 civil penalty from Verizon to resolve an FCC investigation into Verizon's "failure to generate the required opt-out notices to approximately two million of the company's customers. These failures deprived those customers of information about Verizon's marketing practices and its customers' right to deny Verizon permission to access or use their personal data to market new Verizon services to those customers."[231] The consent decree required Verizon to:

> (i) implement a process to place an opt-out notice on every invoice (whether electronic or paper) to every customer for whom Verizon relies on opt-out consent; (ii) designate a senior corporate manager as a compliance officer; (iii) implement a process for immediately reporting to the Compliance Officer any problems detected with opt-out notices, regardless of size; and (iv) develop and implement a three-year compliance plan.[232]

---

230. *Id*.

231. *In re* Verizon Compliance with the Comm'n's Rules and Regulations Governing Customer Proprietary Network Info., DA 14-1251, File No.: EB-TCD-13-00007027, Adopting Order (Sept. 2, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1251A1.pdf.

232. *Id*.

6. Telephone Consumer Protection Act of 1991 (TCPA; 47 U.S.C. § 227)

As noted above, the TCPA is the FCC equivalent of the FTC's Telemarketing Act, although the FCC's TCPA jurisdiction is broader than the FTC's Telemarketing Act jurisdiction. As also noted above, given the overlapping authority over telemarketing activity and the joint coordination regarding the National DNC Registry, the FTC and the FCC coordinate many of their telemarketing policy and enforcement activities.

In its findings supporting the TCPA, Congress found, among other things, that "[m]ore than 300,000 solicitors call more than 18,000,000 Americans every day" and that "[t]otal United States sales generated through telemarketing amounted to $435,000,000,000 in 1990, a more than four-fold increase since 1984."[233] Accordingly, Congress instructed the FCC to balance "[i]ndividuals' privacy rights, public safety interests, and commercial freedoms of speech and trade . . . in a way that protects the privacy of individuals and permits legitimate telemarketing practices" and to "consider adopting reasonable restrictions on automated or prerecorded calls to businesses as well as to the home, consistent with the constitutional protections of free speech."[234] The FCC implemented the TCPA in its regulations at 47 C.F.R. § 64.1200.

The TCPA and its implementing rule, with limited exceptions for emergencies and prior express consent, prohibit any "person or entity" from:

- using an automatic telephone dialing system or an artificial or prerecorded voice to call emergency telephone lines; rooms in hospitals, health care facilities,

233. 47 U.S.C. § 227 note.

234. *Id*.

and retirement facilities; paging services; or mobile phones;[235]

- making or causing someone else to make a telemarketing call to any of the above facilities using an artificial or prerecorded voice;[236]
- using an artificial or prerecorded voice to make a telemarketing call to a residential line;[237]
- sending unsolicited advertisements to a telephone facsimile machine;[238]
- using an automatic telephone dialing system in a way that ties up two or more telephone lines of a multiline business;[239]
- causing any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value;[240]
- disconnecting an unanswered telemarketing call before at least 15 seconds or 4 rings;[241]
- abandoning more than three percent of all telemarketing calls in a 30-day period by failing to connect a person who answers with a live sales representative within two seconds;[242]

---

235. *Id.* at § 227 (b)(1)(A).

236. *Id.* at § 227 (b)(1)(B).

237. *Id.* at § 227 (b)(1)(C).

238. *Id.* at § 227 (b)(1)(D).

239. *Id.* at § 227 (b)(4).

240. *Id.* at § 227 (e)(1).

241. 47 C.F.R. § 64.1200(a)(6).

242. *Id*. at § 64.1200(a)(7).

- using any technology to dial any telephone number to determine whether the line is a facsimile or voice line;[243]
- initiating any telephone solicitations before 8:00 a.m. or after 9:00 p.m. local time at the called party's location;[244] or
- initiating any telephone solicitations to numbers listed in the National DNC Registry, although the caller can escape liability for the violation if it can demonstrate that the call was in error and that its routine business practices meet the regulatory standard for DNC compliance.[245]

In addition, any person or entity who makes telemarketing calls to residential lines must have procedures in place to create and maintain an entity-specific DNC list in accordance with the standards set forth at 47 C.F.R. § 64.1200(d), including the requirement to provide the called party with the name of the individual caller, the name of the person or entity on whose behalf the call is being made, and the telephone number or address at which the person or entity may be contacted.

In June 2015, the FCC issued a Declaratory Ruling and Order to resolve "21 separate requests for clarification or other action regarding the TCPA or the Commission's rules and orders."[246] Among other things, the Order confirmed that:

243. *Id*. at § 64.1200(a)(8).

244. *Id.* at § 64.1200(b)(c)(1).

245. *Id.* at § 64.1200(b)(c)(2).

246. *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, FCC 15-72, CG Docket No. 02-278, Declaratory Ruling and Order (June 18, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.pdf.

- callers who are not "currently" or "presently" dialing random or sequential phone numbers still must obtain consumer consent for calls using artificial or prerecorded voices ("robocalls");
- internet-to-phone text messages require consumer consent;
- text messages are "calls" subject to the TCPA;
- the Communications Act and FCC rules do not prevent consumers and their carriers and Voice over Internet Protocol (VoIP) providers from using call-blocking technology to avoid unwanted robocalls; and
- certain free, pro-consumer financial- and healthcare-related messages are exempt from the consumer-consent requirement, subject to strict conditions and limitations to protect consumer privacy.[247]

The FCC's enforcement activities under the TCPA primarily involve marketers who send unsolicited junk faxes. For example, in January 2015, the FCC entered an $87,500 forfeiture order against Worldwide Industrial Enterprises, Inc., which "faxed 17 advertisements to consumers who did not request them, did not want them, and had no established business relationship with the Company."[248] However, the TCPA includes a private right of action for individuals, businesses, and states to recover "actual monetary loss or $500 per violation, whichever is greater," and, for willful or knowing violations, three times those amounts.[249]

---

247. *Id*.

248. *In re* Worldwide Indus. Enters., Inc., FCC 15-6, File No. EB-TCD-12-00000254, Forfeiture Order (Jan. 26, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-6A1.pdf.

249. 47 U.S.C. §§ 227(b)(3), (c)(5).

B. State Statutes of General Applicability

The states have enacted statutes aimed at privacy and consumer protection in a particularly wide variety of areas. The summary below touches on a few of the most prominent subjects of legislation, as well as some interesting outliers.

1. Disclosure of PII by Certain Non-Governmental Entities

(a) Consumer Credit Reporting Agencies

Some states have adopted laws analogous to the federal Fair Credit Reporting Act. For example, California's law requires the consumer credit reporting agencies, among other things, to block information that appears on a report as a result of identity theft, to place security alerts or freezes on a report when a consumer requests it, and to provide free copies of credit reports to victims of identity theft.[250] On the other hand, the statute expressly permits the consumer credit agencies to disclose public record information that they lawfully obtained from an open public record.[251]

(b) Financial Institutions

California's Financial Information Privacy Act prohibits financial institutions from selling or otherwise sharing nonpublic PII without the consumers' consent.[252] The law requires consumers to "opt in" to having their information shared with unaffiliated third parties, but requires them to "opt out" of sharing with the institution's affiliates, subject to a few exceptions.

---

250. CAL. CIV. CODE §§ 1785.1–36.

251. *See id.* at § 1785.11.2.

252. CAL. FIN. CODE §§ 4050–4060.

(c) Insurance Companies

California's Insurance Information and Privacy Protection Act governs insurance companies' collection, use, and disclosure of PII in connection with insurance transactions. The law prohibits companies from disclosing the information without written authorization from the individual, unless disclosure is "necessary for conducting business." The law requires the insurance company to give the individual the opportunity to opt out of disclosures made for marketing purposes.[253]

2. Use of Consumer PII for Marketing Purposes

California's "Shine the Light" statute gives consumers the right to know how their personal information is shared by companies (other than financial institutions, which are subject to the state's Financial Information Privacy Act) for marketing purposes.[254] The law "encourages"—but does not require—businesses to allow consumers to opt out of such sharing. California's Right of Publicity Statute prohibits the misappropriation of a person's name, photograph, likeness, and identity for use in paid advertisements without obtaining that person's consent.[255]

3. Data Disposal Requirements

A majority of states have passed laws requiring businesses (and, in some cases, government agencies) to ensure that consumers' PII is undecipherable when the entity disposes of both

253. *Privacy Laws*, OFFICE OF THE ATTORNEY GEN., STATE OF CAL. DEP'T OF JUSTICE, https://oag.ca.gov/privacy/privacy-laws.

254. CAL. CIV. CODE §§ 1798.83–1798.84.

255. *Id.* at § 3344.

hard-copy and digital records.[256] California's law, for example, requires businesses to shred, erase, or modify the PII when disposing of consumer records under their control.[257]

4. Digital Assets After Death

A small number of states now have laws that cover what happens to a person's digital assets—from email and social media accounts to blogs and other websites—upon the person's death.[258] Most of those states provide for a representative of the decedent's estate to obtain access to the online accounts, subject to varying requirements.[259] In Nevada, however, the executor of the person's estate is only granted authority to terminate the accounts.[260]

5. Children's Online Privacy

Some states have enacted specialized statutes designed to protect the privacy of minors online. For example, California's Privacy Rights for California Minors in the Digital World Act allows minors to request and obtain the removal of content about them posted on a website or other online application.[261] The law also prohibits marketing products based on personal information specific to a minor.

---

256. *See Data Disposal Laws*, NAT'L CONFERENCE OF STATE LEGIS. (Jan. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

257. CAL. CIV. CODE §§ 1798.80–81, 1798.84.

258. *Access to Digital Assets of Decedents*, NAT'L CONFERENCE OF STATE LEGIS. (Mar. 31, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/access-to-digital-assets-of-decedents.aspx.

259. *Id*.

260. NEV. REV. STAT. § 143.18.

261. *See* CAL. BUS. & PROF. CODE §§ 22580–22582.

6. Breach Notification and Data Security Laws

The vast majority of states (currently 47) have breach notification laws requiring notification to individuals (and in some cases, state regulators) where there is an unauthorized access or acquisition of the individual's PII.[262] In addition, a minority of states have also enacted state data security laws requiring companies to maintain data security safeguards to protect state residents' personal information from being compromised, which typically require companies to implement and maintain reasonable security measures.[263]

262. *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGIS. (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. The statutes typically define personal information triggering notification obligations as an individual's name in combination with: social security number; credit/debit card number; financial account number; driver's license or state-issued identification number; or, in some cases, medical/health insurance information.

263. *See* Corey M. Dennis & David A. Goldman, *Data Security Laws and the Cybersecurity Debate*, 17 J. OF INTERNET LAW 1 (Aug. 2013), http://www.governo.com/News/News_News725_1.pdf. For a state-by-state breakdown of the requirements of these statutes, *see* Mintz Levin P.C., *State Data Security Breach Notification Laws* (April 16, 2016), https://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf.

SIDE BAR — GENERAL CONSUMER PROTECTION

There are many general consumer-related privacy laws (state and federal) that govern the collection, use, and disclosure of personal information, as well as marketing and communications to individuals. These include Section 5 of the FTC Act, COPPA, CAN-SPAM, the TCPA, and state laws.

Section 5 of the FTC Act prohibits "unfair and deceptive acts or practices in or affecting commerce." This has been interpreted to include privacy-related misrepresentations (e.g., uses of personal information inconsistent with an organization's privacy policy) and security-related deficiencies (e.g., weak information security practices leading to a security breach).

The Telephone Consumer Protection Act (TCPA) and the Children's Online Privacy Protection Act (COPPA) are key federal privacy laws that organizations should be aware of. The TCPA generally requires prior express consent (and, in many cases, written consent) when calling landlines or cell phones (including text messages) for marketing purposes using an automatic telephone dialing system (or artificial/prerecorded voice); consent is also generally required for non-marketing calls/texts to cell phones. COPPA imposes restrictions and consent/notice requirements regarding the collection of personal information from children under the age of 13.

There are numerous state general consumer-related privacy laws. Chief among these laws are the state breach notification laws, which typically require notification to individuals (and, in some cases, regulators) in the event of an unauthorized access or acquisition of personal information.

V. HEALTH

A. HIPAA

1. Overview of HIPAA Privacy and Security Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is one of the most prescriptive and comprehensive data privacy laws in the world. The HIPAA Privacy Rule ("Privacy Rule"), promulgated in 2000, generally prohibits the unauthorized disclosure of protected health information (PHI) by "covered entities," including health care providers, pharmacies, health insurers, HMOs, and health care clearinghouses.[264]

Covered entities must also require by contract any "business associates" (BA) to whom they disclose protected health information (e.g., third party administrators of health plans, medical billing and transcript companies, accounting firms providing services to health care providers, cloud service providers) to appropriately safeguard the information.[265] Such "business associ-

---

264. *See* 45 C.F.R. § 164.500 *et seq.* "Hybrid entities"—i.e., those that conduct both covered and non-covered functions, such as companies with fully self-insured health plans—may designate the covered components of their organizations to segregate covered from non-covered functions. *See id.* at § 164.103.

265. *See id.* at §§ 160.103, 164.502(e). A "business associate" is defined as a "person" who: (1) on behalf of a covered entity, "creates, receives, maintains, or transmits" PHI for a "function or activity" regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, certain patient safety activities, billing, benefit management, practice management, and repricing; or (2) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity where the services provided involve the disclosure of PHI from such covered entity, or from another BA of such covered entity. *See id.* at § 160.103.

ate agreements" (BAAs) must include certain provisions, including a description of the permitted and impermissible uses of PHI, and a requirement that the BA use appropriate safeguards to prevent impermissible uses and disclosures of PHI.[266]

The HIPAA Security Rule ("Security Rule"), promulgated in 2003, requires covered entities to maintain certain safeguards for the protection of electronic health information, which must be documented in written policies and procedures.[267] The Security Rule also imposes other obligations, including training employees and conducting a thorough "risk analysis" to prevent security violations.[268] HIPAA generally preempts contrary state laws, with few exceptions, such as where the requirements of the state law are more stringent than those under HIPAA.[269]

2. Protected Health Information and the De-Identification Standard

PHI under HIPAA is broadly defined to include "individually identifiable information," including demographic information: (1) that is "created or received" by a HIPAA Covered Entity; and (2) relates to the past, present, or future physical or mental health or condition of an individual, or the provision or payment for such health care; and (3) that identifies the individual, or there is a reasonable basis to believe the information can be used to identify the individual.[270] However, the Privacy Rule does not restrict the use or disclosure of "de-identified health

266. *See id.* at § 164.504.

267. *See id.* at §§ 164.302 *et seq*.

268. *See id.* at § 164.308(a).

269. *See id.* at § 160.203.

270. *See id.* at § 160.103.

information," which neither identifies, nor provides a reasonable basis to identify, an individual.[271]

There are two methods for de-identification under HIPAA:

1) *The Safe Harbor Method*—removal of all 18 HIPAA identifiers, including: (a) names/initials; (b) all dates directly related to the individual (e.g., DOB, admission date); (c) medical record numbers; (d) ages over 89 (must be grouped into 90+); (d) telephone numbers and email addresses; or (e) any unique identifying number (e.g., hospital number), characteristic (e.g., "CEO"), or code (if derived from PHI)
2) *The Expert Determination Method*—based upon a statistical analysis by a recognized expert, to ensure there is a "very small" risk of re-identification[272]

3. Uses and Disclosures of PHI

The basic principle of the Privacy Rule is that a covered entity may not use or disclose PHI, except either (1) as the Privacy Rule permits or requires, or (2) as the individual or the individual's personal representative permits pursuant to a written authorization. Under the Privacy Rule, a valid authorization must contain:

1) a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
2) the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

271. *See id.* at §§ 164.502(d), 164.514.

272. *See id.* at § 164.514.

3) the name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;
4) a description of each purpose of the requested use or disclosure;
5) an expiration date/event ("none" or similar language is sufficient if the disclosure is for research);
6) signature of the individual (or personal representative) and date; and
7) statements regarding: (a) the individual's right to revoke the authorization (including to revoke the authorization and exceptions to the right to revoke); (b) the potential for information disclosed to be subject to re-disclosure and no longer subject to the Privacy Rule; and (c) the ability or inability to condition treatment, payment, enrollment, or eligibility for benefits (i.e., stating that the covered entity may not do so, or the consequences if the individual refuses to sign when the covered entity may do so).

The authorization must also be written in plain language, and a copy must be provided to the individual. The authorization requirements under HIPAA differ from the elements of informed consent under the FDA regulations governing clinical trials, which include additional requirements (e.g., a statement that the study involves research, and an explanation of the research purpose, procedures to be followed, risks and benefits of the study, and the extent confidentiality of records will be maintained).

A covered entity is required to disclose PHI in only two situations: (1) to individuals or their representatives when they request access to PHI or an accounting of disclosures of PHI; and (2) to HHS when it is undertaking a compliance investigation, review, or enforcement action.

The "minimum necessary" requirement is a key principle of the Privacy Rule. Under this principle, a covered entity must implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. This includes implementing policies and procedures that restrict access to PHI based on specific roles of members of their workforce (i.e., access should be limited only to those who need access to fulfill their job duties), as well as policies and procedures limiting PHI disclosed for routine/recurring disclosures.

(a) Permitted Uses and Disclosures

The Privacy Rule sets forth a number of exceptions to the general rule requiring an authorization for disclosures of PHI, which are described below. A covered entity is permitted to use and disclose PHI, without an individual's authorization:

1) to the individual;
2) for treatment, payment, or health care operations;
3) for certain uses and disclosures where the individual has an opportunity to agree or object (e.g., for healthcare facility directors or to an individual's family or friends);
4) for incidental uses or disclosures that are otherwise permitted by the Privacy Rule (e.g., a hospital visitor overhears a provider's confidential conversation with another provider or patient), provided that the covered entity has complied with the "minimum necessary rule";
5) for public health activities;
6) in certain circumstances (e.g., victims of abuse, neglect, or domestic violence);

7) for health oversight activities (e.g., audits and investigations necessary for oversight of healthcare systems and government benefit programs);
8) in judicial and administrative proceedings (if ordered by a court or administrative tribunal);
9) for law enforcement purposes;
10) to decedents (e.g., to funeral directors, coroners, and medical examiners in certain circumstances);
11) to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue;
12) where necessary to prevent a serious threat to health or safety;
13) for essential government functions (e.g., assuring proper execution of military mission, conducting authorized intelligence and national security activities, protecting the health and safety of inmates or employees of correctional institutions, and determining eligibility for certain government benefit programs); and
14) as authorized by, and to comply with, workers' compensation laws and similar programs.

(b) Research

The rules regarding disclosure of PHI for research purposes under HIPAA seek to balance the rights of privacy and confidentiality in research subjects' personal information with the public policy in favor of public health and developing life-saving treatments. Clinical research is not only vital to achieving these goals, but is also required for the development of pharmaceutical drugs and devices.

Research under the Privacy Rule is defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." In general, the Privacy Rule requires that a covered

entity obtain an individual's authorization before using and disclosing PHI for research purposes. However, there are several exceptions to this rule:

1) Institutional Review Board (IRB) waiver—An IRB or Privacy Board may grant a waiver of authorization where research cannot practicably be conducted without the disclosure of PHI and there is minimal privacy risk.
2) Preparatory to Research—PHI may be disclosed if the researcher represents that the use of PHI is necessary (and solely) for purposes preparatory to research (e.g., research study/protocol design or feasibility), and that the PHI will not be "removed" from the covered entity.
3) Limited Data Set—A researcher may access a "limited data set," which includes indirect identifiers (e.g., DOB, dates of treatment, city), but excludes direct identifiers (e.g., name, address, phone number) where the researcher and covered entity execute a "data use agreement."
4) Research on Decedents—PHI of decedents may be disclosed where the researcher represents (written or orally) that the use is necessary (and solely) for the research and provides documentation of the subject's death.
5) Limited Data Set with a Data Use Agreement—A covered entity may disclose a limited data set to the researcher for research, public health, or health care operations pursuant to a data use agreement.

The Privacy Rule generally requires an individual's written authorization before a use or disclosure of protected health information can be made for "marketing," which is defined as

making "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." However, there are several exceptions to this rule:

1) Communications made to describe a health-related product or service that is provided by a covered entity or its plan of benefits (e.g., the entities participating in a healthcare provider network, enhancements to a health plan)
2) Communications made for the treatment of the individual (e.g., pharmacy prescription refill reminders or primary care physician referrals to a specialist)
3) Communications made for case management or care coordination (e.g., recommending alternative treatments or healthcare providers)

In addition, face-to-face-marketing communications or communications regarding a promotional gift of nominal value from the covered entity do not require an authorization.

4. Notice of Privacy Practices

Covered health plans and healthcare providers must generally provide a notice of privacy practices (NPP) to all individuals of the use or disclosure of their PHI, which must describe the ways in which the PHI may be used and disclosed, state the covered entity's duties to protect privacy and abide by the NPP, describe the individuals' rights (e.g., to the covered entity or to HHS), and include a point of contact for further information and for making complaints.[273]

273. *See id.* at § 164.520.

The NPP must be made available to any individual who requests it and prominently posted on any website providing information about its customer services or benefits. Health plans must also provide the notice to all new enrollees at the time of enrollment and provide a revised notice to individuals within 60 days of a material revision, while healthcare providers must generally provide the notice to the individual on the first date of service and obtain a written acknowledgement from patients of receipt of the NPP.[274]

5. Rights of Access, Amendment, and Disclosure Accounting

Individuals generally have a right to access and obtain a copy of their PHI in a covered entity's designated record set.[275] Excluded from the right to access are psychotherapy notes and information compiled for legal proceedings.[276] Individuals also have a right to have their PHI amended if it is inaccurate or incomplete.[277]

In addition, individuals have a right to an accounting of the disclosure of their PHI to a covered entity's business associates made in the preceding six years. However, no accounting is required:

a) for treatment, payment, or health care operations;

---

274. *See id.* at § 164.520.

275. *See id.* at § 164.524(a). "Designated record set" is defined as the group of records maintained by the covered entity that is: (1) medical records and billing records about the individuals; (2) used (in whole or in part) to make decisions about individuals; or (3) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by a health plan. *See id.* at § 164.520.

276. *See id.* at § 164.524(a).

277. *See id.* at § 164.526.

b) to the individual or the individual's personal representative;
c) for notification to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories;
d) pursuant to an authorization;
e) of a limited data set;
f) for national security or intelligence purposes;
g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or
h) incident to otherwise permitted or required uses or disclosures.[278]

6. Administrative Requirements

The Privacy Rule sets forth a number of administrative requirements, including:

1) developing and implementing written policies and procedures in compliance with the requirements of the Privacy Rule;
2) designating a "privacy official" (Privacy Officer) who is responsible for developing and implementing policies and procedures, and a contact person/office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices;
3) applying sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule;
4) mitigating any harmful effect that may be caused by an improper use or disclosure of PHI;

278. *See id.* at § 164.528.

5) maintaining reasonable and appropriate administrative, technical, and physical safeguards to prevent improper uses and disclosures of PHI (e.g., shredding documents with PHI before discarding them);
6) maintaining procedures for individuals to complain about its compliance with policies and procedures or the Privacy Rule;
7) banning retaliation against any person who exercises rights provided by the Privacy Rule, and prohibiting a waiver of an individual's rights under the Privacy Rule as a condition of obtaining treatment, payment, and enrollment or benefits eligibility;
8) maintaining, until the later of six years after its creation or last effective date, its privacy policies and procedures, NPP, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.[279]

The Security Rule also sets forth numerous administrative, technical, and physical safeguards with which covered entities and business associates must comply.[280] However, those requirements are beyond the scope of this primer, which focuses on privacy, rather than security laws.

279. *See id.* at § 164.530. Fully-insured group health plans that do not create or receive PHI, with the exception of enrollment data and "summary health information" (as defined under 45 C.F.R. §164.504(a)) are only subject to the following administrative requirements: (1) ban on retaliatory acts and waiver of individual rights; and (2) health plan documentation requirements if plan documents are amended to allow disclosure of PHI by an insurance company to the plan sponsor. *See id.* at § 164.530(k).

280. *See id.* at § 164.302.

7. Breach Notification Under the Health Information Technology for Economic and Clinical Health (HITECH) Act

In January 2013, HHS issued the final omnibus HIPAA/HITECH rule, which makes important changes to the privacy and security requirements under HIPAA and the HITECH Act. Some of the more significant changes include:

1) HIPAA violation liability is extended to business associates to whom protected health information is disclosed;
2) "business associate" is now more broadly defined to include subcontractors of business associates (thus, business associates themselves must obtain business associate agreements from their subcontractors);
3) the threshold for reporting breaches has been reduced such that more breaches may be reported—an impermissible use/disclosure is now presumed to be a breach unless it is shown, based upon a risk assessment, that there is a low probability of PHI being compromised; and
4) non-compliance penalties are increased based on the level of negligence, with a maximum penalty of $1.5 million per violation (for cases involving willful negligence).[281]

The HITECH Act's breach notification regulations require HIPAA covered entities to report data breaches affecting 500 or more individuals to the affected individuals, to HHS, and to "prominent media outlets serving a State or jurisdiction." Breaches affecting fewer than 500 individuals must be reported

281. *See id.* at §§ 164.400 *et seq.*; 42 U.S.C. §§ 17931 *et seq.*; 42 U.S.C. § 1320d-5.

to HHS annually. In addition, business associates must notify covered entities of any breaches.[282]

8. Audits

In 2011, HHS began an audit program to evaluate organizations' HIPAA compliance with the HIPAA Privacy, Security, and Breach Notification Rules. The results of Phase 1 of the audits revealed that the vast majority of covered entities failed to comply with mandatory HIPAA requirements, and that the most common cause of non-compliance was a fundamental lack of awareness of those requirements.[283]

HHS Office for Civil Rights (OCR) Senior Adviser Linda Sanches explained that "security was overwhelmingly an area of concern," noting that most of the healthcare providers had not done a complete and accurate risk assessment.[284] The negative findings were forwarded to OCR investigators for consideration. The OCR has now begun Phase 2 of the audits, which focuses on both covered entities and business associates.

9. Enforcement

Since the HITECH Act became effective, HHS has substantially increased its enforcement efforts relating to HIPAA. In 2013, former OCR Director Leon Rodriguez noted that the OCR would "vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held

---

282. *See id.* at §§ 164.404 *et seq*.

283. *See* Linda Sanches, *HIPAA Privacy, Security and Breach Notification Audits: Program Overview & Initial Analysis*, HCCA 2013 COMPLIANCE INSTITUTE (Apr. 23, 2013), http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print1.pdf.

284. Joe Carlson, *Audits find organizations unaware of new data, privacy rules*, MODERN HEALTHCARE (April 23, 2013), http://www.modernhealthcare.com/article/20130423/NEWS/304239958.

by a health plan, a health care provider, or one of their business associates."[285] And in February 2015, the OCR noted that it will continue to "aggressively enforce" these rules.[286] Examples of recent investigations and fines include the following:

- In March 2016, the Feinstein Institute for Medical Research agreed to pay $3.9 million to settle potential HIPAA violations following an incident in which an unencrypted laptop containing PHI of 13,000 patients and research participants was stolen from an employee's car; the OCR found that Feinstein's HIPAA policies, procedures, and processes were non-compliant and insufficient to address privacy and security risks relating to that information.[287]
- In March 2016, North Memorial Health Care of Minnesota settled potential HIPAA violations for $1.55 million based on allegations that it failed to enter into a BAA with a major contractor and failed to conduct an organization-wide risk analysis and management plan as required by HIPAA.[288]

---

285. *See New Rule Protects Patient Privacy, Secures Health Information*, DEP'T OF HEALTH & HUMAN SERVS. (Jan. 17, 2013), http://www.hhs.gov/news/press/2013pres/01/20130117b.html.

286. *See* OFFICE FOR CIV. RIGHTS, DEP'T OF HEALTH & HUMAN SERVS., OCR FISCAL YEAR 2016 CONGRESSIONAL JUSTIFICATION (Feb. 2, 2015), http://www.hhs.gov/sites/default/files/budget/office-of-civil-rights-budget-justification-2016.pdf.

287. *See Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement*, DEP'T OF HEALTH & HUMAN SERVS. (Mar. 17, 2016), http://www.hhs.gov/about/news/2016/03/17/improper-disclosure-research-participants-protected-health-information-results-in-hipaa-settlement.html.

288. *See $1.55 million settlement underscores the importance of executing HIPAA business associate agreements*, DEP'T OF HEALTH & HUMAN SERVS. (Mar. 16, 2016), http://www.hhs.gov/about/news/2016/03/16/155-million-settlement-

- In November 2015, Triple-S Management Corporation (an insurance company, formerly known as American Health Medicare Inc.) agreed to a $3.5 million HIPAA settlement. Following multiple breach notifications involving PHI, the OCR found widespread non-compliance with the Privacy and Security Rules, including failure to develop appropriate policies and procedures, implement necessary technical safeguards, conduct a risk analysis, and implement required training.[289]

Other recent breaches include the following:

- In August 2015, an oncology practice agreed to pay $750,000 following a breach involving the theft of unencrypted backup media where the OCR's investigation revealed widespread non-compliance with the Security Rule, including failure to conduct a risk analysis or to have a policy in place regarding removal of electronic media containing PHI.[290]
- In February 2015, health insurer Anthem suffered a breach involving 80 million current and former members, the largest ever disclosed by a healthcare company, which affected customers of all products lines, including Anthem Blue Cross, and Anthem Blue Cross and Blue Shield. The breach prompted a multi-

---

underscores-importance-executing-hipaa-business-associate-agreements.html.

289. *See Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement*, DEP'T OF HEALTH & HUMAN SERVS. (Nov. 30, 2015), http://www.hhs.gov/about/news/2015/11/30/triple-s-management-corporation-settles-hhs-charges.html#.

290. *See $750,000 HIPAA settlement emphasizes the importance of risk analysis and device and media control policies*, DEP'T OF HEALTH & HUMAN SERVS. (Sept. 2, 2015), http://www.hhs.gov/news/press/2015pres/09/20150902a.html.

state insurance regulator investigation and more than 50 putative class action lawsuits.[291]

- In May 2014, New York and Presbyterian Hospital and Columbia University agreed to pay $4.8 million to settle potential HIPAA violations following a breach resulting in the disclosure of the electronic personal health information of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.[292]

In addition, it should be noted that although most private lawsuits based upon data breaches have been dismissed in the past, recent decisions ruling in favor of plaintiffs—including a Connecticut Supreme Court decision that could give rise to negligence liability based upon HIPAA violations[293]—may lead to an increase in litigation and more difficulty for defendants facing such cases.[294]

---

291. *See* Joseph Conn, *Legal liabilities in recent data breach extend far beyond Anthem*, MODERN HEALTHCARE (Feb. 23, 2015), http://www.modernhealthcare.com/article/20150223/NEWS/302239977/legal-liabilities-in-recent-data-breach-extend-far-beyond-anthem; Anna Wilde Mathews, *Insurance Regulators to Investigate Recent Data Breach at Anthem*, WALL ST. J. (Feb. 6, 2015), http://www.wsj.com/articles/insurance-regulators-to-investigate-recent-data-breach-at-anthem-1423268574.

292. *See Data breach results in $4.8 million HIPAA settlements*, DEP'T OF HEALTH & HUMAN SERVS. (May 7, 2014), http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

293. *See* Byrne v. Avery Ctr. for Obstetrics and Gynecology, P.C., 314 Conn. 433, 436, 102 A.3d 32, 36 (Conn. 2014) (holding "HIPAA may inform the applicable standard of care" in negligence case against physician involving improper disclosure of records).

294. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694–96 (7th Cir. 2015) (holding plaintiff's lost time and money resolving fraudulent charges and protecting themselves against future identity theft by purchasing credit monetary conferred adequate Article III standing); Resnick v.

B. State Laws on Privacy of Health Information

While a review of all 50 states' health privacy laws is beyond the scope of this Primer, the following discussion highlights a handful of state statutes that build on the federal framework, whether by permitting private enforcement or by broadening the scope of statutory protections.

1. Alaska's Genetic Privacy Act

Alaska's Genetic Privacy Act ("Alaska law"), Alaska Stat. §§ 18.13.010–100, treats genetic information, including DNA samples, as the private property of the individual. As such, the statute provides that DNA samples cannot be collected, analyzed, or disclosed without an individual's informed consent. The statute was enacted to "curtain exploitation of [citizens'] valuable genetic information" and to afford Alaskans "the right to keep their genetic information private."[295]

(a) Specific Provisions

The Alaska law makes it illegal for anyone to "collect a DNA sample from a person, perform a DNA analysis on a sample, retain a DNA sample or the results of a DNA analysis, or disclose the results of a DNA analysis" without first obtaining that person's informed consent.[296] The Alaska law specifies that both the

---

AvMed, Inc., 693 F.3d 1317, 1330 (11th Cir. 2012) (holding plaintiffs' allegations of injury and causation were sufficient to withstand a motion to dismiss where they suffered identity theft due to a data breach affecting their health insurer; case later settled for $3M); *cf.* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. Aug. 24, 2015) (upholding FTC's authority to regulate and enforce in the area of data security following data security breach affecting Wyndham hotels' customers).

295. SB 217, 2004 Alaska Legis. Comm. Minutes 1539.

296. ALASKA STAT. § 18.13.010(a)(1).

DNA sample and the results of any analysis of the sample are the exclusive property of the "person sampled or analyzed."[297]

The Alaska law defines "DNA analysis" to mean "DNA or genetic typing and testing to determine the presence or absence of genetic characteristics in an individual," and further defines "genetic characteristics" to include "a gene, chromosome, or alteration of a gene or chromosome that may be tested to determine the risk of a disease, disorder, trait, propensity, or syndrome, or to identify an individual or a blood relative."[298]

The Alaska law contains a number of exclusions that narrow its otherwise sweeping scope. The statute expressly defines "DNA analysis" to exclude "routine physical measurement, a test for drugs, alcohol, cholesterol, or [HIV], a chemical, blood or urine analysis, or *any other diagnostic test that is widely accepted and in use in clinical practice*."[299] Thus, the law arguably has no application to routine tests a person could obtain at most doctors' offices. The statute also exempts five categories of activities, specifying that its prohibitions do not apply to genetic testing for purposes of:

- criminal identifications pursuant to any jurisdiction's DNA registration system;
- law enforcement, including the identification of both victims and perpetrators;
- paternity testing;
- screening of newborns as required by law; or
- emergency medical treatment.[300]

297. *Id*. at § 18.13.010(a)(2).

298. *Id*. at §§ 18.13.100(2)–(3).

299. *Id*. at § 18.13.100(2) (emphasis added).

300. *Id*. at § 18.13.10(b).

The Alaska law makes clear that a "general authorization for the release of medical records or medical information" does not count as the necessary informed consent to release the genetic information the law protects.[301] The law also expressly permits a person, at any time, to revoke or amend their informed consent to analysis or disclosure of genetic information.[302]

(b) Enforcement

In Alaska, unlawful DNA collection, analysis, retention or disclosure is a class A misdemeanor punishable by up to one year in jail and a fine of up to $10,000.[303] The statute specifies that a person is criminally liable only if he or she acts "knowingly," which need not include any intention to violate the law. Rather, under Alaska law, a person acts "knowingly" if he or she is aware that the circumstance making the conduct unlawful exists, or if he or she is aware of a substantial probability that the circumstance exists.[304]

The Alaska law also creates a private right of action for anyone whose genetic information is collected, analyzed, retained, or disclosed in violation of the statute. The statute provides for statutory damages of $5,000, in addition to any actual damages suffered by the person whose genetic information was misused. If the violator profited from the violation, the statutory damages increase to $100,000.

---

301. The law contemplates that the Alaska Department of Health and Social Services may adopt a uniform informed and written consent form, the use of which would immunize a person from civil or criminal liability under the statute. ALASKA STAT. § 18.13.10(c). However, as of the date of this publication, no such regulation has been adopted.

302. *Id*. at § 18.13.10(c).

303. *Id*. at § 18.13.030(c); *see also id*. at §§ 12.55.035, 12.55.135.

304. *Id*. at § 11.81.900(a)(2).

Although the statute has been on the books for more than a decade, it appears to have been invoked only rarely. In 2014, a plaintiff named Michael Cole filed a putative class action lawsuit in Alaska against Gene by Gene, Ltd., a Texas company doing business as "Family Tree DNA."[305] According to the complaint, Family Tree DNA is a commercial genetic testing company that sells DNA tests to consumers for the purpose of helping them to research and identify their ancestry.[306] Cole alleges that Family Tree ships DNA collection kits to consumers, who collect cotton swab samples and return them to the company for analysis. When the analysis is complete, Family Tree invites the customer to sign in to the Family Tree database to search for "matches" based on the customer's DNA sequence, and, if a match is found, Family Tree encourages the customer to "join" a "project," or a forum for individuals conducting ancestral research.[307] According to Cole, even though Family Tree never seeks or obtains the customer's consent to disclose the results of his or her DNA analysis with third persons, "when customers join certain 'projects,' Family Tree automatically publishes the full results of their DNA tests to its publicly available websites."[308] Cole alleges that his DNA test results were made publicly available on the Internet and that his full name, email address, and unique DNA kit number were also disclosed to a

305. Cole v. Gene by Gene, Ltd., Case No. 14-cv-00004, Dkt. No. 1 (D. Alaska May 13, 2014). One of the lawyers representing Cole, Jay Edelson, is the immediate past Co-Chair of Working Group 11 and a contributor to this publication.

306. *Id.* at ¶ 1.

307. *Id.* at ¶¶ 1–2, 20–23.

308. *Id.* at ¶¶ 24–26, 32.

separate ancestry research company, RootsWeb.[309] On his own behalf and on behalf of a class of similarly situated individuals, Cole seeks injunctive relief, actual and statutory damages, and an award of attorneys' fees. The complaint alleges that the total damages exceed $5,000,000.[310]

As of the date of this publication, the *Cole* case is still in the discovery phase. Because Family Tree did not move to dismiss the complaint, the court's first opportunity to evaluate the viability of the claim will be when Cole moves for class certification.

2. California Confidentiality of Medical Information Act

The California Confidentiality of Medical Information Act (CMIA), California Civil Code § 56 *et seq.*, includes extensive provisions governing how and when medical information may be disclosed by health care providers and certain other entities in California.

(a) Specific Provisions

The CMIA broadly defines "Medical Information" to include any "individually identifiable information" about "a patient's medical history, mental or physical condition, or treatment," in any format that is possessed by or "derived from" certain

309. *Id.* at ¶ 32. In its Answer, Family Tree DNA states that the "projects" are administered by non-employee volunteers who are "genealogy enthusiasts." *See Cole*, Case No. 14-cv-00004, Dkt. No. 20 at 6, 8. Family Tree DNA asserts that such a volunteer was responsible for posting Cole's information on RootsWeb. *Id.* at 8. Family Tree DNA also states that Cole signed a release, which directed him to the company's privacy policy, which notified him that his information would be made available to the "volunteer project administrator." *Id*.

310. *Cole*, Case No. 14-cv-00004, Dkt. No. 1 at ¶¶ 7, 34, 49.

health-related entities.[311] "Individually identifiable" is defined equally broadly, to mean that the information includes "any element of personal identifying information" that would make it possible to identify the individual. In addition to PII like name, address, electronic mail address, telephone number, and social security number, the statute expressly includes "other information that, alone *or in combination with other publicly available information*, reveals the individual's identity."[312]

The CMIA prohibits health care providers from disclosing their patients' medical information without prior authorization, except as provided by statute.[313] The latter caveat is fairly broad, however. The statute expressly *requires* disclosure in a number of situations, including when compelled by a court order, subpoena, or search warrant, or pursuant to a patient's request for inspection pursuant to California's Patient Access to Health Records statute.[314] The CMIA also permits disclosure in a wide variety of circumstances, including, among other things:

- to other health care professionals for purposes of diagnosis or treatment of the patient, including via radio transmissions in emergency situations;
- to an insurer, employee benefit plan, governmental authority, or other entity responsible for paying for health care services rendered to the patient, as needed to establish responsibility for payment;

311. CAL. CIV. CODE § 56.05(j). The statute applies to information possessed by or derived from "a provider of health care, health care service plan, pharmaceutical company, or contractor."

312. *Id*. (emphasis added).

313. *Id*. at §§ 56.10(a), (d), (e).

314. *Id*. at §§ 56.10(b)(1)–(9).

- to a person or entity that provides billing, claims management, medical data processing, or other administrative services for health care providers;
- to agents of professional societies, professional standards review organizations and the like, if they are reviewing the competence or qualifications of the health care provider;
- to a private or public body responsible for licensing or accrediting the health care provider or service plan;
- to public agencies, clinical investigators, and accredited educational institutions for bona fide research purposes;
- to an organ procurement organization or tissue bank for the purpose of aiding in the transplantation of tissue into the body of another person;
- to a third party "for purposes of encoding, encrypting, or otherwise anonymizing data"; and
- to a local health department for the purpose of preventing or controlling disease, injury, or disability.[315]

The CMIA also expressly permits a psychotherapist to disclose information if he or she believes, in good faith, that "disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a reasonably foreseeable victim or victims, and the disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat."[316] The CMIA specifies that the recipient of a permitted disclosure may not further disclose the information in violation of the statute.[317] The CMIA also requires health care

315. *Id*. at §§ 56.10(c)(1)–(22).

316. *Id*. at § 56.10(c)(19).

317. *Id*. at § 56.13.

providers and other covered entities that create, maintain, preserve, store, abandon, destroy, or dispose of medical records to do so in a manner that preserves the confidentiality of the information contained within those records.[318]

The CMIA spells out exactly what is necessary for an authorization of disclosure to be valid, including that the signature executing the authorization must serve no other purpose than to execute the authorization, and that the authorization must include an expiration date.[319] The CMIA also gives patients the right to cancel or revoke their authorization at any time, so long as the provider actually receives the written revocation.[320]

(b) Enforcement

A violation of the CMIA constitutes a misdemeanor if it causes economic loss or personal injury to a patient.[321] In California, misdemeanors are punishable by probation, jail time, fines, community service, or a combination. The CMIA also creates a private right of action against any person or entity that violates the statute by negligently releasing the plaintiff's confidential information or records.[322] If the plaintiff suffered economic loss or personal injury, he or she can recover actual damages, if any, and punitive damages up to $3,000; attorneys' fees up to $1,000; and the costs of litigation.[323] The CMIA also provides for statutory damages of $1,000, which do not require

318. *Id*. at § 56.101(a).

319. *Id*. at § 56.11.

320. *Id*. at § 56.15.

321. *Id*. at § 56.36(a).

322. *Id*. at § 56.36(b).

323. *Id*. at § 56.35; *see also id*. at §§ 56.36(b), (e).

proof that the plaintiff suffered actual damages[324] unless the defendant establishes the affirmative defense added to the act effective January 1, 2013.[325]

The affirmative defense applies if a covered entity or business associate released confidential information solely to another covered entity or business associate, and all of the following are true:

- the defendant complied with any obligation to notify affected individuals;
- the disclosure was not in connection with medical identity theft;
- the defendant took appropriate preventive actions to protect the information and records under both HIPAA and applicable state laws, including, among other things, using encryption;
- the defendant took appropriate corrective action after the disclosure, including measures to prevent similar occurrences in the future; and
- the recipient did not use or release the information or records and returned or destroyed the material promptly.[326]

In general, a defendant may only take advantage of the affirmative defense once, unless the court determines that the justification for the defense is "compelling" and applying it would promote reasonable conduct consistent with the CMIA.[327] The CMIA also explicitly instructs courts to consider the equities of

---

324. *Id*. at § 56.36(b)(1).

325. *Id*. at § 56.36(e).

326. *Id*. at §§ 56.36(e)(2)(A)–(H).

327. *Id*. at § 56.36(e)(2)(I).

the situation when deciding whether to apply the affirmative defense.[328]

The CMIA also provides for administrative fines and civil penalties in varying amounts for certain violations,[329] which may be imposed by the State Department of Public Health, a licensing agency, a certifying board, or a court.[330] Only specified public officials, including the state attorney general, any district attorney, and certain city attorneys, may bring a civil action, in the name of the people of the State of California, seeking civil penalties.[331]

A person who negligently discloses information in violation of the statute faces a fine or penalty of up to $2,500 per violation, irrespective of whether the violation caused any actual damages.[332] Anyone other than a licensed health care professional who knowingly or willfully obtains, discloses, or uses medical information in violation of the statute is liable for up to $25,000 per violation.[333] If the violation was for the purpose of financial gain, the fine or penalty may be up to $250,000 per violation, as well as disgorgement of the ill-gotten gains.[334]

A licensed health care professional who knowingly and willfully obtains, discloses, or uses medical information in violation of the law is subject to fines or penalties of up to $2,500 for the first violation, $10,000 for the second violation, and $25,000 for

328. *Id*. at § 56.36(e)(3).

329. *Id*. at §§ 56.36(c)–(d).

330. *Id*. at § 56.36(d).

331. *Id*. at § 56.36(f).

332. *Id*. at § 56.36(c).

333. *Id*.

334. *Id*. at § 56.36(c)(3)(A). The penalty similarly rises to $250,000 per violation if the person was not permitted under the statute to receive medical information.

a third or subsequent violation. If the violation was for the purpose of financial gain, the fines or penalties grow to $5,000 for a first violation, $25,000 for the second one, and $250,000 for a third or subsequent violation, as well as disgorgement.[335]

A handful of recent cases applying and interpreting the CMIA have emphasized the statute's focus on preserving the confidentiality of information. For example, in *Regents of the Univ. of Cal. v. Super. Ct.*,[336] the California Court of Appeals concluded that negligently maintaining or storing medical information, by itself, did not give rise to a cause of action under the CMIA. The court held that plaintiffs must plead that their information was in fact improperly viewed or accessed by an unauthorized person, and not just lost, in order to support a claim under the CMIA.

Similarly, *Sutter Health v. Super. Ct.*,[337] arose from the theft of a health care provider's computer, which contained the medical records of some four million patients. The plaintiffs brought the case on behalf of themselves and a putative class of all of the affected individuals, and sought an award of as much as $4 billion. After the trial court refused to dismiss the complaint, the defendant appealed. A unanimous panel of the court of appeals held that the plaintiffs had failed to state a claim under the CMIA because they did not allege that any unauthorized person actually viewed the stolen medical information. In so ruling, the court reasoned that the focus of the CMIA is on "preserving the confidentiality of the medical information, not necessarily preventing others from gaining possession of the paper-based or electronic information itself." Therefore, the court held, a breach of confidentiality is a necessary element of a claim under the

335. *Id*. at § 56.36(c)(3)(B).

336. 220 Cal. App. 4th 549 (2013).

337. Case No. C072591 (Cal. Ct. App. July 21, 2014).

CMIA. Since no breach of confidentiality takes place "until an unauthorized person views the medical information," the failure to plead such unauthorized access was fatal to the plaintiffs' claim.

3. Texas Medical Records Privacy Act

The Texas Medical Records Privacy Act ("Texas law"), Tex. Health & Safety Code Ann. § 181.001 *et seq.*, which became effective on September 1, 2012, builds on HIPAA to provide even more comprehensive protection of medical information.

(a) Specific Requirements

The Texas law broadens HIPAA's definition of "covered entity" to include *any* person who "comes into possession" of PHI.[338] The statute expressly includes anyone who assembles, collects, analyzes, uses, evaluates, obtains, stores, or transmits PHI, whether that person is a health care provider, business associate, governmental unit, or other entity.[339] The statute also makes explicit that employees, agents, or contractors of anyone falling within the definition of a "covered entity" are also "covered."[340] However, the Texas law exempts employee benefit plans, workers' compensation programs, and the American Red Cross, among other entities, from the statute's reach.[341]

Among other affirmative requirements, the Texas law mandates training for a covered entity's employees as to state and

338. TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2)(B).

339. *Id.* at § 181.001(b)(2).

340. *Id.* at § 181.001(b)(2)(D).

341. *See generally id*. at §§ 181.052–059. The act exempts insurers and employers from some provisions, but not from the statute's prohibitions on re-identification; disclosure or use of PHI for marketing purposes without prior authorization; and sale of PHI. *Id*. at § 181.051. Insurers and employers are also subject to the notice requirement in § 181.154 of the Act.

federal law concerning PHI, as necessary and appropriate for the employee to perform his or her job.[342] Such training must be provided within 90 days of the employee's date of hire. The statute further requires employees to stay current: if the employee's job duties are affected by a material change in the law regarding PHI, the employee must have additional training within one year after the material change in law takes effect. Employers must also obtain a signed statement verifying the employee's completion of the training and retain it for six years.

The Texas law also provides for consumers' right to access their own medical records upon request. With limited exceptions, if a health care provider is using an electronic system capable of fulfilling the request, the provider must provide requested records to the patient, in electronic form, within 15 days of receiving the request.[343]

The statute charges the state attorney general with the duty of monitoring compliance with the law and reporting annually to the legislature about consumer complaints under the Texas law. The Texas law expressly prohibits the re-identification (or attempted re-identification), without prior consent, of an individual who is the subject of any PHI.[344]

In general, before PHI may be disclosed or used for marketing purposes, a covered entity must first obtain "clear and unambiguous permission" from the individual.[345] This requirement does not apply if the marketing communication is (1) in a face-to-face conversation, (2) a promotional gift of nominal value provided by the covered entity, (3) necessary for administration of a patient assistance program or other prescription

342. *Id*. at § 181.101.

343. *Id*. at § 181.102.

344. *Id*. at § 181.151.

345. *Id*. at § 181.152.

drug savings or discount program, or (4) made at the clear and unambiguous oral request of the individual.[346] Marketing communications sent through the mail (1) must be placed in an envelope showing only the names and addresses of the sender and recipient, (2) must state the name and toll-free number of the entity sending the materials, (3) must explain the recipient's right to be removed from the mailing list, and (4) if the recipient so requests, the entity must remove the person's name within 45 days of receiving the request.[347]

The Texas law broadly prohibits the sale of PHI. The only exceptions to the prohibition on receiving direct or indirect remuneration in exchange of a disclosure of PHI are that a covered entity may disclose PHI to another covered entity for the purposes of treatment, payment, health care operations, certain insurance functions defined by statute, or as otherwise authorized or required by state or federal law.[348] However, a covered entity that discloses information pursuant to these exceptions may not make a profit; its direct and indirect compensation must be limited to its reasonable costs of preparing or transmitting the protected health information.[349]

Finally, the Texas law prohibits any individual disclosure of PHI from being made without prior notice to the individual, which may be done through a notice posted at the covered entity's place of business or on its website.[350] In many cases, the statute also requires the covered entity to obtain written authorization from the individual or his or her representative prior to

346. *Id.* at §§ 181.152(a), (d).

347. *Id.* at §§ 181.152(b), (c).

348. *Id.* at § 181.153.

349. *Id*.

350. *Id*. at § 181.154(a).

disclosure.[351] Prior authorization is not required, however, if the disclosure is to another covered entity for the purposes of treatment, payment, health care operations, certain insurance functions defined by statute, or as otherwise authorized or required by state or federal law.[352]

(b) Enforcement

The Texas law permits the state attorney general to bring an action for injunctive relief to enjoin any violation of the statute or for civil penalties.[353] Under the statute, civil penalties may not exceed $5,000 for each negligent violation; $25,000 for each knowing or intentional violation; and $250,000 for each violation in which the covered entity knowingly or intentionally used PHI for financial gain.[354] Total penalties are capped at $250,000 per year if the disclosure was only to another covered entity for the purposes of treatment, payment, health care operations, or certain statutorily-defined insurance functions *and* the disclosed PHI was encrypted; the recipient of the PHI did not use or release it; and, as of the time of the disclosure, the covered entity had developed, implemented, and maintained security policies, including training.[355] On the other hand, if a court finds that violations have occurred frequently enough to constitute a "pattern or practice," the court may assess a civil penalty as

351. *Id.* at § 181.154(b). The Texas attorney general has developed a standard authorization form for this purpose. *See* https://texasattorneygeneral.gov/files/agency/hb300_auth_form.pdf.

352. TEX. HEALTH & SAFETY CODE ANN. § 181.154(c).

353. *Id*. at § 181.201.

354. *Id*.

355. *Id.* at § 181.201(b-1).

large as $1.5 million per year[356] and the entity may be precluded from participating in any state-funded health care program.[357]

Covered entities may be subject to disciplinary action by appropriate Texas licensing authorities, including possible revocation of the entity's license if the violation is sufficiently egregious,[358] and compliance audits under both HIPAA and the Texas law.[359] The statute, however, does not include any private right of action through which individuals could seek to remedy an improper disclosure of their own information, nor has it been the subject of any reported decisions.

356. *Id.* at § 181.201(c).

357. *Id.* at § 181.203.

358. *Id*. at § 181.202.

359. *Id.* at § 181.206.

SIDE BAR — HEALTH PRIVACY

Companies handling health information must understand the complex framework of laws and regulations comprising the healthcare privacy legal landscape.

Organizations processing or storing health information should understand whether this might subject them to the regulatory obligations of "covered entities" or "business associates" under HIPAA. Such organizations must comply with the HIPAA Privacy and Security Rules, which impose comprehensive requirements regarding the privacy and information security of protected health information.

Entities that are subject to HIPAA face the risk of potential regulatory audits, enforcement actions, and liability. Following the enactment of the final omnibus HIPAA/HITECH rule in January 2013, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services has aggressively enforced HIPAA violations. Since that time, there have been numerous multimillion dollar OCR settlements based upon HIPAA non-compliance, often subsequent to large security breaches and OCR investigations.

Organizations processing or storing health information should understand that even if they are not subject to the regulatory obligations of "covered entities" or "business associates" under HIPAA, they may nevertheless be subject to certain state privacy laws imposing restrictions on the uses and disclosures of such information. Some of these laws apply more broadly than HIPAA, and even provide individuals with a private right of action to seek redress based on non-compliance with the law.

VI. FINANCIAL

Records containing the personal financial data of individuals have long been a focus in the ongoing privacy debate. Exposure of the records for over 100,000 U.S. taxpayers during a 2015 data breach at the Internal Revenue Service provided a clear reminder that both financial institutions and government agencies collect and retain a great deal of this data.[360] For that reason, a number of regulations have been created over the years to attempt to address the confidentiality of personally identifiable financial information, while permitting financial institutions to conduct business in a safe and secure manner.

A. The Gramm-Leach-Bliley Act

1. Overview of The GLBA

Enacted in 1999, the Financial Services Modernization Act, more commonly known as the Gramm-Leach-Bliley Act (GLBA)[361] was designed to provide financial institutions with requirements for protecting the personal information of customers and consumers. This was accomplished through a set of Safeguard Rules and Privacy Rules, the latter of which will be discussed in detail here.

At the time the GLBA was enacted, the financial services sector had long been moving toward consolidation.[362] In response

360. *Data Thieves Gain Access to 100,000 U.S. Taxpayers' Information: IRS*, REUTERS (May 26, 2015), *available at* http://www.reuters.com/article/us-usa-tax-cybersecurity-idUSKBN0OB2H520150526.

361. 15 U.S.C. §§ 6801–6809 (1999), *available at* https://www.law.cornell.edu/uscode/text/15/chapter-94/subchapter-I.

362. *See* Joe Mahon, Fed. Reserve Bank of Minneapolis, *Financial Services Modernization Act of 1999, Commonly Called Gramm-Leach-Bliley*, FED. RESERVE HISTORY (Nov. 22, 2013), *available at* http://www.federalreservehistory.org/Events/DetailView/53.

to the stock market crash of 1929 and the subsequent Great Depression, regulations[363] had been put into place to create separations between financial services entities such as banks and securities firms.[364] In amending these regulations, the GLBA broke down the barriers between these entities so as to allow them to function in a more integrated fashion, thereby permitting financial institutions to serve a customer's needs across the banking spectrum. Acknowledging that one of the natural results of this integration would be that these financial institutions would have increased access to higher volumes of customer information, the GLBA set out to establish boundaries on how those institutions could handle that data in a safe and secure way.[365]

The terms of the GLBA apply to "financial institutions" that are required to implement technical safeguards around the personal data of their customers. The term is defined broadly to account for essentially all U.S. companies that, "the business of which is engaging in financial activities [that are financial in nature]."[366] Examples of such entities include, "companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance."[367]

---

363. *See, e.g., Federal Reserve Bank of New York Circulars: 1248. Banking Act of 1933*, FED. RESERVE ARCHIVE, *available at* https://fraser.stlouisfed.org/scribd/?item_id=15952&filepath=/docs/historical/ny%20circulars/1933_01248.pdf#scribd-open.

364. *See id*.

365. For additional background on the Congressional debate, *see* Financial Services Modernization Act of 1999, 145 CONG. REC. S13871-S13881, S13883-S13917 (Nov. 4, 1999), and Conference Report on S. 900, Gramm-Leach-Bliley Act, 145 CONG. REC. H11513-H11551 (Nov. 4, 1999).

366. 15 U.S.C. § 6809(3).

367. *Gramm-Leach-Bliley Act,* FED. TRADE COMM'N (Sept. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

The GLBA takes care to distinguish between "consumers" of financial institutions and "customers." Under the GLBA, a consumer is an "individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual."[368] This can be a one-time or infrequent touch point. A customer, by contrast, is an entity that is in a longer term, more continual relationship with the financial institution.[369] As more fully described below, this distinction is significant in that the notification requirements of the GLBA vary for customers and consumers.

2. Information Protected by the GLBA

The GLBA is designed to provide requirements for the handling and protection of "nonpublic personal information" provided by a consumer to a financial institution. Such information includes "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."[370] This would exclude any information that is otherwise already publicly available, but does account for any combination of information (e.g., grouping, list, description) that is derived from nonpublic personal information.[371] Examples can include information provided in connection with a loan

368. 15 U.S.C. § 6809(9).

369. *Id*. at § 6809(11); *see also How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FED. TRADE COMM'N (July 2002), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm#obligations.

370. 15 U.S.C. § 6809(4).

371. *Id*.

application packet, bank account data, and other personal financial data submitted in connection with a request for services from a financial institution.

3. Obligations of the GLBA

The GLBA has requirements for both the internal management and handling of nonpublic personal information by a financial institution ("The Safeguard Rules") and restrictions on the use and sharing of that data ("The Privacy Rules"). The Safeguard Rules are designed to serve as "standards for the financial institutions subject to" the jurisdiction of agencies with regulatory authority over such institutions as identified by § 6805 of the GLBA:

> relating to administrative, technical, and physical safeguards—(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[372]

The Privacy Rules outline the manner in which nonpublic personal information may be shared by the financial institution with other parties, and the permitted purposes under the GLBA for such sharing. At the heart of these privacy protections is the concept of consumer/customer notification.

372. 15 U.S.C. § 6801(b).

(a) Notification Obligations

At the creation of a customer relationship with a financial institution, and on a no less than annual basis thereafter, the financial institution must make the customer aware of its policies and practices concerning handling and sharing the customer's nonpublic personal information.[373] The content of such notifications must include the financial institution's policies concerning disclosure of nonpublic personal information to nonaffiliated third parties, both while an individual is a customer of the financial institution and after the customer relationship ends; a description of the type and kind of nonpublic personal information that is collected by the financial institution; a description of the protections in place to safeguard the data; and a listing of any disclosures required under the Fair Credit Reporting Act.[374]

Customers must receive these notices as described above automatically and on an annual basis thereafter (or at the point in time when the privacy practices of the financial institution change in such a way that additional notification is required). *Consumers*, by contrast, receive notifications only when the financial institution shares nonpublic personal information with a nonaffiliated third party in a manner that is not already contemplated within one of the GLBA's exceptions. In the event of such sharing, consumers must be offered the ability to opt out of certain data sharing prior to the transmission of any nonpublic information to a nonaffiliated third party.[375]

(b) Nonaffiliated Third Parties

In general, the GLBA restricts a financial institution's ability to share nonpublic personal information with a nonaffiliated

373. *Id*. at § 6803(a).

374. *Id*. at § 6803(c).

375. *Id*. at § 6802(b).

third party.[376] Section 6802 of the GLBA prohibits sharing with such parties unless the sharing is permitted under one of the specifically identified exceptions. The identified exceptions include sharing of nonpublic personal information with parties who perform services for or functions on behalf of the financial institution, which includes marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements that contain provisions requiring all parties to protect the confidentiality of the information shared.[377] Other more general exceptions are also outlined within § 6802, including but not limited to, the relaying of nonpublic personal information to effect the transaction requested by the consumer, the sharing of nonpublic personal information with the consumer's consent, the sharing of nonpublic personal information in order to assist with fraud detection or institutional risk management efforts, and also sharing with law enforcement and regulatory agencies as permitted or required by law.[378] In each instance, the receiving nonaffiliated third party must not further use the nonpublic personal information it receives for any purpose other than that for which it was originally provided.[379]

376. "The term 'nonaffiliated third party' means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution." *Id*. at § 6809(5).

377. *Id*. at § 6802(b)(2).

378. *Id*. at § 6802(e).

379. *Id*. at § 6802(c).

(c) Model Privacy Form

A variety of agencies[380] have rulemaking authority under § 6804 of the GLBA, and, as directed by § 6803(e) of the GLBA, the groups have combined efforts to develop Model Privacy Forms that can be leveraged by financial institutions looking to comply with these notification requirements.[381] Financial institutions that choose to use their regulating agency's model form qualify for safe harbor and are considered to have acted in compliance with the GLBA.[382]

4. Relationship with State Regulations

Section 6807 of the GLBA affirms that nothing contained within the GLBA shall be interpreted as, "superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency."[383] In fact, to the extent that related state laws afford an individual more protection than is outlined in the GLBA, it states that such additional protections are not to be construed as "inconsistent."[384] The authority to determine whether a state's financial privacy regulations are inconsistent with the GLBA

380. CFPB, SEC, CFTC, FTC (15 U.S.C. § 6804(1)). *See also* 15 U.S.C. §6805 for enforcement powers of these agencies.

381. For an example of such Model Privacy Forms, *see* 12 C.F.R. Part 1016 (Appendix), *available at* http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=d98a14fe2ed1d022d4e943885dbb70aa&ty=HTML&h=L&n=pt12.8.1016&r=PART#ap12.8.1016_117.1.

382. 15 U.S.C. § 6803(e)(4).

383. *Id*. at § 6807(a).

384. *Id*. at § 6807(b).

currently rests with the Bureau of Consumer Financial Protection (CFPB) under the GLBA.[385] As a result, some states have taken it upon themselves to enact stricter data privacy regulations for the protection of consumer nonpublic personal information.

(a) California Financial Information Privacy Act

Effective July 1, 2004, the California Financial Information Privacy Act (also known as "SB1" or "FIPA") was put in place by the state legislature because "[t]he policies intended to protect financial privacy imposed by the Gramm-Leach-Bliley Act are inadequate to meet the privacy concerns of California residents."[386] Notably, SB1 does not distinguish between customers who have a continuing relationship with financial institutions and consumers who may have less frequent touch points, opting instead to universally identify "consumers" as parties protected by its provisions.[387] Further, while, like the GLBA, SB1 requires a financial institution obtain "explicit prior consent" from a consumer when sharing the consumer's nonpublic personal information with a nonaffiliated third party,[388] it also requires the institution annually "clearly and conspicuously" notify consumers and obtain their consent to disclose nonpublic personal information with affiliates in certain circumstances.[389] In 2008 this provision came up for review by the Ninth Circuit in

385. *Id*.

386. CAL. FIN. CODE §§ 4051.5(3) (July 1, 2004), *available at* https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=FIN&division=1.4.&title=&part=&chapter=&article.

387. CAL. FIN. CODE § 4052(f).

388. *Id*. at § 4052.5; *see also, Your Financial Privacy Rights*, STATE OF CAL. DEP'T OF JUSTICE (June 2014), *available at* https://oag.ca.gov/privacy/facts/financial-privacy/rights.

389. CAL. FIN. CODE § 4053(b).

American Bankers Association v. Lockyer (now known as *ABA v. Brown*), where the Court upheld the affiliate-sharing requirement of SB1 to the extent the nonpublic personal information involved was not considered "consumer report" information under (and is therefore preempted by) the Fair Credit Reporting Act.[390] As with the GLBA, SB1 also provides a safe harbor for financial institutions that leverage the provided Model Form entitled "Important Privacy Choices for Consumers."[391]

(b) Additional State Financial Privacy Regulations

Other states have adopted an "opt-in" posture for sharing nonpublic personal information with both affiliates and nonaffiliated third parties. Under Title 6 of the Alaska Statutes, the "records of financial institutions relating to their depositors and customers and the information in the records," are to be kept confidential, and the financial institution is required, if possible, to notify a consumer prior to disclosing such information.[392] Vermont's Financial Privacy Act likewise has similar restrictions in place.[393] Still other states have chosen to more closely align with the GLBA standard of providing notification in the context of data sharing with nonaffiliated third parties. Because of the fluctuating nature of state data protection regulations, it is advisable to refer to the current text of a state's statutes for the most up-to-date requirements for that given state or territory.

---

390. Am. Bankers Ass'n v. Lockyer, 541 F.3d 1214 (9th Cir. 2008).

391. CAL. FIN. CODE § 4053(d), and Model Form, *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/sb1_standards.pdf.

392. ALASKA STAT. § 06.01.028.

393. VT. STAT. ANN. tit. 8, §§ 10201 *et seq*., tit. 9, § 2480e.

5. Rulemaking and Enforcement

When originally enacted, primary rulemaking authority for the GLBA fell under the purview of the FTC. With the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act in July 2010, that responsibility shifted to the CFPB.[394] Since that time, the CFPB has formally adopted one rule related to the GLBA. In October 2014, the CFPB issued a final rule that relaxed some of the requirements concerning annual customer privacy notifications.[395] Prior to adoption of the final rule, financial institutions had been required to deliver hard-copy notices to all impacted consumers annually (or electronically transmit the notices to consumers who had agreed to electronic delivery), leading to a significant expenditure of time and resources in order to comply with GLBA. The final rule now allowed for the online posting of these notices by financial institutions so long as individuals have been given the option to exercise any available opt-out rights and have not done so, all required notifications have been provided to date, the information included in the privacy notice has not changed since the last notification was delivered, and the financial institution uses the Model Privacy Form as provided by its relevant regulating agency.[396]

---

394. 12 U.S.C. §§ 5841(12)(J), 5514(b)–(c), 5515(b)–(c). Additional summary information of the CFPB's responsibilities under GLBA and the CFPB's interpretation of the act can be found in CONSUMER FIN. PROT. BUREAU, CFPB SUPERVISION AND EXAMINATION MANUAL, at GLBA Privacy 1–10 (Oct. 2012), relevant portion *available at* http://www.cfpaguide.com/portalresource/Exam%20Manual%20v%202%20-%20GLBA.pdf.

395. Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P), 79 Fed. Reg. 64,057 (Oct. 28, 2014), *available at* http://www.gpo.gov/fdsys/pkg/FR-2014-10-28/pdf/2014-25299.pdf.

396. *Id*.

The GLBA is enforced by federal banking agencies and other federal regulatory authorities as well as state insurance authorities. The GLBA Privacy Rule is enforced by the FTC.[397]

B. The Fair Credit Reporting Act

1. Overview of the FCRA

The Fair Credit Reporting Act (FCRA) was enacted in 1970 to regulate the consumer reporting industry and provide privacy rights in consumer reports.[398] The FCRA mandates accurate and relevant data collection, provides consumers with the ability to access and correct their information, and limits the use of consumer reports to defined permissible purposes.[399] The FCRA applies to "any consumer reporting agency" that furnishes a "consumer report"[400] as well as, in limited circumstances, any person or entity that "furnishes" credit-related information to a consumer reporting agency.[401]

---

397. *See* FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT (July 2002), at 14, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

398. 15 U.S.C. § 1681 (1970). FCRA amendments in 1996 strengthened consumer access and correction rights and included provisions for non-consumer-initiated transactions. FCRA was further amended by the Fair and Accurate Credit Transaction Act in 2003, which enacted additional consumer protections.

399. *See, e.g.*, *The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/fcra; Gorman v. Wolpoff & Abramson, LLP, 584 F.3d 1147, 1153 (9th Cir. 2009) ("Congress enacted the Fair Credit Reporting Act . . . to ensure fair and accurate credit reporting, promote efficiency in the banking system, and protect consumer privacy." (internal quotation omitted)).

400. 15 U.S.C. § 1681b.

401. *Id.* at §§ 1681b, 1681s-2.

The FCRA defines "consumer reporting agencies" (CRAs) as entities which, for a monetary fee, "regularly engage in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[402] Well known CRAs include Equifax, TransUnion, and Experian Information Solutions, but there are also thousands of smaller CRAs.

A "consumer report" is any "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used for the sole purpose of serving as a factor in establishing the consumer's eligibility for . . . credit or insurance purposes, employment purposes, or any other purpose authorized under section 1681b of this title."[403] Courts have held that "even if a report is used or expected to be used for a non-consumer purpose, it may still fall within the definition of a consumer report if it contains information that was originally collected by a consumer reporting agency with the expectation that it would be used for a consumer purpose."[404]

2. Duties of Consumer Reporting Agencies

The FCRA specifically requires CRAs to adhere to the following requirements:

---

402. *Id.* at § 1681a(f).

403. *Id.* at § 1681(d).

404. Ippolito v. WNS, Inc., 864 F.2d 440, 453 (7th Cir. 1988); Bakker v. McKinnon, 152 F.3d 1007, 1012 (8th Cir. 1998) (quoting *Ippolito*, 864 F.2d at 453).

- Accuracy—"Wherever a consumer reporting agency prepares a consumer report, it shall follow reasonable procedures to assure maximum accuracy of the information concerning the individual about whom the report relates."[405]
- Disclosure—CRAs, at the request of the consumer, must disclose, among other things, "[a]ll the information in the consumer's file at the time of the request."[406]
- Investigation—If a consumer disputes the accuracy of any information, a consumer reporting agency, "shall, free of charge, conduct a reasonable investigation to determine whether the disputed information is inaccurate."[407]
- Free Consumer Reports—CRAs must provide a free consumer report once a year at the request of a consumer. Consumers can obtain their reports at https://www.annualcreditreport.com.
- Permissible uses—A CRA can furnish a consumer report only for permissible purposes which includes:
    1) in response to a court order or grand jury subpoena;
    2) to the person to whom the report pertains;
    3) to a "person which [the agency] has reason to believe" intends to use the information in connection with:
        a) the extension of credit;
        b) employment purposes;
        c) insurance underwriting;

405. 15 U.S.C. § 1681e(b).

406. *Id.* at § 1681g.

407. *Id.* at § 1681i(a).

d) licensing or the conferral of governmental benefits;
e) assessment of credit risks associated with an existing credit obligation; or
f) a "legitimate business need" when engaging in a "business transaction involving the consumer";

4) to establish a person's capacity to pay child support;
5) to an agency administering a state plan for use to set initial or modified child support award; or
6) to the Federal Deposit Insurance Corporation or National Credit Union Administration.[408]

- Notice and Opt Out—A CRA may share consumer report information with its affiliates. However, consumers whose information is shared with an affiliate must be notified of the disclosure and given an opportunity to opt out.[409] In addition, entities that receive consumer report information from affiliates may not use it to offer products or services to the consumer unless the affiliate gave certain strong disclosures and an opt-out opportunity to the consumer.[410] Disclosure to non-affiliates is governed by the GLBA.

3. Furnishers of Information to CRAs

To ensure that credit reports are accurate, the FCRA imposes some duties on the sources that provide credit information to

408. *Id.* at § 1681b.

409. *Id.* at § 1681a(d)(2)(A)(iii).

410. *Id.* at § 1681s-3(a)(1).

CRAs, called "furnishers" in the statute.[411] Among those obligations are the duties to provide accurate information to CRAs and upon receiving a report that the consumer disputes the accuracy or completeness of the information provided, to investigate and, if needed, to correct the report of any "inaccurate or incomplete" information.[412] If the completeness or accuracy of any information furnished by any person to any CRA is disputed to such person by a consumer, the person may not furnish the information to any CRA without notice that such information is disputed by the consumer.

4. Users of Consumer Reports

Users of consumer reports include employers who use consumer reports in employment decisions as well as lenders, insurance companies, and others. Users must certify to the CRA the permissible purpose for which the report is being obtained and that the report will be used for no other purpose.[413] Users must also notify consumers when adverse action is taken with respect to any consumer that is based in whole or in part on any information contained in a consumer report.[414] The notice must point out the adverse action, explain how to reach the agency that reported on the consumer's credit, and tell the consumer

411. Longman v. Wachovia Bank, N.A., 702 F.3d 148, 150–51 (2d Cir. 2012) (citing 15 U.S.C. § 1681s-2). "The most common . . . furnishers of information are credit card issuers, auto dealers, department and grocery stores, lenders, utilities, insurers, collection agencies, and government agencies." H.R. REP. NO. 108–263, pt. 1, at 24 (2003).

412. 15 U.S.C. § 1681s–2(a); *see Longman*, 702 F.3d at 150 ("Among these are duties to refrain from knowingly reporting inaccurate information, *see* § 1681s-2(a)(1), and to correct any information they later discover to be inaccurate, *see* § 1681s-2(a)(2).").

413. 15 U.S.C. § 1681e(a).

414. *Id.* at § 1681m.

that he can get a free copy of the report and dispute its accuracy with the agency.[415]

The FCRA provides that a person may not procure a consumer report for employment purposes unless the employer or potential employer discloses in writing to the consumer that a report is to be obtained and the consumer authorizes in writing that a report can be obtained. A CRA may not furnish a consumer report for employment purposes unless the person who obtains such report certifies to the CRA that the consent of the individual was obtained and that the information in the consumer report will not be used in violation of any equal employment opportunity law or regulation.[416]

5. Limitations on Information Contained in Credit Reports

No CRA may make any consumer report containing any of the following items of information:

1) cases under Title 11 or under the Bankruptcy Act that, from the date of entry of the order for relief or the date of adjudication, antedate the report by more than ten years;
2) civil suits, civil judgments, and records of arrest that, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period;
3) paid tax liens which, from date of payment, antedate the report by more than seven years;
4) accounts placed for collection or charged to profit and loss which antedate the report by more than seven years;

415. *Id*.

416. *Id.* at § 1681b(b)(1)(A)(i).

5) any other adverse item of information, other than records of convictions of crimes which antedates the report by more than seven years; or
6) the name, address, and telephone number of any medical information furnisher that has notified the agency of its status, unless (A) such name, address, and telephone number are restricted or reported using codes that do not identify, or provide information sufficient to infer, the specific provider or the nature of such services, products, or devices to a person other than the consumer; or (B) the report is being provided to an insurance company for a purpose relating to engaging in the business of insurance other than property and casualty insurance.[417]

The above provisions, however, are not applicable in the case of any consumer credit report to be used in connection with (1) a credit transaction involving, or which may reasonably be expected to involve, a principal amount of $150,000 or more; (2) the underwriting of life insurance involving, or which may reasonably be expected to involve, a face amount of $150,000 or more; or (3) the employment of any individual at an annual salary that equals, or which may reasonably be expected to equal $75,000, or more.

6. Private Rights of Action and Damages

Private rights of action exist to enforce negligent or willful violations of the FCRA. It permits consumers to recover actual damages from "any person who is negligent in failing to comply with a requirement" it imposes; or actual, statutory, and poten-

417. *Id.* at § 1681c.

tially punitive damages from a person whose violation was willful.[418] "Actual damages" has been interpreted to include damages for emotional distress.[419]

While consumers have a private remedy against "negligent or willful misconduct by a furnisher" of consumer credit information, this right only arises once the furnisher has received a notice from the CRA disputing the accuracy or completeness of the information provided.[420] The FCRA's statute of limitations extends to two years after the date when plaintiff discovers the violation or five years after the date of the violation, whichever occurs earlier.

7. Rulemaking and Enforcement

In addition to private litigants, the FCRA is enforced by the FTC and the CFPB. The Dodd-Frank Act of 2010 assigned the CFPB primary federal authority for enforcement and rulemaking regarding the FCRA. The Dodd-Frank Act also created a Consumer Financial Civil Penalty Fund to receive civil penalties obtained by the CFPB for violations of consumer financial protection statutes.

C. The Right to Financial Privacy Act of 1978

In response to a string of court decisions declaring that an individual has no reasonable expectation of privacy in his or her financial records, most notably the Supreme Court's decision in *United States v. Miller*,[421] Congress enacted the Right to Financial

418. *Id.* at §§ 1681o–n.

419. *See* Taylor v. Tenant Tracker, Inc., 710 F.3d 824, 828 (8th Cir. 2013); Robinson v. Equifax Info. Servs., LLC, 560 F.3d 235, 239 (4th Cir. 2009); Guimond v. Trans Union Credit Info. Co., 45 F.3d 1329, 1333 (9th Cir. 1995).

420. 15 U.S.C. §§ 1681s-2(a)–(b); Boggio v. USAA Fed. Sav. Bank., 696 F.3d 611 (6th Cir. 2012).

421. United States v. Miller, 425 U.S. 435, 442–43 (1976).

Privacy Act of 1978 (RFPA).[422] The RFPA prohibits agencies of the federal government from obtaining such records from financial institutions without first giving the individual notice and an opportunity to object to the disclosure.[423]

1. Overview of the RFPA

The RFPA explicitly governs requests made by "any agency or department of the United States, or any officer, employee, or agent thereof," and does not apply to equivalent agencies at the state and local government levels.[424] As discussed below several states have chosen to enact similar legislation on their own, but the RFPA only applies to federal government agencies.

As with the GLBA, the RFPA defines "financial institutions" required to comply with its terms broadly. This includes entities you might expect to be a financial institution such as depository banks, loan companies, savings associations, and credit unions; but also pulls in "card issuers" as defined by the Truth in Lending Act.[425] As a result, any entity that issues a credit card to a consumer, including entities such as retailers and gas stations, must follow RFPA notification provisions prior to making disclosures to the federal government.

The records protected by the RFPA are all documentation (i.e., financial records) that evidences a customer's relationship with the financial institution. The RFPA is limited, however, to

422. 12 U.S.C. §§ 3401–3422 (1978), *available at* https://www.law.cornell.edu/uscode/text/12/chapter-35.

423. *Id.* at § 3402.

424. *Id.* at § 3401.

425. 15 U.S.C. § 1602(o).

the records of individuals or a partnership "of five or fewer individuals."[426] For that reason, the accounts of companies or entities comprising more than five individuals are not considered "financial records" under the RFPA.

2. Obligations of the RFPA

The RFPA places obligations on both the federal agency requesting a customer's financial records and on the financial institution that releases the data to the federal government.

(a) Limitations on Federal Government Requests

A federal agency seeking the financial records of an individual must be able to clearly state the purpose for which the information is sought, including the provision of a valid and properly served administrative or judicial subpoena, summons, or search warrant, or a formal written request from the agency if such vehicles are not available.[427] The RFPA provides required notification language to be included in the request document that identifies the specific basis for the government's request and the nature of its inquiry into the financial records.[428] Once the data has been received, the agency may not further transmit the information provided to another agency or department unless "the transferring agency or department certifies in writing that there is reason to believe that the records are relevant to a legitimate law enforcement inquiry, or intelligence or counterintelligence activity, investigation or analysis related to international terrorism within the jurisdiction of the receiving agency or department."[429]

---

426. 12 U.S.C. § 3401(4).

427. *Id.* at § 3402.

428. *Id.* at §§ 3405(2), 3406(b), 3407(2), 3408(4)(A).

429. *Id.* at § 3412(a).

(b) Financial Institution's Obligations

Upon receipt of the government's request for a customer's financial records, financial institutions subject to the RFPA must obtain from the customer a signed and dated form of consent that:

1) authorizes disclosure of the customer's financial records for a period not in excess of three months;
2) states that the customer may revoke such authorization at any time before the financial records are disclosed;
3) identifies the financial records which are authorized to be disclosed;
4) specifies the purposes for which, and the Government authority to which, such records may be disclosed; and
5) states the customer's rights under the RFPA.[430]

The financial institution cannot make a customer's consent to release information a condition upon which the institution will do business with the customer, and the customer under most circumstances has the right to obtain a copy of the data that was released to the government.[431]

(c) Exceptions

Under § 3409 of the RFPA, notification to a customer may be delayed under a proscribed set of circumstances. More specifically, if the government is able to evidence that the request is being made pursuant to an ongoing investigation and notification would jeopardize the investigation or the life or safety of

430. *Id.* at § 3404(a).

431. *Id.* at §§ 3404(b), (c).

another, or the notification would otherwise create the opportunity for the intimidation of a witness to the matter or create a flight risk for the individual being investigated, a court is able to grant a request for a delay in notification with an initial period not to exceed 90 days.[432] Further, the RFPA does not apply to requests for financial records that do not particularly identify an individual, records whose disclosure is required by federal rule, disclosures made pursuant to the Federal Rules of Civil or Criminal Procedure, disclosures made to uncover crimes made against the financial institution by criminal insiders, and disclosures made to certain regulatory agencies like the Federal Housing Finance Agency and the CFPB, among other identified exceptions in § 3413 of the act.[433] In early 2015, legislation introduced in the House of Representatives sought to remove the CFPB's exemption in the RFPA.[434] At the time of the publication of this Primer, the legislation was still pending review in the House Committee on Financial Services.

3. Civil Penalties for Non-Compliance

The RFPA provides recourse for individuals who are able to successfully demonstrate that either their financial institution or the government acted in a manner contrary to the provisions of the RFPA. Liability under the RFPA can equal the sum of:

1) $100 without regard to the volume of records involved;
2) any actual damages sustained by the customer as a result of the disclosure;

---

432. *Id.* at § 3409.

433. *Id.* at § 3413.

434. Consumer Right to Financial Privacy Act of 2015, H.R. 1262, 114th Cong. (Mar. 4, 2015), *available at* https://www.congress.gov/bill/114th-congress/house-bill/1262.

3) such punitive damages as the court may allow, where the violation is found to have been willful or intentional; and
4) in the case of any successful action to enforce liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.[435]

Federal agents found to have violated the RFPA may be subject to further internal discipline from the Director of the Office of Personnel Management.[436] Financial institutions have immunity from civil liability for disclosures made as a part of reporting criminal activity evidence contained in records to a government authority via mechanisms such as a Suspicious Activity Report (SAR) with Financial Crimes Enforcement Network (FinCEN).[437]

4. Relationship with State Regulations

As mentioned above, the RFPA does not apply to requests made by state or local government agencies. Several states, however, have enacted regulations with terms similar or equivalent to those of the RFPA, including Alabama, Alaska, Connecticut,[438] California,[439] Illinois,[440] Louisiana,[441] Maryland,[442] Maine,

435. 12 U.S.C. § 3417(a).

436. *Id.* at § 3417(b).

437. *Id.* at § 3403(c).

438. CONN. GEN. STAT. § 36a-43, *available at* http://cga.ct.gov/current/pub/chap_664a.htm#sec_36a-43.

439. CAL GOV'T CODE §§ 7460–7493.

440. 205 ILL. COMP. STAT. 5/48.1.

441. LA. REV. STAT. § 6:333, *available at* http://law.justia.com/codes/louisiana/2011/rs/title6/rs6-333.

442. MD. CODE ANN., FIN. INST. §§ 1-301 to 1-306 (2014).

New Hampshire, North Carolina,[443] North Dakota, Oklahoma, Oregon, Utah, and Vermont. For the most up-to-date information regarding a state's financial privacy regulations, consult the current text of a state's statutes.

SIDE BAR — FINANCIAL PRIVACY

The regulations in place protecting personal financial data of individuals are wide-ranging, and can impact more than just financial institutions.

Take care when sharing nonpublic personal information with third parties. Financial institutions that want to share such data with nonaffiliated third parties should validate that the data is being shared under one of the permitted purposes specifically outlined in the GLBA or obtain the individual's consent prior to transferring the data.

The obligations concerning protection of personal information contained in a credit report can extend to parties beyond Credit Reporting Agencies. Under the FCRA, producers of consumer credit reports, parties that furnish data to credit reporting agencies, and recipients of consumer credit reports all have specific obligations for handling of credit reports, ranging from sharing to future use of the data. Companies should become familiar with their role in the process and whether there are restrictions in place on their behavior vis-à-vis credit reports.

Become familiar with both the federal and state laws that may apply to your company as it manages personal financial data. At times, state regulations can be even more restrictive and protective of a consumer's right to privacy than the federal standards.

443. North Carolina Financial Privacy Act, N.C. GEN. STAT. ANN. § 53B-1 *et seq.*, *available at* http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/ByChapter/Chapter_53B.pdf.

VII. WORKPLACE PRIVACY

More than ever before, employers have a wealth of powerful and new technologies that allow them to monitor employee communications, such as telephone calls, email and text messages, and Internet access; and to monitor employees' movements using video cameras and satellite-based Global Positioning System (GPS) tracking devices. There are legitimate and well-accepted business reasons for employee monitoring: to make certain that employees spend working hours actively engaged in work-related activities; to protect confidential information and trade secrets; to ensure compliance with governmental regulations; and to guard against illegal activities.[444]

Employee monitoring and surveillance is not without limits. As discussed below, while there have been advances in the enactment and application of workplace privacy laws, technology continues to test their limits.

444. According to a 2007 survey conducted by the American Management Association and the ePolicy Institute, 66% of employers surveyed monitored employee Internet connections, nearly half tracked content, keystrokes, and time spent at the keyboard, and only slightly fewer employers stored and reviewed computer files. Of the 43% of companies that monitored email communications, nearly three-quarters used technology to automatically monitor email, and over a third assigned an individual to manually read and review email. *The Latest on Workplace Monitoring and Surveillance*, AM. MGMT. ASS'N (Nov. 17, 2014), http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx.

A. Legal Framework

1. Regulatory Protections

The Electronic Communications Privacy Act[445] (ECPA) is a key privacy law that applies in the context of network surveillance and monitoring of employees.[446] The ECPA prohibits the intentional interception of "any wire, oral or electronic communication" while those communications are being made, are in transit, and while stored on computers. There are two exceptions to the ECPA that generally exempt employers from its prohibitions.[447] First, an employer is exempt if an employee is using a company computer or device and the employer can show a valid business reason for monitoring an employee's communications or activities.[448] Second, an employer is exempt from the ECPA if the employee has consented to email or telephone call monitoring.[449]

2. U.S. Constitution

The Fourth Amendment to the U.S. Constitution provides an additional layer of privacy protection available to government employees by guaranteeing "[t]he right of the people to be se-

445. 18 U.S.C. §§ 2510–2520, 2701 (2012).

446. Title I of the ECPA, known as the "Wiretap Act," regulates the interception of transmitted communications. Title II, referred to as the "Stored Communications Act," governs access to stored communications and records held by communications service providers. Both are aimed at protecting private communications, such as email, from unwarranted government and private intrusion.

447. 18 U.S.C. §§ 2510 *et. seq*. (2012).

448. *Id.* at § 2511(2)(a)(i).

449. *Id.* at § 2511(2)(c).

cure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[450] A pivotal determination in cases involving governmental invasion of privacy is whether the government employee has a reasonable expectation of privacy in relation to the conduct of the governmental employer.[451] Please refer to Section III.A.4 of this Primer for further information regarding the right to privacy under the Fourth Amendment.

3. State Issues

As discussed in Section II.A of this Primer, common law privacy rights afford varying degrees of protection for individuals, including private employees. These rights are generally predicated on a reasonable expectation of privacy by the employee and a highly offensive violation by the employer.[452] Employees, in proving a claim based on this tort, must establish that the employer's intrusion "would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object."[453]

Given the increasing use of technology by employees in their private lives and the growth of technology permitting employee monitoring, there is an emerging trend among states to favor the

450. U.S. CONST. amend. IV.

451. O'Connor v. Ortega, 480 U.S. 709, 716 (1987).

452. *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of is privacy, if the intrusion would be highly offensive to a reasonable person.").

453. *Id.* at § 652B cmt. d.

protection of personal information of private employees.[454] Two states, Connecticut and Delaware, have passed legislation requiring employers to give notice to employees prior to monitoring email communications or Internet access.[455] Connecticut[456] requires employers engaged in electronic monitoring to give prior written notice to all employees, informing them of the types of monitoring implemented. An employer is exempt from giving this notice if it has reasonable grounds to believe that (1) employees are engaged in illegal conduct, and (2) electronic monitoring may produce evidence of the misconduct. Delaware[457] prohibits employers from monitoring or intercepting electronic mail or Internet access/use of an employee unless the employer has first given a one-time written or electronic notice to the employee. A Delaware employer is exempt from providing prior notice for processes that are performed solely for the purpose of computer system maintenance and/or protection, and for court-ordered actions.

There is no "one size fits all" when it comes to determining whether employee privacy claims trump the rights of an employer to access an employee's personal information. Resolution of workplace privacy issues are intensely fact-driven and often turn on such considerations as who owns the device, the existence and scope of a computer usage policy, and whether an employee has consented to being monitored.

---

454. *Access to Social Media Usernames and Passwords*, NAT'L CONFERENCE OF STATE LEGIS. (July 6, 2016), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

455. CONN. GEN. STAT. ANN. § 31-48d; DEL. CODE. ANN. tit. 19, § 705; *see also generally* NAT'L CONFERENCE OF STATE LEGIS., *supra* note 454.

456. CONN. GEN. STAT. ANN. § 31-48d.

457. DEL. CODE. ANN. tit. 19, § 705.

B. Use of Company Equipment and Email

Underpinning court decisions on an employer's alleged violations of an employee's right to privacy, is whether the employee had a *reasonable expectation* of privacy in the personal information sought to be protected. The conclusion reached on this issue often turns on whether the employer or the employee owns the device.

In 2010, the Supreme Court was faced with applying the law of privacy in the broader context of technological advances in electronic communications in *City of Ontario v. Quon*.[458] *Quon* involved the privacy interest of a government employee in text messages that he sent on a government-owned pager.[459] Without resolving the issue of whether the employee had a reasonable expectation of privacy in the text messages, the Court held that the government's search of the messages was reasonable since it was "justified at its inception" and "the measures adopted [were] reasonably related to the objectives of the search and [were] not excessively intrusive in light of the circumstances giving rise to the search."[460]

The Court was, however, reluctant to establish precedent on broader employee privacy rights given the rapid pace of evolving technologies, explaining, "[t]he Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of

458. 560 U.S. 746 (2010).

459. Although *Quon* involved Fourth Amendment privacy issues of governmental searches, the Court concluded that the search would be regarded as reasonable and normal in the private-employer context. *Quon*, 560 U.S. at 764–765.

460. *Id*. at 761.

emerging technology before its role in society has become clear."[461]

Since *Quon*, numerous courts around the country have found that employer-supplied electronic devices, such as computers, cell phones, and tablets, may be subject to monitoring regardless of whether the specific device is identified by an employer as being monitored. However, monitoring the content of employees' private communications may present legal risks to employers in certain circumstances. In addition to ownership of the device, courts consider the existence and scope of a company's computer usage policy, steps taken by the employee to maintain the privacy of personal emails, the use of the company-owned computer system, and the content of the communication at issue. For example, in *Stengart v. Loving Care Agency, Inc.*, the New Jersey Supreme Court held that a private company employee had a reasonable expectation of privacy in personal emails on company computers, such that employers should not read the specific contents of such emails.[462] The court noted the important public policy concerns at issue in the case because the personal emails between the employee and her attorney were protected by the attorney-client privilege, but the case is instructive regarding an employee's reasonable expectation of privacy more generally.

461. *Id*. at 759.

462. 990 A.2d 650, 663 (N.J. 2010).

C. Bring Your Own Device Policies

More and more, employers are transitioning from employer-owned devices to employee-owned devices.[463] With the widespread usage of smartphones, tablets, and personal laptops, employers and employees alike are finding that policies that permit employees to utilize their own devices in the workplace provide both convenience and cost savings. But while connecting an employee-owned personal device to an employer computer system to access email and data on the employer network allows an employee to work anytime, anywhere, the bring-your-own-device revolution is causing tensions between how much access an employer is permitted to have to an employee's device and how much privacy the employee can expect.[464] Companies are concerned about related issues, such as keeping confidential data from falling into a competitor's hands and preventing disclosure of other corporate or personally identifiable data to outsiders, while employees want to keep personal photographs, text messages, and personal emails private.[465]

Issues also arise as to how to effectively deal with company and personal information on the devices after employment terminates. In a case out of the Southern District of Texas, *Rajaee v.*

---

463. In a 2012 survey conducted by SANS, 60% of employers allowed employees to bring their own devices to work. Kevin Johnson, *SANS Mobility/BYOD Security Survey*, SANS INST. (2012), http://www.sans.org/reading-room/whitepapers/analyst/mobility-byod-security-survey-35210. Notably, the same year, a survey conducted by Ovum revealed that only 30% of employers required their employees to a sign BYOD agreement. Adrian Drury & Richard Absalom, *BYOD: An Emerging Market Trend In More Ways Than One*, OVUM (2012), http://www.us.logicalis.com/globalassets/united-states/whitepapers/logicalisbyodwhitepaperovum.pdf.

464. Marilyn Odendahl, *Bring Your Own Device Creates Privacy Issues for Employees*, INDIANAPOLIS BUS. J. (August 20, 2014), http://www.ibj.com/articles/49128-bring-your-own-device-creates-privacy-issues-for-em.

465. *Id*.

Design Tech Homes, Ltd., an employee who had worked in the home construction sales industry was required to have open and constant communication with clients.[466] The employee chose to not use an employer-owned cell phone and instead utilized his own iPhone for work calls, emails, calendars, and business contacts.[467] Upon notifying his employer that he would be resigning, the employee was immediately terminated and the employer's network administrator remotely wiped his phone—deleting all data—both personal and work related.[468] The court rejected the employee's claim under the ECPA, reasoning that information an individual stores on a hard drive or cell phone does not qualify as electronic storage under the statute.[469] Accordingly, the plaintiff could not recover damages arising from the loss of videos, pictures, and other personal data on the plaintiff's personal device.[470]

D. Social Media Privacy

From Twitter and Facebook to LinkedIn, Pinterest, and YouTube, social media offers a vast array of opportunities for companies to engage with both job applicants and employees. However, employer exposure to the potentially costly and protracted risks associated with social media is greater now than ever before. Employers may face harassment, discrimination,

---

466. Rajaee v. Design Tech Homes, Ltd., Civ. A. No. H-13-2517, 2014 U.S. Dist. LEXIS 159180, at *2 (S.D. Tex. Nov. 11, 2014).

467. *Id*.

468. *Id.* at *3.

469. *Id.* at *5 (citing Garcia v. City of Laredo, Tex. 702 F.3d 788, 791 (5th Cir. 2012) and 18 U.S.C. § 2701(a)(1)).

470. An overview of BYOD policies in the context of litigation may be found at Andrew Hinkes, *BYOD Polices: A Litigation Perspective*, AM. BAR ASS'N (July 8, 2013), *available at* http://apps.americanbar.org/litigation/committees/corporate/articles/spring2013-0713-byod-policies-litigation-perspective.html.

and invasion of privacy claims, and in some cases, find that their electronic business connections may be compromised with the departure of particular employees. Social media sites nevertheless offer significant benefits to employers such as the ability to screen candidates prior to hiring and to monitor employees while they are on the clock.

1. Passwords and Other Login Information

The most significant privacy violations in the context of workplace social media monitoring are employer policies that compel employees to hand over their passwords and other login information. Since 2012, nineteen states have enacted laws that protect employee privacy in this regard. For example, Illinois,[471] Colorado,[472] Oregon,[473] and Washington[474] prohibit an employer from requesting access to an employee's personal social media

471. 820 Ill. Comp. Stat. 55/1 makes it illegal for an employer to request a password or related account information from an employee or prospective employee in order to access their social media accounts.

472. The Colorado Social Media and the Workplace Law, COLO. REV. STAT. § 8-2-127, prohibits employers from requesting, suggesting, or compelling an employee or job applicant to change, submit, or disclose login information related to the person's social media site.

473. OR. REV. STAT. § 659A.330 (prohibits employers from accessing employees' private social media sites).

474. WASH. REV. CODE § 49.44.200 (bans employers from requesting user names and passwords of current or prospective employees' personal social media accounts).

accounts, and California[475] and Michigan[476] prohibit an employer from requesting an employee to access his or her personal account in the *presence* of the employer.[477] Generally, many state social media laws bar employers from requiring or even requesting that an applicant or employee disclose the login information for his or her personal social media account.[478] Other restrictions include prohibiting applicants and employees from changing the privacy settings on his or her accounts, "following" coworkers or employers, or adding either as "friends."[479] Although these laws have a common goal of protecting employee privacy and speech, they are often inconsistent and have, in turn, caused confusion for multistate employers.

2. Content Monitoring

There is a delicate balance between protecting employee speech and privacy while simultaneously protecting the reputations of employers. In *Ehling v. Monmouth*, the U.S. District Court for New Jersey found that a nonprofit hospital did not violate the Federal Stored Communications Act (SCA) or the

475. CAL. LAB. CODE § 980 (limits employers from asking employees for social media account information).

476. Michigan Internet Privacy Protection Act, MICH. COMP. LAWS ANN. §§ 37.271 *et seq*. (prohibits employers and educational institutions from accessing the social media accounts of employees, job applicants, students, and prospective students).

477. Christine Lyon and Melissa Crespo, *Employer Access to Employee Social Media: Applicant Screening, 'Friend' Requests and Workplace Investigations*, MORRISON & FOERSTER LLP (Mar. 17, 2014), http://media.mofo.com/files/Uploads/Images/140317-Employee-Social-Media.pdf.

478. *Id*.

479. *Id*.

employee's right to privacy after it used screenshots of the employee's social media page as grounds for suspension.[480] In *Ehling*, the plaintiff alleged that her employer violated the SCA by accessing her Facebook wall posts that were limited by her privacy settings to only be accessible by her "friends."[481] Although the court found that nonpublic Facebook wall posts *are* protected by the SCA, it reasoned that the employer did not violate the SCA because the employer viewed the content from a person who was "authorized" to view the posts without any coercion or pressure.[482]

Employers also face challenges by accessing employee social media accounts for other legitimate purposes such as candidate evaluations, promotions, or terminations because both state and federal laws prohibit employers from making employment related decisions based upon legally-protected characteristics such as religion, national origin, age, citizenship, sexual orientation, pregnancy or medical conditions, marital status, or other lawfully-protected (yet frowned upon) conduct.[483] For example, in *Gaskell v. Univ. of Kentucky,* the court held that an employee's

480. 961 F. Supp. 2d 659, 671 (D.N.J. 2013).

481. The employee who had become Facebook "friends" with her coworkers was terminated after one of her coworkers took screenshots of a post in which she criticized Washington, D.C., paramedics for saving the life of an 88-year-old white supremacist after he opened fire in the Holocaust museum. *Id*. at 663.

482. *Id*. at 669. Similarly, in Roberts v. CareFlite, No. 02-12-105-CV, 2012 WL 4662962 (Tex. Ct. App. Oct. 4, 2012), an employee was terminated after she publicly posted that she wanted to "slap" an unruly patient. *Id.* at *1. The employee alleged that her employer invaded her privacy by reading her posts but was unable to present any evidence that her employer invaded her privacy by terminating her based on her public posts. *Id.* at *5.

483. Melissa M. Crespo and Christine E. Lyon, *Social Media Can Be An Employer's Friend Or Its Foe*, L.A. DAILY J. (Jul. 29, 2014), *available at* http://www.mofo.com/~/media/Files/Articles/140729SocialMediaCanBe.pdf.

discriminatory failure-to-hire claim could proceed at summary judgment where the employer had knowledge of the candidate's religious faith learned through social media screening.[484]

The National Labor Relations Board (NLRB) has ruled on issues arising in the context of social media monitoring in the unionized workplace. In *Three D, LLC*, the NLRB set a high bar for employers before they can terminate employees based on online speech and determined that "liking" a post constitutes protected dialogue.[485] Two employees were terminated after their employer viewed a Facebook exchange that was highly critical of the employer. In finding for the employee, the NLRB found a key provision in the employer's social media policy to be overbroad.[486]

In another decision, the NLRB concluded that Costco was in violation of the National Labor Relations Act (NLRA) by maintaining and enforcing a rule prohibiting employees from electronically damaging the company or any employee's reputation.[487] The NLRB stated that a violation is dependent upon a showing that: (1) employees would reasonably construe the language to prohibit protected activity under Section 7 of the NLRA; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights.[488] Using this analysis, the NLRB disregarded the

484. Civ. A. No. 09-244-KSF, 2012 WL 2867630, at *7–*9 (E.D. Ky. Nov. 23, 2010).

485. Three D, LLC, 361 N.L.R.B. No. 31 (2014). The case is listed on the NLRB website as *Triple Play Sports Bar*. https://www.nlrb.gov/cases-decisions/board-decisions?volume=361&=Apply.

486. "An employer rule is unlawfully overbroad when employees would reasonably interpret it to encompass protected activities." Three D, LLC, 361 NLRB No. 31, at 7 (2014).

487. Costco Wholesale Corp. *et al*., 358 NLRB No. 106, at 1101 (2012).

488. *Id*.

employer's intent not to apply the policy to protected activity, and effectively questioned any policy that states that employees can be disciplined or fired for social media posts, stating that these policies are overbroad.[489]

SIDE BAR — WORKPLACE PRIVACY

Navigating the legal framework, policies, and best practices applicable to workplace privacy and technology in the workplace can be challenging for both employers and employees alike. Employers are well-advised to follow these best practices:

Employers should ensure that hiring practices comply with governing state technology monitoring and privacy laws. Both employers and employees should understand the restrictions imposed by applicable state privacy laws and should draft policies that are in accordance with their jurisdictional requirements.

Employers should implement strict guidelines to mitigate risks. Employers should ensure that all levels of management understand the legal and ethical guidelines imposed by their respective jurisdictions and corporate programs, and should allow for transparency about the programs in order to facilitate compliance and bolster employee trust.

Employers should provide sufficient notice about monitoring practices to employees. Both current employees and job candidates should be provided with sufficient notice about the monitoring technologies that are utilized and employers should ensure that employees are reminded when new technologies replace their current systems.

489. *Id*.

VIII. STUDENT PRIVACY

For institutions that receive federal funding, privacy protections are afforded under U.S. law to educational records, including grades, disciplinary actions, and other school information about a particular student. The following federal laws govern the privacy protections for education records.

A. Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA)[490] was enacted to protect the privacy of student education records by limiting the transferability of those records without "eligible student" or parental consent. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

1. Overview

FERPA prohibits educational entities from releasing or providing access to "any personally identifiable information in education records" without the written consent of a parent.[491] The regulation implementing FERPA provides that personally identifiable information includes:

- the student's name;
- the name of the student's parent or other family members;
- the address of the student or student's family;
- a personal identifier, such as the student's social security number, student number, or biometric record;
- other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

490. 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

491. 20 U.S.C. § 1232g(b)(2).

- other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and
- information requested by a person the school reasonably believes knows the identity of the student to which the educational record is linked.[492]

For the purposes of FERPA, the term "education records" is broadly defined as those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution, or by a person acting for such agency or institution.[493] However, an educational institution is allowed to disclose "directory information" if it has given public notice to parents of students in attendance and eligible students in attendance at the institution of: (1) the types of PII the institution has designated as directory information; (2) the right to refuse to let the institution disclose any or all of those types of information about the student; and (3) the period of time to notify the institution in writing that he or she does not want any or all of those types of

492. 34 C.F.R. § 99.3.

493. 20 U.S.C. § 1232g(a)(4)(A). The following records are not considered "education records" under FERPA: (a) campus police records; (b) employment records; (c) treatment records (i.e., health records that are created or maintained by a professional health practitioner for the purpose of treating a student, and not disclosed to anyone except those providing the treatment); (d) applicant records of those who are not enrolled in the university; (e) alumni records created by the school after the individual is no longer a student; and (f) grades on peer-graded papers before they are collected and recorded by a faculty member or other university representative.

information about the student designated as directory information.[494] In addition, educational institutions may disclose directory information of former students regardless of notice, provided that they honor valid opt-out requests made while the student was enrolled.[495]

FERPA rights initially belong to the parent/guardian of a student. When a student either turns 18 or attends an institution of post-secondary education, FERPA rights transfer from the parent to the student. At the college level, FERPA rights always belong to the student, regardless of age.

2. Consent Requirements and Exceptions

As a general rule, FERPA provides that no funds shall be made available to any educational agency or institution with a policy or practice of releasing educational records without written consent.[496] This written consent must be signed and dated by the eligible student or parent, and must indicate which records are to be released, the purpose of the release, and to whom the records are to be released.[497] The eligible student or parent may also request a copy of the records to be disclosed.[498]

---

494. 34 C.F.R. § 99.37(a). Directory information is "a type of personally identifiable information not usually considered harmful [or an invasion of privacy] if disclosed." It includes, but is not limited to, the student's name; address; telephone number; email address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance (e.g., academic years, semesters, or quarters when enrolled); degrees, honors, and awards received; and the most recent educational agency or institution attended. *Id.* at § 99.3.

495. *Id.* at § 99.37(b).

496. 20 U.S.C. § 1232g(b)(1).

497. 34 C.F.R. § 99.30.

498. *Id.* at § 99.30.

Written consent is not required, however, to release educational records to certain categories of recipients, including:[499]

- certain officials, including school officials and officials of schools where a student intends to enroll;
- accrediting organizations or organizations conducting certain types of studies;
- parents; or
- victims of certain offenses, limited to the final results of the relevant disciplinary proceeding.

In addition, disclosure can be made without consent when it is:

- in connection with financial aid applications or awards;
- to comply with a judicial order or subpoena;
- in connection with a health or safety emergency;
- in connection with a disciplinary proceeding at a postsecondary educational institution;
- related to sex offenders and the information was provided to the educational institution under applicable federal guidelines; or
- directory information.[500]

Finally, written consent is not required when the educational records have been de-identified such that all PII has been removed and the educational institution has made a reasonable determination that the student's identity is not identifiable.[501]

499. *Id.* at § 99.31(a).

500. *Id.* at § 99.31(a).

501. *Id.* at § 99.31(b).

3. Intersection with COPPA

As educational institutions increasingly begin to rely on web-based technologies for their students, notice and consent issues can arise that may have implications under the Children's Online Privacy Protection Act (COPPA). Enacted in 1998, COPPA grants the FTC the authority to govern the controls around the online collection of information from children younger than thirteen years old.[502] Acknowledging that some concerns related to this collection can arise in a classroom environment, the FTC included a section on "COPPA and Schools" in its published series of FAQs concerning the regulation.[503] In essence, the FTC advised that under certain circumstances a web-based service provider who is acting for a specific educational purpose on behalf of and at the direction of an educational institution may accept the institution's representation that consent has been obtained from the child's parent when it collects personal information.

The service provider must provide the school with all of the notices required under COPPA, and, upon request from the school, provide information concerning the type of personal information being collected and how it will be used, and give the school the opportunity to delete any provided information and/or limit its use by the service provider.[504] This exchange of information does not eliminate any notification obligations outlined under FERPA, or the Protection of Pupil Rights Amendment (PPRA), as discussed below.

---

502. 15 U.S.C. §§ 6501–6505. For additional details concerning COPPA, *see supra* Section IV.A.2.

503. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Mar. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools.

504. *Id*.

4. Right of Access

FERPA provides students with the right to access and review their education records. Once a student has issued the request, the educational institute must provide access to the records within 45 days of that request.[505] It also must respond to reasonable requests from students for explanation of the records.

Students, however, do not have the right to inspect the financial records of their parents, confidential letters of recommendation, treatment records, attorney-client privileged information, or records excluded from the definition of education records (i.e., law enforcement records). Also, when the request pertains to a record containing information about more than one student, the requesting students may access only the parts pertaining to themselves.[506]

5. Enforcement

In 2002, the Supreme Court held that FERPA does not create a private right of action that can be enforced through 42 U.S.C. § 1983.[507] Rather than file a lawsuit, parents or eligible students who wish to allege a FERPA violation may instead file a written complaint with the Family Policy Compliance Office (FPCO). This complaint must be filed within 180 days from the time when the violation was known or reasonably should have been known to the complainant, and it must provide specific allegations.

Upon initiating an investigation, the FPCO will issue a notice to the complainant and educational agency or institution involved outlining the allegations and requesting a written re-

505. 34 C.F.R. § 99.10.

506. *Id.* at § 99.12(a); 20 U.S.C. § 1232g(a)(1)(A).

507. Gonzaga Univ. v. Doe, 536 U.S. 273 (2002).

sponse from the educational agency or institution. After it completes its investigation, the FPCO will issue written findings. If a violation is found to have occurred, the FPCO may require corrective action such as policy revisions or training. The complaint is closed when the educational agency or institution has completed the corrective action.

B. Protection of Pupil Rights Amendment

The Protection of Pupil Rights Amendment (PPRA),[508] which is complementary to FERPA, was enacted to protect the rights of parents and students in the collection of student personal information by schools in connection with federally funded surveys and survey-related instructional materials. Whereas FERPA requires schools to protect the confidentiality of certain student information, the PPRA is intended to prevent schools and third parties from learning certain information about students.[509]

The PPRA protects the collection of student information in two ways:

1) It seeks to ensure that schools and their contractors make all instructional materials related to surveys, analysis, or evaluations in which their child is to participate available for inspection by parents or guardians.
2) It seeks to ensure that parents provide schools and their contractors with written parental consent of a

508. 20 U.S.C § 1232h; 34 C.F.R. Part 98.

509. The PPRA defines "student" as any elementary school or secondary school student. Thus, the PPRA does not apply to post-secondary educational institutions. 20 U.S.C. § 1232h(c)(6)(F).

minor student before the student is required to participate in any survey, analysis, or evaluation that reveals information concerning:

a) political affiliations or beliefs of the student or the student's parent;
b) mental or psychological problems potentially embarrassing to the student or the student's family;
c) sex behavior or attitudes;
d) illegal, anti-social, self-incriminating, and demeaning behavior;
e) critical appraisals of other individuals with whom respondents have close family relationships;
f) legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
g) religious practices, affiliations, or beliefs of the student or student's parent; or
h) income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).[510]

For the purposes of the PPRA, the term "instructional material" is broadly defined as instructional content that is provided to a student, regardless of its format, including printed or representational materials, audio-visual materials, and materials in electronic or digital formats. The definition does not include academic tests or academic assessments.

510. 20 U.S.C. § 1232h(b).

1. Parental Rights

The PPRA requires educational institutions that receive funding under any applicable Department of Education program to develop and adopt local policies, in consultation with parents, regarding:

- the parent's or guardian's right to inspect (and in some cases opt out of) surveys created by a third party or any instrument used in the collection of personal information before they are administered or distributed to a student, and beyond those surveys or instructional materials for which affirmative consent is required;[511]
- the parent's right to inspect any instructional material, in addition to those in federally funded programs and used as part of the educational curriculum for the student;[512]
- advance notice and an opportunity to opt out of certain non-emergency, invasive physical examinations or screenings to be administered to a student;[513] and

511. *Id.* at § 1232h(c)(1)(A)(i); *id.* at § 1232h(c)(1)(F)(i).

512. *Id.* at § 1232h(c)(2)(C)(i).

513. *Id.* at § 1232h(c)(2)(C)(iii).

- advance notice and an opportunity to opt out of the collection, disclosure, or use of personal information[514] collected from students for the purpose of marketing or for selling that information.[515]

The general notice of rights under the PPRA may include specific local policies, as described in the Model Notification of Rights Under the Protection of Pupil Rights Amendment. Notices of rights under the PPRA are available on the FPCO website.[516]

Parents are not required by the PPRA to be notified about the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions, such as:

- colleges or other post-secondary education recruitment, or military recruitment;
- book clubs, magazines, and programs providing access to low-cost literary products;

---

514. The PPRA defines "Personal Information" as individually identifiable information including:

(i) a student or parent's first and last name;

(ii) a home or other physical address (including street name and the name of the city or town);

(iii) a telephone number;

(iv) or a Social Security identification number.

Id. at § 1232h(c)(6)(E).

515. *Id.* at § 1232h(c)(1)(E).

516. Family Policy Compliance Office (FPCO), Model Notification of Rights Under the Protection of Pupil Rights Amendment (PPRA), and the PPRA Model Notice and Consent/Opt-Out for Specific Activities, are *available at* http://www2.ed.gov/policy/gen/guid/fpco/index.html, and http://www2.ed.gov/policy/gen/guid/fpco/hottopics/index.html.

- curriculum and instructional materials used by elementary schools and secondary schools;
- tests and assessments used by elementary schools and secondary schools to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students (or to generate other statistically useful data for the purpose of securing such tests and assessments) and the subsequent analysis and public release of the aggregate data from such tests and assessments;
- the sale by students of products or services to raise funds for school-related or education-related activities; and
- student recognition programs.[517]

The notification exceptions under the PPRA are not to be interpreted as preempting provisions of state law that require parental notification and do not apply to any physical examination or screening that is permitted or required under state law, including those examinations that are permitted without parental notification.[518]

2. Enforcement

Like FERPA, the PPRA provides no express private right of action. Instead, a student, parent, or guardian of a student directly affected by a violation of their rights under the PPRA may file a written complaint with the FPCO located within the Department of Education. This complaint must contain (1) specific allegations of fact that provide reasonable cause to believe that a violation has occurred, and (2) evidence of attempted resolution of the complaint at the local level (and at the state level if a

517. 20 U.S.C. 1232h(c)(4).

518. *Id*.

state complaint resolution process exists), including the names of local and state officials contacted and significant dates in the attempted resolution process.[519] The FPCO investigates each complaint that it receives to determine whether the educational institution (recipient) or contractor failed to comply with the PPRA.[520]

After receiving a complaint, the FPCO issues a written notice to the complainant and the educational institution or contractor involved that describes the substance of the alleged violation and informs the educational institution or contractor that the FPCO will investigate the complaint. The recipient or contractor may then submit a written response to the complaint.[521] After it completes its investigation, the FPCO then issues written findings and the basis for its findings. If a violation is found to have occurred, the FPCO may require that specific corrective steps be taken and provide a reasonable period of time during which the educational institution or contractor may comply voluntarily.[522] The remedies available under the PPRA if the educational institution does not voluntarily comply are limited to the termination of federal funding.[523] If a contractor fails to voluntarily comply, a notice may be issued for the contractor to (i) suspend operations or (ii) to terminate for default. If no violation is found, written notice of the decision and the basis of the decision are provided to all parties involved.[524]

519. 34 C.F.R. § 98.7.

520. *Id*.

521. *Id.* at § 98.8.

522. *Id.* at § 98.9.

523. *Id.* at § 98.10.

524. *Id*.

3. Proposed Legislation

On May 14, 2015, Senator David Vitter proposed significant amendments to section 444 of the General Education Provisions Act in an effort to improve privacy protections available to students and their parents.[525] Among other things, the proposed "Student Privacy Protection Act" seeks to strike a balance and insert language that defines "student data" with greater particularity. It also prohibits any school that receives federal funding from disseminating student data, including PII to third parties without (i) obtaining parental consent; (ii) providing 30 days' notice that the data is to be accessed and that it will only be available with consent; (iii) permitting parents to access the data; (iv) requiring that all student data be destroyed when the student is no longer a student; and (v) holding the third party liable for any violation.[526] The bill was reviewed and referred to the Committee on Health, Education, Labor and Pensions in May 2015 but has not been updated since.

C. State Laws

While the primary focus of this section has been on federal legislation concerning the privacy rights of students and protections over student personal information, it is important to note that many states have enacted or are in the process of enacting similar regulations. In 2015 alone, 14 states enacted such legislation, including Arkansas, Connecticut, Georgia, Louisiana, Maine, Maryland, Nevada, New Hampshire, North Dakota, Oregon, Texas, Utah, Virginia, and Washington.[527] Still other

525. *See* S. 1341, 114th Cong. (2015).

526. *Id*.

527. *See U.S. State Education Privacy Legislation 2015*, INT'L ASS'N OF PRIVACY PROF'LS, *available at* https://iapp.org/resources/article/u-s-state-education-privacy-legislation-2015/ (information current as of 8/7/15).

states, such as California, had previously adopted regulations concerning student privacy rights.[528] Because of the ever-evolving state of data protection regulations, it is advisable to refer to the current text of a state's statutes for the most up-to-date requirements for that given state or territory.

SIDE BAR — STUDENT PRIVACY

Institutions receiving federal or state funding must remain aware of the complex scheme of regulations designed to protect student privacy.

Parental notice and consent is often the key to proper handling of student personally identifiable information. In most instances, this right transfers to the student when he or she turns eighteen (18) years of age, or enrolls in a post-secondary institution (regardless of his/her age).

Protected material can be broadly defined. Under FERPA, "education records" is broadly defined and, with limited exception, encompasses all files and material maintained by the institution that directly relate to a student. The PPRA extends protection to personal information that includes not only traditional identifiers like social security numbers, but also survey responses that may give insight into political beliefs, religious affiliation, or sex behavior or attitudes, among other topics.

Primary educational institutions need to take care with student information handled online. To remain in compliance with COPPA, FERPA, and the PPRA, the personally identifiable information of children younger than thirteen (13) years old should only be relayed to online service providers after the institution has properly obtained consent from the child's parent and has reviewed the notifications the online service provider will provide to users of its site.

528. *E.g.*, California's Student Online Personal Information Protection Act, CAL. BUS. & PROF. CODE § 22584; *see also* CAL. EDUC. CODE §§ 49060–49083.

IX. CONCLUSION

Privacy laws have evolved considerably over the past several decades, and today there exists a complex patchwork of state and federal privacy laws in the United States. Many of these laws are esoteric, presenting significant compliance challenges for organizations, as well as confusion among a wide variety of stakeholders, from practitioners to legislators to the judiciary. It is our hope that this Primer proves to be a useful resource on privacy laws as they exist today, providing an understanding of the key U.S. privacy laws, along with their applicability and general requirements.

THE SEDONA CONFERENCE FEDERAL RULE OF CIVIL PROCEDURE 34(b)(2) PRIMER: PRACTICE POINTERS FOR RESPONDING TO DISCOVERY REQUESTS

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Drafting Team:

Brian D. Clark
Jennifer S. Coleman
Alison A. Grounds
K. Alex Khoury
Greg M. Kohn
Jenya Moshkovich
Michael J. Scimone

Editors-in-Chief & WG1 Steering Committee Liaisons:

Annika K. Martin
Martin T. Tully

Judicial Participant:

The Honorable Andrew J. Peck (ret.)

Copy Editor:

Susan M. McClain

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which any of the participants belongs, 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.

This publication may be cited as follows:

> The Sedona Conference, *Federal Rule of Civil Procedure 34(b)(2) Primer*, 19 SEDONA CONF. J. 447 (2018).

PREFACE

Welcome to the final, March 2018, version of The Sedona Conference *Federal Rule of Civil Procedure 34(b)(2) Primer*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). 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 public comment version of this Primer was published in September 2017 and stems from the December 2015 changes to Federal Rule of Civil Procedure 34(b)(2) ("Rule 34"), which were intended to address systemic problems in how discovery requests and responses traditionally were handled, and the observation that, over a year later, despite numerous articles, training programs, and conferences about the changes, their implementation had been mixed, at best. After a 60-day public comment period, the editors reviewed the public comments received and, where appropriate, incorporated them into this final version.

On behalf of The Sedona Conference, I want to thank all of the drafting team members for their dedication and contributions to this project. Team members that participated and deserve recognition for their work are: Brian D. Clark, Jennifer S. Coleman, Alison A. Grounds, K. Alex Khoury, Greg M. Kohn, Jenya Moshkovich, and Michael J. Scimone. The Sedona Conference also thanks the Honorable Andrew J. Peck for serving as Judicial Participant, and Annika K. Martin and Martin T. Tully for serving as both the Editors-in-Chief and Steering Committee Liaisons. Finally, The Sedona Conference and the Drafting Team are grateful to Karin Scholz Jenson for her exceptional efforts in developing the initial outline on which this Primer was based.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; 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
March 2018

TABLE OF CONTENTS

I. INTRODUCTION

As Chief Justice John G. Roberts observed, the changes to the Federal Rules of Civil Procedure ("Rule(s)") that became effective December 1, 2015, were intended to address systemic problems in how discovery requests and responses traditionally were handled.[1] "[O]ne change that affects the daily work of every litigator is to Rule 34,"[2] which was revised with the aim of "reducing the potential to impose unreasonable burdens by objections to requests to produce."[3] Thus, the changes to Rule 34 were part of the broader aspiration to reduce the costs and delay in the disposition of civil actions by advancing cooperation among the parties, proportionality in the use of discovery procedural tools, and early and active judicial case management.[4] The drafters of those amendments intended to address certain obstacles to securing "the just, speedy, and inexpensive determination of every action and proceeding," which in the context of Rule 34 included:

- overly broad, non-particularized discovery requests that reflexively sought all documents,[5] regardless of the relevance to the claims and defenses at issue;

1. *See* REPORT OF THE ADVISORY COMMITTEE ON FEDERAL RULES OF CIVIL PROCEDURE (June 14, 2014); 2015 YEAR-END REPORT ON THE FEDERAL JUDICIARY.

2. Fischer v. Forrest, Case No. 1:14-cv-01307, 2017 WL 773694, at *1 (S.D.N.Y. Feb. 28, 2017).

3. FED. R. CIV. P. 34 advisory committee's note to 2015 amendment.

4. *See* REPORT OF THE ADVISORY COMMITTEE ON FEDERAL RULES OF CIVIL PROCEDURE (May 2, 2014).

5. Throughout this Primer, the term "documents" is intended to include paper documents as well as electronically stored information (ESI), unless otherwise specified.

- overuse of boilerplate objections that provided insufficient information about why a party was objecting to producing requested documents;
- responses to requests that failed to clarify whether responsive documents were being withheld on the basis of objections; and
- responses that stated requested documents would be produced, without providing any indication of when production would begin, let alone completed, often followed by long delays in production.

Yet, "[d]espite the clarity of the no-longer-new 2015 Amendments," courts are still seeing "too many non-compliant Rule 34 responses" as well as non-compliant requests.[6] Many practitioners continue to rely on their prior practices; templates; boilerplate[7] requests, instructions, definitions, and objections; and forms. This failure to adapt may be caused by a lack of awareness of the changes, but is more likely caused by many practitioners who are in "wait and see" mode, hoping that a clear picture of how to implement the amended Rules emerges from the case law interpreting them. Wait no more: "It is time for all counsel to learn the now-current Rules and update their 'form' files."[8]

The Sedona Conference Working Group 1 has prepared this Rule 34(b)(2) Primer with practice pointers on how to comply with the amended Rules. The amendments to Rule 34(b)(2) en-

6. *Fischer*, 2017 WL 773694, at *3.

7. "Boilerplate" language includes "[r]eadymade or all-purpose language that will fit in a variety of documents." U.S. v. Needham, 718 F.3d 1190, 1199 (9th Cir.) (quoting BLACK'S LAW DICTIONARY (9th ed. 2009)).

8. *Fischer*, 2017 WL 773694, at *6.

courage conversation between requesting and responding parties about what is being sought and what will be produced—this Primer seeks to provide a framework for how those conversations may proceed. This Primer is not intended to be the last word on how to implement the amendments, as there is no "correct" way to do so, and new ideas and best practices are emerging every day. Rather, this Primer gathers advice and observations from: (i) requesting and responding parties who have successfully implemented them; and (ii) legal decisions interpreting the amended Rules. This Primer is focused on amendments to Rule 34(b)(2), relating to responses and objections, but should be considered together with amendments to Rule 26(b)(1), which have changed the standard for the permissible scope of discovery requests, and which are outside the focus of this Primer. Judicial opinions issued to date have given a clearer picture on how the amendments to Rule 34(b)(2) will be interpreted and implemented by the bench, and any practitioner that does not adapt their practice to incorporate these amendments does so at his or her own risk. **Appendix A** summarizes a number of cases that have addressed the specificity of requests for production, and the specificity of responses and objections to requests for production**. Appendix B** lists standing orders, checklists, and pilot programs that address discovery requests, discovery responses, and guidelines for when and how parties should confer regarding requests and responses.

II. 2015 RULES AMENDMENTS THAT IMPACT REQUESTS FOR PRODUCTION AND RESPONSES THERETO

The 2015 Amendments to Rule 34(b)(2) require the following:

- Responding parties must respond to Rule 34 Requests for Production ("RFPs") within 30 days of service or, if the request was delivered prior to the Rule 26(f) conference, within 30 days after the parties' first Rule 26(f) conference.
- Objections to RFPs must be stated with specificity.
- Responses must state whether responsive materials are being withheld on the basis of objections. Advisory Committee Note to Rule 34 states that describing the search to be conducted can satisfy the specificity requirement.
- Responses to RFPs may state that the responding party "will produce documents" but must do so within 30 days "or another reasonable time specified in the response."

III. PRACTICE POINTERS

A. Conferences by the Parties[9]

1. Early Discovery Conference

A substantive conference between the parties early in the case provides an opportunity to comply with the Rules amendments and avoid disputes about requests for productions or responses to those requests. Below are some key topics particularly relevant to Rule 34(b)(2) that should be addressed for an effective conference:[10]

---

9. Rule 26(f) specifically requires the parties to litigation to "confer as soon as practicable" for the purpose of planning for discovery and in preparation for a conference with the court under Rule 16(b). The 1993 Advisory Committee Notes to Rule 26(f) provided that "[t]he revised rule directs that in all cases not exempted by local rule or special order the litigants must meet in person and plan for discovery." FED. R. CIV. P. 26 advisory committee's note to 1993 amendment. However, in 2000, Rule 26(f) was "amended to require only a 'conference' of the parties, rather than a 'meeting,' because "geographic conditions in some districts may exact costs far out of proportion to these benefits." *See* FED. R. CIV. P. 26 advisory committee's note to 2000 amendment. The 2000 amendment allowed the court by case-specific order to require a face-to-face meeting, but did not authorize "standing" orders requiring such meetings. *Id*. Throughout this Primer, unless specified otherwise, "conference" generically refers to any occasion on which it is required or advisable for the parties to litigation to confer on discovery issues, regardless of the manner of doing so.

10. Numerous resources exist for more general information on topics to address in an effective conference, beyond those directly related to Rule 34. *See, e.g.*, Ariana J. Tadler, Kevin F. Brady & Karin Scholz Jenson, *The Sedona Conference "Jumpstart Outline": Questions to Ask Your Client & Your Adversary to Prepare for Preservation, Rule 26 Obligations, Court Conferences & Requests for Production*, THE SEDONA CONFERENCE (March 2016), https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20%22Jumpstart%20Outline%22; *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1 (2018), https://thesedonaconference.org/publication/The

- Scope of Discovery: By discussing with particularity the types of documents expected to be relevant to the claims and defenses of the parties and proportional to the needs of the case under Rule 26(b)(1), the parties can focus the discussion of discovery issues including those below.
- Location and Types of Relevant Data and Systems: By discussing likely sources of relevant documents in discovery conferences, the parties can reduce overbroad requests that lead to objections, unspecific objections which fail to identify what is being produced, and related discovery disputes.
- Possession, Custody, or Control: Parties may have legitimate bases to claim that certain data is not within their possession, custody, or control. However, it may be advantageous for the party asserting such a position to give notice to the requesting party that such a position is being taken if the data in question is clearly relevant to the claims and defenses.[11] For example, if

%20Sedona%20Principles. Also, a number of District Courts have Standing Orders/General Orders that address these topics. *See* Appendix B. The appropriate topics for discussion, as well as the level of detail required or feasible, may vary depending on the facts and nature of the specific matter.

11. *See* The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* Principle 5, 17 SEDONA CONF. J. 467 (2016), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Rule%2034%20and%20Rule%2045%20%E2%80%9CPossession%2C%20Custody%2C%20or%20Control%E2%80%9D. ("If a party responding to a specifically tailored request for Documents or ESI (either prior to or during litigation) does not have actual possession or the legal right to obtain the Documents or ESI that are specifically requested by their adversary because they are in the 'possession, custody, or control' of a third party, it should, in a reasonably timely manner, so notify the requesting party to enable the requesting party to obtain the Documents or ESI from

the complaint centers around the conduct of a particular individual who is an employee of Defendant A, and Defendant A believes it is not in possession, custody, or control of that employee's cellphone or tablet device, then Defendant A's response to requests for production may wish to provide notice of that legal position to permit the requesting party an opportunity to address that position before relevant electronically stored information (ESI) is lost, even inadvertently. Indeed, whenever a responding party does not possess that which is requested, it should simply say so up front. If the responding party does not timely raise the issue, the parties may be left in the unfortunate position of experiencing the destruction of highly relevant evidence, resulting in otherwise avoidable satellite motion practice concerning claims of spoliation.

- Phasing: The parties should discuss whether producing ESI in phases could result in cost savings or efficiencies.
- ESI Protocol: The parties should consider entering into an ESI stipulation that includes the parties' responsibilities and obligations for Rule 34 requests and responses.[12]

---

the third party. If the responding party so notifies the requesting party, absent extraordinary circumstances, the responding party should not be sanctioned or otherwise held liable for the third party's failure to preserve the Documents or ESI.").

12. *See, e.g.,* MODEL STIPULATED ORDER RE: DISCOVERY OF ELECTRONICALLY STORED INFORMATION FOR STANDARD LITIGATION (N.D. Cal. Dec. 2015), *available at* http://www.cand.uscourts.gov/eDiscoveryGuidelines.

- Privilege: The parties should consider whether they can agree on ways to identify documents withheld on the grounds of privilege or work product to reduce the burdens of such identification, such as categorical privilege logs or agreeing that certain categories of documents do not need to be logged (e.g., communications with litigation counsel, or documents created after a certain date). Also, the parties should strongly consider whether they will enter into a Fed. R. Evid. 502(d) stipulation and order to prevent the waiver of privileges and protections.
- Identification of Claims and Defenses: An impediment to a meaningful conference concerning discovery can be the lack of a formal answer to the complaint by the defendant during the pendency of a motion to dismiss, or uncertainty by the defendant as to the nature and bases for the claims asserted. If discovery responses need to be addressed notwithstanding, practical solutions include the defendant informally identifying its defenses so the parties can discuss the scope of relevant discovery, or formally filing a "protective" answer while the motion is pending.

If the parties confer regarding these issues and put an ESI plan in place early in the case, it may assist in achieving the objectives of shaping the scope of Rule 34 requests and minimizing, or even avoiding, the need for judicial involvement in discovery issues.

Of course, advance preparation by all participants is essential to an effective discovery conference. Failure to do so will undermine, if not eliminate, the ability to achieve the foregoing objectives and may breed distrust among the parties.

2. Early Delivery of Rule 34 Requests

The 2015 amendments allow for delivery of Rule 34 requests 21 days after service of the complaint.[13] According to the 2015 Advisory Committee Notes, "[t]his relaxation of the discovery moratorium is designed to facilitate focused discussion during the Rule 26(f) conference."[14] Indeed, the expectation is that "[d]iscussion at the conference may produce changes in the requests."[15] Therefore, parties may benefit from early delivery of Rule 34 requests because it affords an opportunity for the parties to informally discuss any objections before they are due or made in writing. Whether they confer as part of the Rule 26(f) process or through separate discussions, a substantive conference early in the case provides an opportunity to comply with the Rule changes and avoid discovery disputes.

If one or more of the parties exchange Rule 34 requests in advance of the Rule 26(f) conference, the parties can be more specific at the conference about potential objections to the requests, the relevance (or lack thereof) of the documents requested to the claims and defenses, the proportionality of the requests under Rule 26(b)(1), and the search the responding party is willing to conduct. Counsel should share these requests with their clients prior to the conference to help identify potential objections and the efforts necessary to make the requested production. It also will help the responding party identify objections that may be inappropriate, such as a burden objection to a request that appears burdensome on its face but may not be in fact, as well as requests that could be refined or focused to avoid objections. Finally, early requests can help narrow the focus of the preservation discussion, a topic that is now required

13. FED. R. CIV. P. 26(d)(2).

14. FED. R. CIV. P. 26 advisory committee's note to 2015 amendment.

15. *Id*.

as part of a Rule 26(f) conference. It can feel "unnatural" to have a conference about requests prior to responding to them in writing, but it is one way that parties can comply with the Rules.

3. Documentation of Resolutions Concerning Rule 34 Requests and Responses

One challenge in discovery conferences concerning Rule 34 objections and responses is summarizing the requests, objections, and proposed resolutions for numerous different requests. A sample tracking form for such discussions is provided below, and is just one example of how parties might memorialize their progress towards resolution of objections and proposed responses on a request-by-request basis at a conference.

Rule 34 Request Language	Summary of Tentative Objection(s)	Producing Party's Proposed Limitation(s) to Request	Requesting Party Response	Resolution (Describe full or partial resolution)
Request No. 1: Produce all documents relating to the Ballroom contract.	Overbroad because complaint alleges that only conduct beginning 6 years into the 8-year term of the Ballroom contract is relevant to resolving this lawsuit (*i.e., relevant events starting in 2015, but not back to 2009 when the contract was entered into*).[16]	Limit time period for request to 2015 through the present and produce responsive documents contained in the agreed-upon custodians' email and key network shares that hit on the search term "ballroom," as well as the share drive folder containing only documents about this contract, which will be reviewed for responsiveness without application of search terms.	Limit time period for request to June 2014 through the present, as there were a few communications prior to 2015 we believe are relevant. Agree that custodial data may be culled by search terms, but request that the share drive folder specific to this contract be manually reviewed.	*Resolved at 3/9/2017 discovery conference on terms listed in requesting party response.*

If agreements are made at the conference that define the scope of the requests or the production, best practices suggest the parties should memorialize these agreements in writing, such as by: (i) sending correspondence to confirm the agreements made during the conferring process regarding limitations to the scope of the original requests; (ii) serving revised discovery requests reflecting the agreements made through the conferring process regarding the agreed-upon limitations to the scope of the original requests; or (iii) supplementing the discovery responses subsequent to the conferring process by responding to the original requests as limited, as reflected in the following example:

16. This objection is provided as an example. Other objections may be appropriate.

> "Request No. 1: Produce all documents relating to the Ballroom contract."
>
> **Response to Request No. 1:** As discussed at the discovery conference on March 18, 2017, this Request is objectionable because the contract was entered into in 2009, but responding party is not presently aware of any relevant events regarding alleged non-compliance with contract terms prior to 2015. The parties agreed that responding party will review and produce responsive, non-privileged documents that hit on the search term "ballroom" in the agreed-upon custodians' email accounts and key network share folders, but the departmental share folder specific to the Ballroom contract will be manually reviewed, without search terms, for responsive materials. The agreed-upon custodians are Jane Smith, Jean Jones, and Bob Smith, the principal individuals involved in responding party's compliance with the Ballroom contract from January 2014 through the present. The production of the documents described in this response will be completed within 30 days from the date of this response.

By stating its search will be limited to a given period of time or specified sources in response to an overbroad request, the responding party is more likely to meet Rule 34's specificity requirement and is in a better position to comply with the requirement that the production be made by a certain date, because the scope of the production will be identified. This is especially true where, for example, the responding party has had the opportunity to test the search terms and/or other search parameters prior to the written response and ascertain whether the volume of data it implicates is reasonable and proportional.

When determining how to memorialize agreements reached during discovery conferences, consider what documentation is required or accepted in discovery applications before your

court. For example, if your court only allows the text of disputed discovery requests and responses to be pasted into a motion to compel, but does not allow exhibits such as post-conference letters to be attached to the motion, the parties will want to memorialize agreements by revising the affected discovery requests or responses, rather than simply putting the agreements into a letter that cannot be put before the court in the event of a dispute.

B. Requests for Production

1. Definitions and Instructions

In drafting requests for production, requesting parties should determine what is needed relative to the claims alleged or defenses raised. The requests also should be proportional to the needs of the case.[17]

Requesting parties should attempt to minimize the need for objections by avoiding boilerplate requests, instructions that exceed or contradict the requirements of the Federal Rules, definitions that are not actually used in the requests, blanket requests for "any and all documents," and documents that "refer or relate to," in order to encourage substantive responses to the requests from the producing party thereby increasing the chances that documents will be produced sooner. The following may help draft requests that comply with the amended Rules 26(b)(1) and 34:

a) To minimize objections to definitions and instructions, consider using the definitions and instructions in the federal or local rules, without elaboration.

b) Avoid overbroad definitions. For example, do not include in the definition of "You" people or entities that

17. *See* FED. R. CIV. P. 26(b)(1).

are more properly subject to discovery through Rule 45.[18]

c) Avoid overbroad instructions. For example, avoid (unless necessary) an instruction that the responding party must search deleted data, data in slack space, ESI on disaster recovery tapes, and other non-primary sources of ESI which may not be readily accessible in the normal course.[19]

d) Consider using instructions designed to reduce across-the-board objections. For example, consider including an instruction that the requests should not be

---

18. *See* The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467 (2016), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Rule%2034%20and%20Rule%2045%20%E2%80%9CPossession%2C%20Custody%2C%20or%20Control%E2%80%9D.

19. *See, e.g.*, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, Principle 8 (2018), https://thesedonaconference.org/publication/The%20Sedona%20Principles; 7TH CIRCUIT ELECTRONIC DISCOVERY COMMITTEE, PRINCIPLES RELATING TO THE DISCOVERY OF ELECTRONICALLY STORED INFORMATION, Principle 2.04(d) (Rev. 8/1/2010), http://www.discoverypilot.com/sites/default/files/Principles8_10.pdf ("The following categories of ESI generally are not discoverable in most cases, and if any party intends to request the preservation or production of these categories, then that intention should be discussed at the meet-and-confer or as soon thereafter as practicable: (1) 'deleted,' 'slack,' 'fragmented,' or 'unallocated' data on hard drives; (2) random access memory (RAM) or other ephemeral data; (3) online access data such as temporary internet files, history, cache, cookies, etc.; (4) data in metadata fields that are frequently updated automatically, such as last-opened dates; (5) backup data that is substantially duplicative of data that is more accessible elsewhere; and (6) other forms of ESI whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary course of business.").

construed to request privileged or work product documents created on or after the filing of the complaint.

e) Be thoughtful in applying across-the-board date ranges for the requests.

2. Individual Requests

Similarly, individual RFPs should be well-tailored, and not overbroad or disproportionate to the needs of the case:

a) Per Rule 26, requests must be limited to ESI that relates to the claims or defenses and be proportional to the needs of the case. Recall that the 2015 amendment to Rule 26 deleted the former language about "discovery of any matter relevant to the subject matter involved in the action" or that is "reasonably calculated to lead to the discovery of admissible evidence."

b) Per Rule 34(b)(1)(A), the requests "must describe with reasonable particularity each item or category of items to be inspected."

c) Determine whether the client has information about specific documents or types of documents in the responding party's possession, custody, or control that relate to the claims or defenses in the case; use that information to narrowly tailor requests that target those specific documents or types of documents.

d) Consider specifying subsets of documents—such as "communications." Identifying categories rather than referring broadly to "all documents" makes it easier in the meet and confer process to identify requests that can be addressed by searching particular sources, such as key custodians' email accounts.

e) Where possible, avoid beginning requests with "any and all documents and communications that refer or relate" to a particular subject (and similar preambles). Any increase in scope gained by such language is likely to be offset by wasted time spent resolving objections or narrowing the scope of the request, or by motion practice in which the request may be viewed as overbroad. Consider replacing "refer or relate" and similar language with requests for specific ESI, or with more specific terminology such as "describing," "reflecting," or "containing." In some instances, local court rules will provide specific definitions applicable to all discovery requests.[20]

f) Consider the scope of each request individually. Requests generally can be put in three categories:

   i. *Requests for specific documents:* These documents are readily identifiable, such as tax returns, a personnel file, bank records, board meeting minutes, etc. A responding party should be able to identify and produce these quickly. Bogging down requests for specific documents with the "any and all" preamble usually serves to draw objections and delay production. Instead, make the request a simple one, such as "Produce plaintiff's work performance evaluations from 2012 to 2015."

   ii. *"Sufficient to show" requests:* These requests seek documents on a topic for which you need information, but you do not need the responding party to find and produce every document

20. *See, e.g.*, S.D.N.Y. L.R. 26.3(c), *available at* http://www.nysd.uscourts.gov/rules/rules.pdf.

that contains or relates to that information. For example, if seeking the locations where the responding party did business, a request for ESI "sufficient to show all locations where Company A did business in 2012 to 2015" would be more appropriate than a request for "all ESI that reflects or relates to the locations where Company A did business." Also, consider whether an interrogatory may be a more efficient way to get the needed information.

iii. *Everything else:* This category often includes subjects on which the requesting party has limited information regarding the existence of responsive documents, but for which a comprehensive response is needed. In most cases, a discovery conference will help target the request, as the responding party has knowledge (or should be able to obtain knowledge) about the types and categories of documents that exist in the case that are in its possession, custody, or control. The amendments to Rule 1 support this type of conference. Either before or after the conference, consider ways to tailor the request or specify the documents sought, such as the following:

   a. Provide examples of document types falling within the general description. This can be a useful starting point to talk about other, related documents, and whether or not they are necessary.

   b. Consider using factual contentions raised by the responding party to define the limits of a request. For example, you

might seek "all documents concerning any disciplinary action that Defendant claims was taken concerning the Plaintiff."

c. Requests seeking "all" documents on a subject are more likely to be reasonable in scope where the documents are of a type maintained by a specific custodian, or relate to a specific topic, for example, "all documents that relate to the decision to classify the Assistant Manager position as exempt from overtime."

d. In contrast, an "any and all" request that covers a general topic, such as "any and all documents that refer or relate to Defendant's customer relationships," is virtually certain to draw objections. Unless the requesting party can articulate what the request covers, it will be difficult to sustain when challenged.

e. If, as a requesting party, you cannot see a way to narrow an "any and all" request, prepare for a conference on the topic with a list of questions that would allow you to narrow the scope of the request.

f. Information learned in a discovery conference can be used to narrow a request like the one in III(B)(2)(f)(iii)(d), *supra*, to something like, "all documents main-

tained on the Business Management Department's shared drive concerning the Acme Widgets account."

g. Consider using interrogatories when they are a more appropriate and less burdensome method to discover necessary information. For example, instead of requesting "all ESI that relates to the ACME Widgets account," consider an interrogatory that asks the responding party to list all products sold to Acme, the dates those products were sold, and prices the products were sold at.

3. Rule 26(g) Certification

Requesting parties should be mindful that the certification requirement of Rule 26(g) applies to all document requests. *See* Section III(E), *infra*, for more on the requirements of Rule 26(g).

C. Responses to Requests for Production

In drafting responses to RFPs, counsel for responding parties should meet with their clients as early as possible to determine what documents exist, what requested documents are going to be withheld and for what reasons, and what requested documents are going to be produced and when that production can be completed. This will allow the responding party to avoid using general objections and boilerplate responses that state only "responsive non-privileged documents will be produced." The following may help draft responses that comply with amended Rule 34:

1. Time to Respond

The responding party must respond in writing within 30 days after being served or, if the request was delivered under Rule 26(d)(2), within 30 days after the parties' first Rule 26(f) conference.[21] A shorter or longer time may be stipulated to or be ordered by the court.[22] However, when altering response deadlines, parties and courts should be cautious about setting a deadline that is triggered by an unfixed event—for example, a deadline that is "30 days after the parties have agreed on keywords [or some other unfixed event or action]" —because this can create an opportunity for taking advantage by slow-rolling or delaying the unfixed event such that the response deadline is never triggered. Instead, discovery response deadlines should be triggered by fixed dates or actions that are themselves subject to firm deadlines, so that parties can accurately anticipate when responses are due and can be held accountable when deadlines are missed.

The 30-day deadline in Rule 34(b)(2)(A) applies to the written response to the request for production—not the date for producing the ESI. The deadline for producing the ESI is in Rule 34(b)(2)(B): "the time specified in the request or another reasonable time specified in the response." To the extent setting dates for production is not possible for a subset of the production universe at the time the response is due (because the scope of production is still being negotiated or because additional information that is unavailable at the time of the response period is necessary to provide a definite date of production), responding parties should state the scope of production that they are willing and able to produce without objection and the specific date of such production. The parties can continue to confer on the final

21. FED. R. CIV. P. 34(b)(1)(A).

22. FED. R. CIV. P. 34(b)(2)(A).

scope of production, including any potential search terms or search methodologies (e.g., technology assisted review) for filtering ESI, and set a date for supplemental productions. These measures should be in addition to, and not in lieu of, completing specific, unobjectionable productions within a specific timeframe, and should not be used to delay or avoid deadlines.

2. General Objections

Amended Rule 34 requires that objections: (i) be stated with specificity, including the reasons for the objections; and (ii) state whether any responsive materials are being withheld on the basis of that objection.[23] Because of these requirements, general objections should be very limited.

a) General objections should be used only if the objections apply to all the document requests or are expressly incorporated by reference in the sub-set of requests to which they are being asserted to avoid repeating the objection. General objections as to form of production, time period/date range, or other global-scope objections may be listed as a general objection, but the reason for the objection still must be specified in order to facilitate a meaningful discovery conference. For example, instead of this typical general objection, "Company A objects to these Requests to the extent they are not limited in time," consider including more specificity in the general objection if it applies to all of the requests, or including the specificity in the individual responses where appropriate: "The Requests do not specify the date range for the requested production. Unless otherwise stated in the

23. *See* FED. R. CIV. P. 34(b)(2)(B)–(C).

response below, Company A will search for responsive documents between January 1, 2014, the date the contract negotiations began, and June 1, 2014, the date the contract was executed." Here are some typical general objections that may be appropriate:

i. *Privilege Objection.* Responding Party will not produce information protected from disclosure by the attorney-client privilege or the attorney work-product doctrine. If any documents are withheld from production on the basis of any such privilege, other than those excluded by the parties pursuant to the Joint Case Management Conference Statement, a privilege log will be served on the requesting party within fourteen (14)[24] days of production of documents from which such protected documents were withheld.

ii. *Confidentiality Objections.* Responding Party has documents in its possession, custody, or control that contain proprietary, trade secret, or other confidential information, which Responding Party is withholding until a Protective Order is in place. Responding Party also has various documents in its possession, custody, or control that are subject to third-party confidentiality provisions. If any documents are withheld from production on the basis of this objection, Responding Party may be able to identify such third party, begin discussions with that third party regarding disclosure of

24. The number of days required for the generation of a privilege log may vary significantly based on the volume of documents at issue.

information, and advise Requesting Party of its efforts relating to same.[25]

iii. *Overbroad*. Responding Party objects to all individual requests herein, as they do not comply with the "reasonable particularity" requirement of Rule 34(b)(1). Responding Party attempted to confer with Requesting Party on multiple occasions regarding this issue and provided case law to support its positions; however, Requesting Party advised that it disagreed and suggested that Responding Party limit the requests as it saw appropriate and respond based on said limitations. While Responding Party does not believe that this is appropriate under Rule 34, unless it does so, Requesting Party will have effectively prevented any type of meaningful response to the Request which could expose Responding Party to sanctions. Based on the foregoing, Responding Party has attempted to appropriately narrow each individual request so that it can comply with the requirements of Rule 34.

b) Boilerplate general objections, even if made out of "an abundance of caution," are not allowed. As Rule 34 makes clear, and as a growing number of courts are holding, such objections may result in a waiver of the objection or even the imposition of sanctions.[26]

---

25. Alternatively, the response might specify that Responding Party will redact or anonymize documents that contain confidential information of third parties.

26. *See, e.g.*, Fischer v. Forrest, No. 14 Civ. 01304, 2017 WL 773694 (S.D.N.Y. Feb. 28, 2017) (Any discovery response that does not comply with Rule 34's

c) A commonly used but improper boilerplate general objection includes the caveat "to the extent that" prior to describing the condition, as shown in the following example: "Company A objects to each of the requests to the extent that they are overbroad, unduly burdensome, repetitive, ambiguous, oppressive, vague, improper, and/or seek information or production of documents not relevant to the claims or defenses of any party and not reasonably calculated to lead to the discovery of admissible evidence, including documents which are remote in time and/or subsequent to the operative facts set forth in the parties' pleadings in this action." Instead, the responding party should separately identify which aspects of the RFP are objectionable and for what reasons and, if applicable, indicate which portions of the request are not objectionable. The 2015 Advisory Committee Note to Rule 34 provides examples that illustrate the concept that "[an] objection may state that a request is overbroad, but if the objection recognizes some part of the request is appropriate the objection should state the scope that is not overbroad."[27] Note that in addition to the boil-

requirement to state objections with specificity (and to clearly indicate whether responsive material is being withheld on the basis of objection) will be deemed a waiver of all objections (except as to privilege).); Liguria Foods, Inc. v. Griffith Labs, Inc., No. 14 Civ. 3041, 2017 WL 976626 (N.D. Iowa Mar. 14, 2017) (Using "boilerplate" objections to discovery in any case places counsel and their clients at risk for substantial sanctions.) By creating meaningful disincentives to the use of boilerplate objections, courts are using the Rule 34 amendments to strike at the core of the culture of discovery paranoia that has made boilerplate objections so pervasive.

27. "Examples would be a statement that the responding party will limit the search to documents or electronically stored information created within

erplate nature of this general objection, it is also problematic because "reasonably calculated to lead to the discovery of admissible evidence" has been stricken from Rule 26.

d) Another opaque general objection is: "Company A objects to the Requests to the extent they seek documents in the possession of third parties, over which it has no control." To improve this objection, the responding party would object to the specific requests that overtly seek documents from sources that are not in the responding party's possession, custody, or control. As noted earlier, it may be advantageous for the responding party to identify in the response who does have possession, custody, or control, if known to the responding party.[28]

e) Another problematic general objection is one with a "reservation of rights." Either the Rules or case law give a party a right or they do not, but reserving a right in a discovery response is not likely to create a right where none existed previously. For example: "Company A reserves all objections to the compe-

---

a given period of time prior to the events in suit, or to specified sources. When there is such an objection, the statement of what has been withheld can properly identify as matters 'withheld' anything beyond the scope of the search specified in the objection." *See* FED. R. CIV. P. 34 advisory committee's note to 2015 amendment.

28. *See* The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* Principle 5, 17 SEDONA CONF. J. 467 (2016), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Rule%2034%20and%20Rule%2045%20%E2%80%9CPossession%2C%20Custody%2C%20or%20Control%E2%80%9D.

tency, relevance, materiality, privilege, and/or admissibility of documents produced in response to the Requests." Or, "Company A's responses to the Request shall not be construed as an admission that any fact or circumstance alleged in any of the requests occurred or existed or that any responsive document exists or does not exist." These kinds of general objections, without more information about how they apply to a specific request, typically do *not* reserve any rights.

f) It would, however, be appropriate to point out and object to general instructions and definitions in RFPs that exceed what is required by the Federal Rules.

Other than the limited exceptions described above, an objection should be provided in an individual response. Either way, the objection should explain the reason it is being made.

3. Specific Responses and Objections

a) One reason that Rule 34 was revised was to address the uncertainty of what is meant by the commonly used phrase, "subject to and without waiving these objections, [responding party] will produce responsive, non-privileged documents responsive to this request."[29] Responding parties should ask themselves the following questions when determining how to respond: Does "subject to and without waiving" mean the party is withholding something? If so, what and why? Although the phrase has been part of the discovery lexicon for decades, Rule 34 and the 2015 Advisory Committee Notes explicitly require a responding party to either state what they are withholding

29. *See* FED. R. CIV. P. 34 advisory committee's note to 2015 amendment.

because of an objection or, alternatively, describe the scope of the production they are willing to make. The amended Rules require a clarification as to whether documents actually are being withheld on the basis of the objection. The Committee Notes further clarify that the withholding party is not required to specifically identify or log withheld documents and may comply with this requirement by stating the scope of what it will produce, as described in III(C)(3)(c), below.

b) When stating what is being withheld, the intention is to "alert the other parties to the fact that documents have been withheld and thereby facilitate an informed discussion of the objection."[30] Taking the direct approach is recommended, if possible: "Because the marketing department had no role in the contract negotiations and therefore its documents are not relevant to the claims or defenses in this case, Company A will not search for, collect, or produce documents from the marketing department."[31]

---

30. FED. R. CIV. P. 34 advisory committee's note to 2015 amendment.

31. *See, e.g.*, Wal-Mart Stores, Inc., et al. v. Texas Alcoholic Beverage Commission, et al., No. A-15-CV-134-RP, 2017 WL 1322247 (W.D. Tex. April 10, 2017) (where Wal-Mart found a request too broad to merit a search, but also felt there were likely to be some responsive documents somewhere in its network, and so responded that it was withholding documents on the basis of its objection, the Court found that while that may technically be accurate, it is not what the new Rules were after in adding the requirement in Rule 34(b)(2)(C) that "an objection must state whether any responsive materials are being withheld on the basis of the objection." The court suggested that a "more helpful response would have been something along the lines of 'Based on these objections, Wal-Mart has not conducted a search for responsive documents, and while it is likely that some responsive documents may exist,

c) When a responding party intends to produce a more limited scope of documents than requested, it can meet Rule 34's requirements by describing the scope of what it is willing to produce, which may include the parameters of a search for documents, such as custodians, sources, date ranges, and search terms (or search methodology).

d) Regarding the timing of document productions, a general response that "documents responsive to this request will be produced" is insufficient. Production either must be completed by the time specified in the request or another reasonable time specified in the response.[32] Here, again, responding parties should ask themselves when will responsive documents be produced? If responsive documents will be produced on a "rolling basis," what does that mean? When rolling productions are necessary, the best practice is to provide a schedule as to what will be produced and when; if that is not possible, the response at least should specify the start and end dates of the production.

e) When a responding party is willing to search for some or all of the requested documents but does not yet know if those documents exist and where, it can meet Rule 34's requirements by describing the scope of what it is willing to search for.

f) In instances where the full scope of the potential documents and the estimated time for production is not

---

Wal-Mart has not identified any such document, and is not withholding any identified document as a result of these objections.'").

32. FED. R. CIV. P. 34(b)(1)(B).

known at the time of the written responses, the responding party can provide an estimated time for substantial completion and supplement the responses to reflect additional details regarding scope and timing once known.

g) The responding party should include enough detail as necessary to support the objection, and keep in mind that its objection may have to be justified to the court. Objections on the grounds that a request is vague or ambiguous should explain why, and should be based on a logical interpretation of what is being requested. For example, if a request broadly seeks "any and all documents related to policies" and an objection is on the grounds that it is vague, overly broad, and burdensome, explain why each objection applies and carve out what will be produced: "Responding Party objects to producing any and all documents related to policies on the grounds that the term 'policy' is vague and not limited to the specific claims and defenses raised in this dispute. Moreover, as written, the request could be read to seek all drafts and communications about policies, including emails from thousands of the company's employees who routinely receive emails with updated policies and updates. Searching for emails relating to any and all policies of the company would require an extensive search of all employee emails and would not likely generate information relevant to the claims or defenses in this matter. Responding party will produce final copies of its loan origination policies from 2012–2014 from a network drive used by its Compliance

> Department to maintain all historical final policies related to loan originations. Responding Party objects to producing any drafts or emails related to policies."

4. Rule 26(g) Certification

Responding parties should be mindful that the certification requirement of Rule 26(g) applies to all responses and objections to document requests. *See* Section III(E), *infra*, for more on the requirements of Rule 26(g).

D. Court Involvement

While it is best to resolve discovery disputes without court involvement, that cannot always be accomplished. In motion practice regarding the scope of discovery requests, the parties should give the court something to work with. Courts are not likely to engage in a wholesale rewriting of discovery requests and may be hesitant to strike a request in its entirety. If either the requesting or responding party believes that there is an appropriate limitation or structure to a request that makes sense, they should identify that limitation or change in structure for the court. This will allow the court to determine what scope or construction should be considered, and will inform the court with its questions relating to or its ruling on any motion filed. An example is provided below:

> *Original Request:* Produce all documents relating to all contracts entered into by the parties.
>
> *Proposed Limited Request:* Produce any contracts entered into between the parties from 2013 to December 31, 2016.

Although the responding party is not under any affirmative duty to rewrite the requests, it may save significant time and expense if it makes a reasonable proposal for an alternative request, instead of just saying "No." Also, reasonable proposals

inform the court of what information a party believes is appropriate, and begins the discussion between the parties and the court that should inform the at-issue discovery and future discovery regarding scope and time frame. Absent the proposed scope and time limitation, the court may not have the information needed to participate in a substantive discussion regarding the discovery motion, which could result in unsatisfying rulings for all parties involved.

Another consideration for court involvement beyond motion practice is the use of informal discovery conferences to resolve disputes, as suggested by Rule 16(b)(3)(B)(v). Parties should consider requesting that the Court include a provision for such informal conference in the Rule 16(b) scheduling order.

E. Requesting and Responding Parties' Obligations under Rule 26(g)

Attorneys failing to comply with the amended Federal Rules could face sanctions under Rule 26(g). Rule 26(g) requires that the requesting and responding attorneys certify that their requests, responses, and objections are consistent with the Rules and are "not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation" and are "neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action."[33]

33. FED. R. CIV. P. 26(g): SIGNING DISCLOSURES AND DISCOVERY REQUESTS, RESPONSES, AND OBJECTIONS

(1) *Signature Required; Effect of Signature*. Every disclosure under Rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney of record in the attorney's own name—or by the party personally, if unrepresented—and must state the signer's address, e-mail address, and telephone

According to the language of the rule, Courts "must" impose Rule 26(g) sanctions against requesting parties who seek disproportionate discovery or upon responding parties for attempting to cause unreasonable delay or needlessly increase the cost of litigation without substantial justification.

---

number. By signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry:

(A) with respect to a disclosure, it is complete and correct as of the time it is made; and

(B) with respect to a discovery request, response, or objection, it is:

(i) consistent with these rules and warranted by existing law or by a non-frivolous argument for extending, modifying, or reversing existing law, or for establishing new law;

(ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and

(iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.

(2) *Failure to Sign.* Other parties have no duty to act on an unsigned disclosure, request, response, or objection until it is signed, and the court must strike it unless a signature is promptly supplied after the omission is called to the attorney's or party's attention.

(3) *Sanction for Improper Certification.* If a certification violates this rule without substantial justification, the court, on motion or on its own, must impose an appropriate sanction on the signer, the party on whose behalf the signer was acting, or both. The sanction may include an order to pay the reasonable expenses, including attorney's fees, caused by the violation.

APPENDIX A:
CASES INTERPRETING THE SPECIFICITY REQUIREMENTS IN RULE 34 AND STATE LAW EQUIVALENTS

Specificity of Requests for Production

1. ***Caves v. Beechcraft Corp.*, Case No. 15-CV-125-CVE-PJC, 2016 WL 355491 (N.D. Okla. Jan. 29, 2016)** (denying motion to compel and sustaining defendant's objections to: (i) document requests seeking "any and all" testimony concerning any "other litigation" as "clearly objectionable" because "[n]either Defendants nor the Court should have to guess what Plaintiff is really seeking. Nor is it the Court's job to redraft Plaintiff's discovery requests;" and (ii) document request for "all correspondence between Defendants and any and all regulatory agencies" because such a request "does not identify with reasonable particularity what is being sought" and was unlimited in temporal scope).

2. ***In re Bard IVC Filters Prod. Liab. Litig.*, 317 F.R.D. 562, 2016 WL 4943393 (D. Ariz. Sept. 16, 2016)** (rejecting request for communications between defendants' foreign affiliates and foreign regulators based on their "marginal relevance" and clarifying that the proper scope of discoverability is whether evidence is "'relevant to any party's claim or defense,' not whether it is 'reasonably calculated to lead to admissible evidence'").

3. ***Loop AI Labs, Inc. v. Gatti*, Case No. 15-cv-00798-HSG (DMR) (No Slip Copy Reported in Westlaw) (N.D. Cal. May 6, 2016) (Re: Dkt. Nos. 592, 594)** (denying plaintiff's motion to compel responses to several RFPs because they were "incurably overbroad").

4. ***Loop AI Labs, Inc. v. Gatti*, Case No. 15-cv-00798-HSG (DMR), 2016 WL 2342128 (N.D. Cal. May 3, 2016) (Re: Dkt.**

Nos. 547, 518) (denying defendant's motion to compel supplemental production to several RFPs because "[w]hile the RFP[s] seek[] documents related to [the parties'] allegations, [they are] overbroad and unbounded by subject matter or temporal scope").

5. ***Morgan Hill Concerned Parents Assoc. v. Cal. Dep't of Ed.*, No. 2:11-cv-3471-KJM-AC, 2016 WL 304564 (E.D. Cal. Jan. 26, 2016)** (denying motion to compel response to document request for documents "constituting, describing or relating to" various categories, including the actual documents sought in discovery, as such requests are too broad and vague to compel production, especially where a large number of documents and a large volume of electronically stored information is involved; and, denying motion to compel document request for "all documents constituting or describing communications between various entities relating to any of the other documents sought," as being "overbroad on its face").

6. ***Vailes v. Rapides Parish School Bd.*, Civil Action No. 15-429, 2016 WL 744559 (W.D. La. Feb. 22, 2016)** (denying motion to compel RFP that asks defendants to provide "[a] copy of all records, reports, writings, notes, documents, memoranda, emails, photographs, videotapes, text messages, tape recordings, or other statements, recordings, or communications in response to Plaintiff's First Set of Interrogatories directed to each and every Defendant," because such a request "does not meet Rule 34's reasonable particularity standard").

7. ***Ye v. Cliff Veissman, Inc.*, No. 14-cv-01531, 2016 WL 950948 (N.D. Ill. Mar. 7, 2016)** (document request for "[a] full archive of any documents, notes, messages, photographs, or any other information from any social media account held

by the decedent [and by any next of kin of the decedent], including an archive from any Facebook account . . . from 2007 until the date of [the decedent's] death [in 2013]" was not reasonably tailored to a reasonable time period before the death of plaintiff's decedent or to content that is relevant to a claim or defense in the case; however, offering defendant opportunity to reformulate their request because "[t]here is no dispute that *some* of the decedent's and her next of kin's social media profiles contain information that is relevant to a claim or defense in this lawsuit") (emphasis in original).

Specificity of Objections

1. ***Arrow Enterprise Computing Solutions, Inc. v. BlueAlly, LLC*, No. 5:15-CV-00037-FL, 2016 WL 4287929 (E.D.N.C. Aug. 15, 2016)** (deeming defendants' objections waived because they "are nothing more than boilerplate objections: they fail to specify why the requested documents are not relevant to a party's claim or defense and not proportional to the needs of the case. Instead, they simply regurgitate the amended version of Rule 26(b)(1) of the Federal Rules of Civil Procedure"; yet applying the incorrect standard for relevancy ("reasonably calculated to lead to the discovery of admissible evidence").

2. ***Brown v. Dobler*, No. 1:15-cv-00132, 2015 WL 9581414 (D. Idaho Dec. 29, 2015)** (noting "[d]efendants utterly failed to answer any question, and instead simply cut and pasted the same or similar objection in response to each discovery request," but also "some of Plaintiff's requests are overly broad, and [the court] will not require Defendants to . . . produce documents seeking clearly irrelevant information or information outside a reasonable period of time," and holding defendants may limit their responses in accordance with ex-

amples given in the Court's Order, and "advising" defendants to review amended Fed. R. Civ. P. 34(b), which requires the objecting party to state whether responsive materials are being withheld on the basis of the objection, and permit inspection of any other documents not subject to the objection).

3. ***Douglas v. Kohl's Department Stores*, Case No: 6:15-cv-1185-Orl-22TBS, 2016 WL 1588651 (M.D. Fla. Apr. 20, 2016)** (overruling defendant's general objections, which "do not explain why the requests are irrelevant, overbroad, or otherwise objectionable" under amended Fed. R. Civ. P. 34(b)(2)(B), and awarding legal expenses, including attorney's fees, to prosecute the motion to compel for, among other reasons, failing to comply with amended Fed. R. Civ. P. 34(b)(2)(C) by stating whether responsive materials are being withheld on the basis of a privilege).

4. ***FDIC, as Receiver for AmTrust Bank Plaintiff, v. Ark-La-Tex Financial Services, LLC d/b/a Benchmark Mortgage*, Case No. 1:15 CV 2470, 2016 WL 3460236 (N.D. Ohio June 24, 2016)** (awarding attorney's fees, in part, because plaintiff's responses to RFPs "are all made subject to its sixteen general objections and do not make clear which specific objection or objections each response relies on," and instructing, "Going forward . . . the parties may not rely on a laundry-list of general objections for withholding documents but may instead only withhold documents based on specific objections," because the purpose of the amendment to Fed. R. Civ. P. 34(b)(2)(c) is to "end the confusion that frequently arises when a producing party states several objections and still produces information, leaving the requesting party uncertain whether any relevant and responsive information has been withheld on the bases of the objections").

5. ***Fischer v. Forrest*, No. 14 Civ. 01304, 2017 WL 773694 (S.D.N.Y. Feb. 28, 2017)** (Any discovery response that does

not comply with Rule 34's requirement to state objections with specificity (and to clearly indicate whether responsive material is being withheld on the basis of objection) will be deemed a waiver of all objections (except as to privilege).).

6. ***Grodzitsky v. Am. Honda Motor Co.*, No. CV121142SVWPLAX, 2017 WL 2616917, at *4 (C.D. Cal. June 13, 2017)** (Where responding party objected, but despite repeated requests from requesting party refused to indicate whether documents were being withheld on the basis of objections, Court applied amended Rule 34 and ordered responding party to provide, within 14 days, "a declaration signed under penalty of perjury by a corporate officer or director attesting that . . . no documents or information have been withheld on the basis of the objections . . . , if indeed that is the case," or alternatively, if documents have been withheld, "then [responding party] must so state, and specify the withheld documents.").

7. ***In re: Adkins Supply, Inc., Ries v. Ardinger*, Case No. 11-10353-RLJ-7, Adversary No. 14-01000, Civil Action No. 1:14-CV-095-C, 2016 WL 4055013 (U.S. Bankr. Ct., N.D. Tex. Jul. 26, 2016)** (Defendants responded to 41 of 42 RFPs with general objections. In response to a motion to compel, the court overruled the general objections and ordered production within 15 days stating, "Broad-based, non-specific objections are almost impossible to assess on their merits, and fall woefully short of the burden that must be borne by a party making an objection to an interrogatory or document request. . . . Federal courts are quick to express their disdain for such tactics by waiving all general objections.").

8. ***Kissing Camels Surgery Center, LLC v. Centura Health Corp.*, No. 12-cv-03012, 2016 WL 277721 (D. Colo. Jan. 22, 2016)** (noting many of defendants' RFPs "are improper on

their face as omnibus requests," but also "Plaintiffs' boilerplate objections are no better. . . . As far at the court can tell, Plaintiffs fail to provide any specificity to their objections, including their objection that they have already produced responsive documents").

9. ***Liguria Foods, Inc. v. Griffith Labs, Inc.*, No. 14 Civ. 3041, 2017 WL 976626 (N.D. Ia. Mar. 14, 2017) (N.D. Iowa March 14, 2017)** (Using "boilerplate" objections to discovery in any case places counsel and their clients at risk for substantial sanctions.).

10. ***Loop AI Labs, Inc. v. Gatti*, Case No. 15-cv-00798-HSG (DMR) (No Slip Copy Reported in Westlaw) (N.D. Cal. May 6, 2016) (Re: Dkt. Nos. 592, 594)** (RFP responses "which do not state whether any responsive materials are being withheld on the basis of objections" are improper; ordering supplementation within seven days to comply with amended Rule 34(b)(2).).

11. ***Moser v. Holland*, No. 2:14-cv-02188-KJM-AC, 2016 WL 426670 (E.D. Cal. Feb. 3, 2016)** (granting plaintiff's motion to compel because "(1) defendants do not oppose it, and (2) defendants' initial responses included only boilerplate objections barred by Rule 33 and 34," and awarding sanctions of $1,998.00 for the cost to bring the motion stating, "The court sympathizes with defense counsel's difficulties in communicating with [his client], but this does not excuse delaying compliance with discovery obligations until the discovery period is almost over and plaintiff has no choice but to incur the costs of filing a motion to compel").

12. ***Rosalez Funez v. E.M.S.P., LLC*, Civil Action No. 16-1922, 2016 WL 5337981 (E.D. La. Sept. 23, 2016)** (without citing amended Rule 34, striking defendants' general objections to plaintiff's requests for production).

13. ***Rowan v. Sunflower Elec. Power Corp., Case No. 15-cv-9227-JWL-TJJ*, 2016 WL 3743102 (D. Kan. July 13, 2016)** (Defendant's response to plaintiff's RFPs which stated "the limits that controlled its search for responsive documents" complied with amended Rule 34: "[T]he Advisory Committee's note makes clear that [defendant's] response are sufficient to put Plaintiff on notice that [defendant] withheld documents in connection with its objection. Rule 34 does not require [defendant] to provide a detailed description or log of the documents withheld.").

14. ***Vilia Polycarpe v. Seterus, Inc.*, No. 6:16-cv-1606-Orl-37TBS, 2017 WL 2257571 (M.D. Fla. May 23, 2017)** (overruling "general objections" and boilerplate objections that requests were "vague" and "ambiguous" and finding that responding to discovery "subject to" or notwithstanding" objections "preserves nothing and wastes the time and resources of the parties and the court").

15. ***Wal-Mart Stores, Inc. v. Texas Alcoholic Beverage Commission*, No. A-15-CV-134-RP, 2017 WL 1322247 (W.D. Tex. April 10, 2017)** (Where Wal-Mart found a request too broad to merit a search, but also felt there were likely to be some responsive documents somewhere in its network, and so responded that it was withholding documents on the basis of its objection, the Court found that while that may technically be accurate, it is not what the new Rules were after in adding the requirement in Rule 34(b)(2)(C) that "an objection must state whether any responsive materials are being withheld on the basis of the objection." A more helpful response would have been something along the lines of, "Based on these objections, Wal-Mart has not conducted a search for responsive documents, and while it is likely that some responsive documents may exist, Wal-Mart has not identified any

such document, and is not withholding any identified document as a result of these objections.").

16. ***Wesley Corp. v. Zoom T.V. Prods., LLC*, 2018 WL 372700, No. 17-100212018 (E.D. Mich. Jan. 11, 2018)** (granting sanctions for boilerplate objections, condemning the use of boilerplate objections, and noting that "an objection that does not explain its grounds (and the harm that would result from responding) is forfeited," but giving responding party the opportunity to amend its responses (citing additional cases)).

APPENDIX B: STANDING ORDERS, GUIDELINES, AND CHECKLISTS REGARDING REQUESTS FOR PRODUCTION AND RESPONSES TO THOSE REQUESTS

Several districts have Standing Orders/General Orders concerning the topics that should be specifically addressed in a discovery conference. Some examples are provided below:

- Northern District of California's Standing Order for all Judges of the Northern District of California; Contents of Joint Case Management Statement; Guidelines for the Discovery of Electronically Stored Information; Checklist for Rule 26(f) Meet and Confer Regarding Electronically Stored Information; and Model Stipulated Order Re: Discovery of Electronically Stored Information for Standard Litigation, *available at* http://www.cand.uscourts.gov/eDiscoveryGuidelines.
- District of Colorado's Checklist for Rule 26(f) Meet-and-Confer Regarding Electronically Stored Information, *available at* http://www.cod.uscourts.gov/CourtOperations/RulesProcedures/ElectronicDiscoveryGuidelinesandChecklist.aspx.
- 7th Circuit Electronic Discovery Pilot Program Principles Relating to the Discovery of Electronically Stored Information and Model Standing Order Relating to the Discovery of Electronically Stored Information, *available at* http://www.discoverypilot.com/.
- Northern District of Georgia Standing Order: Guidelines to Parties and Counsel in Cases Proceeding Before The Honorable Amy Totenberg, *available at* http://www.gand.uscourts.gov/sites/default/files/at_case_guidelines.pdf.

- Local Rules, Forms and Guidelines of United States District Courts Addressing E-Discovery Issues, *available at* https://www.ediscoverylaw.com/local-rules-forms-and-guidelines-of-united-states-district-courts-addressing-e-discovery-issues/.

THE SEDONA CONFERENCE COMMENTARY ON BYOD: PRINCIPLES AND GUIDANCE FOR DEVELOPING POLICIES AND MEETING DISCOVERY OBLIGATIONS

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Drafting Team:

Andrea D'Ambra
Emily Fedeles
Katelyn Flynn
Ross Gotler
Peter B. Haskel
Heather Kolasinsky
Mark Michels
Jessica C. Neufeld
Matthew Prewitt
Lauren E. Schwartzreich
Ryan Wasell

Drafting Team Leaders:

Alitia Faccone
David Moncure

WG1 Steering Committee Liaisons:

Dean Kuckelman
Ronni D. Solomon

Copy Editor:

Susan M. McClain

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of The Sedona Conference Working Group 1. 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 BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495 (2018).

PREFACE

Welcome to the final, May 2018, version of The Sedona Conference *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). 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 public comment version of this Commentary was published in January 2018 and stems from the increasing practice of Bring Your Own Device (BYOD), where organizations permit or encourage workers to use their own personal devices to access, create, and manage organization information. After a 60-day public comment period, the editors reviewed the public comments received and, where appropriate, incorporated them into this final version.

BYOD is often accomplished through a BYOD program that includes formal or informal rules and guidelines. This Commentary is designed to help organizations develop and implement workable—and legally defensible—BYOD policies and practices. This Commentary also addresses how creating and storing an organization's information on devices owned by employees impacts the organization's discovery obligations.

On behalf of The Sedona Conference, I want to thank all of the drafting team members for their dedication and contributions to this project. Team members that participated and deserve recognition for their work are: Andrea D'Ambra, Emily Fedeles, Katelyn Flynn, Ross Gotler, Peter B. Haskel, Heather Kolasinsky, Mark Michels, Jessica C. Neufeld, Matthew Prewitt,

Lauren E. Schwartzreich, and Ryan Wasell. The Sedona Conference also thanks Alitia Faccone and David Moncure for serving as the Drafting Team Leaders, and Dean Kuckelman and Ronni D. Solomon for serving as Steering Committee Liaisons.

In addition, we encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; 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
May 2018

TABLE OF CONTENTS

I. INTRODUCTION

A. The Growth of BYOD

Mobile computing has obscured the once distinct boundaries between the workplace and private life. Twenty years ago, when an organization hired a new employee, it assigned the employee a desktop computer and a landline phone. Now, either as part of cost-cutting efforts or to accommodate worker preferences, organizations are permitting or encouraging workers to use their own personal devices to access, create, and manage their information—often after hours and outside the office. This practice is commonly referred to as "Bring Your Own Device" or "BYOD," and is often accomplished through a BYOD program that includes a BYOD policy and practices. Those BYOD programs may *require* employees to use their own devices to conduct the organization's business. The devices that are owned and used by the employees to access the organization's emails and documents typically include smartphones and tablet computers, but can also include personal laptops or desktops that access organization information through virtual private networks (VPNs) or other remote access technologies. This Commentary addresses how creating and storing the organization's information on devices that are owned by the employee impact the organization's discovery obligations and security goals.

Several factors have driven the rise of BYOD programs in recent years. For example, today's rapid technological developments in mobile technology motivate workers to purchase their own sophisticated devices rather than wait for their employer's information technology (IT) upgrade program. And workers purchase those devices with the expectation that they can use them for both personal and business purposes. Also, some organizations have adopted a BYOD policy so they do not have to pay for the devices, but many have found that this just shifted

IT expenditures from device purchases to software intended to protect and manage data on those devices.

Another factor driving BYOD adoption is advances in device security, which has made some organizations more comfortable with permitting access to sensitive data from employees' personal mobile devices. Security measures common to today's mobile devices may greatly reduce the risk that an employee's lost device will expose organization emails or other proprietary data. Mobile device management (MDM) software can be used to require security authentication and to segregate personal information from the organization's data. MDM software also lets organizations remotely wipe the device if it is lost or stolen.

B. The Scope of These Principles and Commentary

This Commentary applies specifically to mobile devices that employees "bring" to the workplace. It does not address all of the programs that govern employees' use of mobile computing devices, such as:

- BYOA (Bring Your Own Access—where employees provide their own wireless access to an organization's systems usually though mobile hotspots);
- BYOE (Bring Your Own Encryption—a cloud computing security process where employees use their own encryption software and encryption keys to access a cloud-based organization system);
- BYOI (Bring Your Own Identity—where employees utilize third-party systems (usually social networking sites) as their credentials for accessing organization systems, e.g., "login using Facebook");
- BYON (Bring Your Own Network—where employees create their own personal network instead of utilizing the organization's network); or

- BYOW (Bring Your Own Wearable—where employees utilize wearable technology such as Apple watches to access organization systems or perform certain job functions).

Furthermore, this Commentary does not specifically address programs where the employer provides the mobile device, or programs where employees can select a device from an authorized provider and then get reimbursed by the organization for the cost of either the device or monthly service, or both. However, many of the concepts discussed in this Commentary apply to any program that results in business information being created and stored outside of the office or the organization's servers.

Additionally, although this Commentary focuses on organizations, the discovery obligations for unique, relevant, and proportional electronically stored information (ESI) on mobile devices applies to organizations and individuals alike.

C. The Structure and Purpose of this Commentary

This Commentary begins with five principles related to the use of BYOD programs and continues with commentary for each. The first two principles and related commentary address determining whether a BYOD program is the right choice for an organization, followed by basic information governance requirements for BYOD—security, privacy, accessibility, and disposition—from the perspective of both domestic and global organizations. Against this backdrop, the principles and commentary then turn to preparing for and responding to discovery obligations under the prevailing U.S. approach to discovery.

There is no one-size-fits-all BYOD for every organization. While recognizing that BYOD is not viable for some organizations, this Commentary is cautiously optimistic that careful

planning and implementation can substantially reduce the risks associated with BYOD for many organizations. The principles encourage parties in litigation and investigations to approach BYOD discovery in a manner that both respects and rewards organizations that engage in proactive, responsible BYOD management.

This Commentary embraces a forward-looking approach to BYOD as a permanent trend that is driven by IT's transformation of both the workplace and society as a whole. This Commentary seeks to provide guidance to organizations on developing and implementing an approach to BYOD that meets the specific needs of the organization and addresses security, privacy, accessibility, and litigation. Organizations that responsibly pursue these goals should be able to proceed with confidence that their reasonable efforts will be respected by courts and will not be undermined by disproportionate discovery burdens.

D. Evaluating Whether to Allow BYOD, and How to Develop a BYOD Program

Principles 1 and 2 are designed to help guide an organization in deciding: (1) whether to allow (or even require) BYOD; and (2) how to develop and implement a BYOD program. Some organizations may find that BYOD is not suitable at all, while others may decide to adopt BYOD for only a portion of their personnel. This threshold decision should be based on the specific needs and resources of each organization. Among the relevant factors an organization should consider are the:

- impact that a BYOD program would have on the costs and risks of discovery;
- sensitivity of the information that would be accessed or stored on the devices;

- organization's legal obligations to restrict disclosure or use of the data;
- ability of the organization to exercise practical and legal control over the data;
- available technology for maintaining data security;
- receptiveness of BYOD users to usage restrictions; and
- in-house resources for user training and support.

For most organizations, BYOD will require balancing competing considerations of data access, security, privacy, cost, and the impact on discovery. Organizations should balance the privacy interests of individuals and the organization's own business needs and legal obligations. Even where an organization has a clear right to access and use the personal information of its employees, it should carefully consider its legal obligations.

If the organization decides to allow BYOD, it should have a policy that tells its employees what the rules are regarding the access, use, and storage of the organization's data on employee-owned devices. Otherwise, employees are left to guess at what is acceptable, and the organization subjects itself to unnecessary cost and risk.

E. Discovery of ESI from BYOD

Principles 3 and 5 address discovery obligations, and Principle 4 explains that organizations likely to be subject to those discovery obligations should consider discovery preparedness when creating BYOD programs. This preparedness should include a policy and practices that limit or prevent unique ESI from being stored on the device. As used in this Commentary, "discovery" includes preservation, collection, review, and production of ESI for litigation or government investigations.

More specifically, Principle 3 explains that relevant ESI on employee-owned devices may be subject to discovery—like all other ESI. Parties cannot ignore their discovery obligations merely because the ESI is on a device that is mobile or owned by an employee. Conversely, Principle 5 explains that ESI that is not relevant or not unique is not subject to discovery from employee-owned devices. In addition to relevance, there are three threshold issues that require special consideration when determining whether ESI on employee-owned devices is subject to discovery: (1) whether the organization has possession, custody, or control over the ESI; (2) whether the ESI is unique or duplicative of other ESI that is more readily accessible; and (3) whether discovery of the ESI is proportional.[1] Although these concepts have broader application beyond BYOD, in this Commentary, we address them solely in the context of ESI on employee-owned devices. We also provide examples and circumstances where courts have and have not found ESI to be discoverable.

1. Proportionality, and possession, custody, and control, are the subjects of two recent Sedona publications: The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141 (2017); The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467 (2016).

II. BYOD PRINCIPLES

Principle 1: Organizations should consider their business needs and objectives, their legal rights and obligations, and the rights and expectations of their employees when deciding whether to allow, or even require, BYOD.

Principle 2: An organization's BYOD program should help achieve its business objectives while also protecting both business and personal information from unauthorized access, disclosure, and use.

Principle 3: Employee-owned devices that contain unique, relevant ESI should be considered sources for discovery.

Principle 4: An organization's BYOD policy and practices should minimize the storage of—and facilitate the preservation and collection of—unique, relevant ESI from BYOD devices.

Principle 5: Employee-owned devices that do not contain unique, relevant ESI need not be considered sources for discovery.

III. COMMENTARIES TO BYOD PRINCIPLES

Principle 1: Organizations should consider their business needs and objectives, their legal rights and obligations, and the rights and expectations of their employees when deciding whether to allow, or even require, BYOD.

Comment 1.a. Organizational factors to consider include the organization's workforce, size, and technical support.

Organizations should consider numerous organizational factors before adopting a BYOD policy, beginning with an assessment of the benefits of BYOD to employees and the organization along with the risks of allowing BYOD. An organization should assess the role of the individual employee within the organization and whether some or all of its employees would benefit from mobile connectivity and access to organization systems beyond the confines of the organization's offices. Some employees may welcome the flexibility and convenience of BYOD, while others may view it as an infringement on work/life balance or an unfair expense imposed by the employer. For many types of workers, mobile access may provide only slight benefit while substantially increasing the risks to the organization. For example, an organization employing cashiers in a retail establishment may find little benefit from giving those cashiers access to the organization's systems when away from their work station (indeed, such access could compromise financial controls). The interests of that organization may be best served by prohibiting BYOD. Conversely, a retail store manager may benefit herself and the organization by being able to access email remotely by mobile device or home computer and quickly respond to emergency situations arising outside normal working hours.

An organization should also assess the types of information that may be accessed by employees who participate in a BYOD program. Some employees may use information that is so highly sensitive that the organization may not want to risk letting them have BYOD access to that information. The organization should consider allowing BYOD for some types of information but prohibiting it for other types of information.

An organization's size and ability to absorb internal IT costs may factor into the decision whether to adopt BYOD. The larger the scale of a business and the more employees who need mobile connectivity, the more attractive a BYOD program may initially appear because the organization can avoid paying for thousands of mobile devices. However, even those organizations that do not pay for mobile devices incur costs associated with BYOD, for example the costs of implementing mobile device management (MDM) software, providing the requisite technical support to assist users in accessing organization systems, and ensuring appropriate security measures are in place.

An organization should also consider the consequential or hidden costs associated with building an infrastructure that can support a BYOD program. In some cases, the risks and the costs may offset or exceed any savings the organization expects to enjoy from adopting the program. For example, organizations that are parties to litigation may incur additional discovery costs to collect, review, and produce ESI from employee personal devices to the extent the information is relevant and unique, a distinction discussed further in Principles 3 and 5. Discovery burdens may be particularly onerous if an organization's operations span a large geographic area, and the unique, relevant ESI contained on the devices necessitate collection or imaging of such devices in multiple locations. The devices may need to be shipped to a vendor or the vendor may need to go onsite. Onsite mobile device acquisition where the devices are

geographically dispersed can be costly, requiring either multiple vendors to cover each location, or the added cost of travel by a single vendor to multiple locations. Shipping devices is no panacea. The loss of use while a device is being shipped for collection—and providing a temporary substitute device—can also increase costs and cause business interruption. These costs and challenges can become compounded when an organization's operations include jurisdictions with strict data privacy regulations.

Companies should also consider whether they have adequate in-house (or outsourced) technical support to assist employees with accessing organization systems through MDM software, or otherwise. The organization's technical or litigation support group should be able to implement appropriate security protocols to protect against intrusion into organization systems through mobile device malware[2] or operating system vulnerabilities.[3]

In the case of litigation or regulatory disclosure requirements (including public records requests for government employers), an organization's litigation support should also be prepared to identify, secure, and work with appropriate service providers, as needed, to facilitate defensible collection of ESI from BYOD devices that contain unique, relevant information.

Various departments within an organization, including Finance, Human Resources (HR), Information Governance (IG),

2. *See, e.g.*, Leon Spencer, *16 million mobile devices hit by malware in 2014: Alcatel-Lucent*, ZDNET (Feb. 13, 2015), http://www.zdnet.com/article/16-million-mobile-devices-hit-by-malware-in-2014-alcatel-lucent.

3. *See, e.g.*, Don Reisinger, *Most Android phones at risk from simple text hack, researcher says*, CNET (July 27, 2015), http://www.cnet.com/news/researcher-finds-mother-of-all-android-vulnerabilities; Jose Pagliery, *The text you never want to get on your iPhone*, CNN MONEY (May 28, 2015), http://money.cnn.com/2015/05/27/technology/iphone-text-message-hack.

Information Technology (IT), Legal/Compliance, and Security should work collaboratively to discuss these considerations and develop a BYOD policy, procedures, training, and enforcement programs. *See* Appendix A, *infra*, describing the various roles and questions for stakeholders from these departments.

Comment 1.b. Legal factors to consider include limitations on the organization's ability to access data on the device.

Organizations should understand the legal limitations on their ability to access ESI on an employee-owned device, which may vary by jurisdiction. For example, data protection laws, labor laws, and other laws and policies (e.g., Works Council rights, bargaining agreements, and telecommunications laws) can delay or even prohibit employer demands to access ESI that exists on employee personal devices.

How an organization will obtain access to information on the employee-owned device—including whether it will need to take physical possession of the device—should be a central consideration when deciding whether to allow, or even require, BYOD. The ability to access the information may vary from device to device and employee to employee. At the very least, access to information is complicated by the defining characteristic of BYOD—the employer doesn't own or possess the device.[4] An organization should therefore consider that it may not be able to obtain access to the contents of employee-owned devices when a need arises.

Organizations face a wide range of possible obstacles to obtaining information from employee-owned devices, including the following:

---

4. *See infra* Comment 3.b. for a discussion of whether an employer has legal possession, custody, or control over ESI on employee-owned devices.

1. Employees may refuse to hand over the personal device, or refuse to provide passwords needed to access data on the device.
2. Even employees who want to cooperate may be unable to provide complete access, e.g., if portions of devices are locked by device manufacturers.
3. Device backups and related device data may be stored in a computer or system that is separate from the device and inaccessible to the employee or employer.
4. An employee's network or cellular service provider may limit the amount and type of information available to a device user if the user is not the primary subscriber of the account or is otherwise not entitled to information the service provider possesses concerning the device (e.g., call records, location information, text messages, voicemail, etc.).
5. The employee may not actually own the device, or the employee may own it jointly with others who may not consent to employer requests concerning the device (e.g., the phone may be owned by a family member, or the cellular service provider may lease the phone to the employee).

Many organizations attempt to increase their ability to access employee-owned devices by making their employees consent to such access as a precondition to employee participation in a BYOD program. A determination of whether this qualifies as "consent" may vary depending on jurisdiction and the facts at issue in the case, including the access sought by the employer. Questions bearing on this issue include the following:

1. Does the employee have an individualized right to privacy that would prevent or negate an employer's assertion of voluntary consent?
2. Does consent by the employee extend to personal information on the device that is not related to his or her employment?
3. When may an employee withdraw consent?
4. If employee consent is considered a quid pro quo element in an exchange between the employer and employee, is there sufficient consideration given by the employer? If providing continued employment is the consideration given by the employer, does the employee's consent necessarily terminate when the employment relationship ends?
5. Does employee consent extend to ancillary locations to which a device is associated? For example, when an employee synchronizes or backs up a device to a home computer or network, does the consent extend to these ancillary locations? Is the employee authorized to provide consent on behalf of all other users of related ancillary locations? These considerations may be magnified in the BYOD context given that consumer devices are often highly integrated with consumer accounts and storage environments in which third-party providers seek to consolidate functions and information within a technology ecosystem (e.g., Apple, Google, Microsoft, and Amazon all provide devices and services which integrate hardware, operating systems, applications, cloud storage, and other services with a user's various accounts and information).

When evaluating whether to allow or require BYOD, an organization should consider how it will balance the privacy interests of its employees against the organization's needs and obligations. Even where an organization has a legal right to access and use the private information of its employees, it would be wise to do so with care, and upon full consideration of the impact that it will have on its employees. Duties to protect data from misuse or disclosure apply in the BYOD context, not necessarily to a greater degree than in other workplace situations, but with a heightened risk of failure given the mobile nature of devices and the extent of commingling that can occur between employer and employee information.

Comment 1.c. Significant legal implications may result if the organization is unable to access its business information on employee-owned devices.

As explained in Comment 3.b., *infra*, whether the organization has the legal right to access ESI on the devices may have a significant impact on whether the organization has a legal obligation to preserve, collect, or produce the ESI in litigation or government investigations. An organization may, in some jurisdictions, reduce the cost and risk of discovery if it does not have a legal right to take the device or access the ESI on the device. However, not having those rights or access can create significant problems for the organization. These problems can include the inability to protect the organization's intellectual property, or get information from personal devices as part of internal investigations.

Comment 1.d. Organizations should consider how they will protect their business information.

BYOD programs present significant security challenges. As noted by the National Institute of Standards and Technology (NIST), many organizations have "established boundaries to

separate their trusted internal IT networks(s) from untrusted external networks. When employees consume and generate corporate information on mobile devices, this traditional boundary erodes."[5] Furthermore, mobile devices, in particular, are a significant source of data breaches.[6] Additional security concerns may arise when users access cloud applications through their devices because malware may be contained in public cloud applications and programs.[7] BYOD devices may also raise heightened security concerns because they co-mingle both personal information and organization information.

Many of the security risks associated with BYOD are inherent in the use of any mobile device with an internet connection. Traditional risks from theft, hacking, and user negligence are ever present on an organization's non-BYOD devices and networks. BYOD enhances those risks, however, because technical and administrative protections are substantially more difficult

---

5. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [hereinafter NIST], U.S. DEPT. OF COMMERCE, *Mobile Device Security for Enterprises*, Building Block 1, V.2 – Final Draft, at 1 (Sept. 12, 2014), *available at* https://nccoe.nist.gov/sites/default/files/nccoe/MobileDeviceBuildingBlock_20140912.pdf.

6. Mobile security breaches have affected more than two-thirds (68 percent) of global organizations in the last 12 months. *See* BRITISH TELECOM, *Art of Connecting: BT Security research on mobile security threats* (October 2014), *available at* http://www.globalservices.bt.com/static/assets/pdf/articles/en/bt_security_research_on_mobile_security_threats_october_2014.pdf.

7. When asked to identify the trends that most impact their security programs, IT professionals revealed that the malware threat and its associated data breach risk is likely to get worse over the coming years specifically because of the (1) continuing evolution of BYOD practices and (2) increasing adoption of cloud technology, both public and private. *See* Elden Nelson, Wisegate, *BYOD and cloud are top data breaches and malware risks, survey shows*, CSO (Apr. 6, 2015), http://www.csoonline.com/article/2906359/data-breach/byod-and-cloud-are-top-data-breaches-and-malware-risks-survey-shows.html.

to develop and implement in a BYOD environment. For example, the organization's own devices may have controls that restrict access to certain websites, particularly those that may contain malware. However, these access controls may be missing on a BYOD device, thereby enhancing the risk the device will become infected with malware. If the employee connects an infected personal device to the organization's network or sends an infected file from a personal device to an organization's network, the infection could spread to that network and to its data absent protective measures.

Issues also arise when employees view BYOD devices as within their exclusive control and believe they possess unrestricted and unlimited rights to do as they see fit. For example, an employee may more readily use a personal device on an unsecured public Wi-Fi network; share the device with friends and family without any protection for organization data; lose, sell, or trade-in the device without wiping data; or open phishing communications containing malware. For these reasons, BYOD should be subject to at least the same level of security, if not greater security, than employer-issued devices.

An organization should consider the technical sophistication of the work force that may use personal mobile devices for work-related purposes. A more technically-sophisticated work force, such as software developers or engineers, may utilize more advanced applications that may integrate organizational tools with organization data (such as tasking reminder tools, translation tools, or email/calendar clients). This type of usage can drive additional risks with respect to the security of the ESI shared with these applications and may drive an organization to adopt a BYOD policy and IT services which limit the amount of ESI and the manner in which such ESI is shared. Less techni-

cally-sophisticated workers might limit their mobile device usage to social media applications, texting, emailing, voicemail, and taking pictures.

Principle 2: An organization's BYOD program should help achieve its business objectives while also protecting both business and personal information from unauthorized access, disclosure, and use.

Comment 2.a. A BYOD policy should be designed to advance the organization's objectives.

Organizations that decide to allow or require BYOD should design and implement a BYOD program that maximizes the benefits that motivated the organization to allow BYOD in the first place, while mitigating the risks and costs of BYOD. The BYOD program should strive to achieve a reasonable balance between improving efficiency and protecting business information and, at the same time, safeguarding personal information. The organization's key objectives in this respect are gains in productivity, reduction in technology and other costs, as well as increased employee satisfaction. Other organizational benefits include increased workplace productivity, and increased flexibility for employees to determine how to fulfill their job responsibilities.

To achieve these objectives, both the organization and its employees should understand their respective responsibilities.

Comment 2.b. A BYOD policy should clearly state the organization's expectations.

Organizations should carefully consider all facets of a BYOD program, from deciding to allow or require BYOD, to designing, implementing, and administering the written BYOD policy. The policy should be written in a way so that employees can easily

understand and comply with it, and be coordinated with the organization's acceptable use and information security policies. The BYOD program should also help employees protect their personal data. Key steps toward fulfilling these goals include: ensuring that a policy complies with applicable labor and technology laws; drafting clear technology and personnel rules, and effectively communicating those rules to employees; providing appropriate training to employees to use BYOD devices consistent with policies and to update applications and hardware to keep up with security standards; and ensuring that employees have access to and know how to access the information they will need whenever questions or problems arise.[8] Addressing non-compliance in a timely manner will help employees understand and appreciate the organization's expectations.

Comment 2.c. Organizations should consider requiring employees to agree to the terms of the BYOD policy.

Where practical, organizations should clarify their employees' rights and obligations by requiring employees to execute consents, authorizations, or end-user agreements as a condition

8. An excellent example of a good reason for an employer to adopt a BYOD policy is presented in *Rajaee v. Design Tech Homes, Ltd.*, No. H-13-2517, 2014 WL 5878477 (S.D. Tex. Nov. 11, 2014). There plaintiff claimed that his former employer unlawfully wiped ESI from his iPhone in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Stored Communications Act component of the Electronic Communications Privacy Act, 18 U.S.C. § 2701. The employer eventually prevailed, but an established BYOD policy that the employee's device, if used in business, would be wiped on termination of employment likely would have avoided litigation entirely. *See also* Brian Hall, *Texas Federal Court decision illustrates need for BYOD policies*, TECHNOLOGY LAW SOURCE (Nov. 25, 2014), http://www.technologylawsource.com/2014/11/articles/information-technology/texas-federal-court-decision-illustrates-need-for-byod-policies.

for participation in a BYOD program. When drafting and implementing those documents, organizations may want to incorporate the following concepts:

1. Clearly set out the circumstances for, and the types of, information that can be stored on the device, and how that information could be subject to monitoring, access, or deletion by the organization.
2. Address ownership and costs of the device and data, including intellectual property licensing considerations and termination of the employment relationship.
3. Explain that unique, relevant ESI may be subject to discovery. Discourage storing unique ESI on the device. *See* Comment 4, *infra*.
4. Identify acceptable use restrictions and the consequences for violating an organization's general computing use policies, such as potential loss of privacy rights in some jurisdictions.
5. Identify steps taken by the organization to segregate personal and business information. Employees should be informed about any device management policies and software.
6. Address the potential for litigation, investigation, regulatory disclosures, and other potential disclosure obligations, and the expectation for access to both the device and the ESI stored on it. The organization should carefully consider the implications of insisting on access to the device and data on the device. Additionally, highlight the potential for waiver of privilege if the employee fails to protect the confidentiality of the privileged ESI.

7. Explain security measures that are in place to protect both business and personal information on the device as well as the device itself.
8. Address privacy to be consistent with other organization policies, including information management policies, employee benefit plans, and others specific to the organization.
9. Address the user's obligation to update certain applications or install patches when issued.

Comment 2.d. The BYOD program should protect the organization's business information.

To protect business information, an organizer should consider developing security policies, practices, and procedures that address data sensitivity (e.g., business value, legal, regulatory and contractual obligations, etc.) and how employees should handle their devices. These BYOD policies, practices, and procedures should take into consideration the organization's tolerance for assuming security risks, and should also be integrated into an organization's overall security policy.

Experience has repeatedly demonstrated that a strict BYOD security policy that is not integrated into an organization's overall security policies will merely negate the efficiency and other potential benefits of BYOD use and potentially leave the organization's data exposed. It also may incentivize employees to "work around" the BYOD policy.

Security policies may need to be more extensive and intrusive as the sensitivity of the information device increases.[9] The

9. For example, NIST has developed a draft guide to demonstrate how to implement security technology for electronic health records. NIST, *SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES, HOW-TO GUIDES FOR SECURITY ENGINEERS*, Public Comment Draft (July 2015), *available at*

policy should address acceptable device types, access controls, software requirements, the purchase of new devices and disposition of old ones, reporting loss or theft of a device, and post-termination protocols.[10] Security policies should also address cloud access because malware may be contained in public cloud applications and programs. In some cases, organizations may place limitations on taking devices outside of the country if highly sensitive data may be stored on the device.[11]

Most security policies have multilevel security components. These security components may include device encryption, in addition to any other device security features. Other security features may include network access restrictions and device activity monitoring. Security protocols may require device registration on the organization's network.[12] Registration provides for identification of "rogue" devices, device tracking, and access logging, which may be useful in the event of a data breach, investigation, or litigation need. Security policies may also include backup procedures and processes for deploying software security updates, upgrades, and patches.

Security policies may differ depending on whether the organization permits commingling of organizational ESI with per-

---

https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1c-draft.pdf.

10. For an in-depth discussion of mobile device security practices, *see* Murugiah Souppaya & Karen Scarfone, NIST, *GUIDELINES FOR MANAGING THE SECURITY OF MOBILE DEVICES IN THE ENTERPRISE*, Special Publication 800-124 Rev. 1 (June 2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

11. *Id.* at 7.

12. This registration helps prevent unauthorized access to the network by assigning a unique identifier to the device, such as a serial number or the International Mobile Equipment Identity (IMEI) number, which the network then uses to determine if the devices attempting to connect are authorized.

sonal data on the device. Organizations may consider implementing software partitions (sometimes called "containers" or "sandboxes"), which segregate organizational from personal data on the device. Such containers or sandboxes are a standard feature in mobile device management (MDM) software that can be placed on BYOD (as well as organization-owned) devices.

According to NIST, "[c]entralized mobile device management technologies are a growing solution for controlling the use of both organization-issued and personally-owned mobile devices by enterprise users."[13] These MDM tools use a messaging server's management capabilities or third-party products.[14] Organizations may find advantages in using these MDM tools for devices to: 1) manage the data on the organizational side of a partition; 2) establish protocols for monitoring software and applications to determine whether there is malware on a device; 3) push software updates and bug fixes to a device, especially security-related updates and bug fixes; 4) permit remote wiping of a device if it is lost, stolen, or the user departs the organization; 5) monitor device activity to identify apps that may be prohibited by policy and identify malware and viruses and remediate them; and 6) provide for cloud-sync blocking.

BYOD security policies that employ MDMs may limit the users' device choices to those that operate effectively with the MDM. This approach also may require the use of specific containerized applications for all organizational networks and data access. One area of particular concern is restricting device-to-device text messages of organizational data since this transmission may likely circumvent the security controls. The technology is developing too fast, and the range of organizational needs is too great to allow detailed suggestions here—the reader

13. *See generally* Souppaya & Scarfone, *supra* note 10, at 7.

14. *Id*.

should consult appropriate experts in designing and implementing any BYOD security policies.

Organizations should also consider employing a BYOD security policy training program. These programs describe potential security threats, explain the security policy, and identify policy compliance requirements. The training policy could identify training frequency and provide documentation verifying an individual's training compliance.

Similarly, organizations should consider conducting periodic security audits to evaluate the BYOD device security protocols and to evaluate users' security compliance. Such audits are part of a typical risk assessment process and, if violations occur, could include procedures for corrective actions and documentation of corrective actions. In some cases, if a vulnerability or breach is discovered, a disclosure may be required. Organizations should consider developing and implementing an exit protocol when an employee with a BYOD device departs the organization. This policy should be designed to ensure that the former employee no longer possesses or has access to organizational data on their personal device. The policy could also include provisions for the organization to retain data that are subject to discovery requirements (e.g., litigation hold, record retention policy).[15] The exit protocol could identify circumstances where forensic examination of the device may be required prior to the employee's exit.

Organizations should tailor their measures to available resources and the nature of corporate information that may be put at risk. Organizations should be careful about introducing a sophisticated state-of-the art security system that the organization cannot afford to maintain, or that the organization's personnel

15. *See supra* Comment 1.b. regarding limitations of these consents, and *infra* Comment 2.f. regarding obligations to protect personal information.

are not trained to use. This may prove to be a greater risk than not employing any security measures at all, because the false sense of security it will engender may encourage risky behavior by BYOD users.

Organizations that have only limited resources for BYOD security measures can still substantially enhance security through administrative safeguards. Administrative safeguards may include warning the people who are providing information to the organization that the information may be vulnerable on the employee-owned devices.[16] Organizations may also prohibit storing some types of data (e.g., client data) on employee-owned devices, or they may require a short retention period for some types of data. User training can also be an important part of an effective security plan.

Investment in data security measures should reflect the value of information to be secured. Organizations that do not have sensitive client data, or other protected data on BYOD devices, may find that the risk of disclosure of business information on such devices is low and thereby forgo investment of state-of-the-art data security measures.

Comment 2.e. The BYOD program should consider employees' privacy interests.

Developing an organization's BYOD security policies involves weighing the organization's need for security against employees' privacy interests. An organization may have to decide whether to incur the additional expense and burden of monitoring device usage. Monitoring would likely be needed to create differing levels of security depending on factors, such as

16. The warning may be analogous to the boilerplate footers that many law firms provide in their email signature lines.

an employee's access to sensitive information, or the sensitivity of specific information.

Technology tools that minimize the commingling of personal and organization data are becoming more common-place, effective, and less expensive. Available measures include encryption, virtual and hardware partitioning of portable devices, and making an organization's data portion of a device akin to a terminal, so that the organization data will continue to reside only on the organization's servers even though the employee can view and create the data through the personal device. Consultation with technology experts is essential for designing appropriate BYOD security measures.

Comment 2.f. The BYOD program should consider employees' protected personal information.

Organizations with obligations to protect personal information of users, employees, or customers, should understand those obligations and implement appropriate safeguards. Various laws mandate the protection of health, financial, and other private information, for example the Health Insurance Portability and Accountability Act (HIPAA), which requires covered entities to comply with the rule's requirements to protect and secure individually identifiable health information. Similar rules requiring the protection of categories of sensitive information from misuse or disclosure can be found in many states and worldwide.

Employees often store protected "personal" data on their personal devices. For example, employees may store their health information on a BYOD device in a health tracking app or other app that syncs with an account associated with the owner's medical provider. Employees may also store their social security number or banking information on their devices via a

personal profile or password manager app or a banking provider's app. Some organizations may choose to restrict the user's ability to download certain apps that may contain sensitive personal content, though doing so may intrude on the positive aspects of BYOD programs that an organization's employees enjoy.

Organizations should additionally factor into their BYOD protocols and policy the likelihood that personal information of third parties may become stored on the BYOD devices in the normal course of business. An employee may have personally identifiable information about customers, relatives, friends, social network "friends," and others. The presence of such information may present special compliance risks for the organization. For example, it would be inordinately difficult to prove that the non-employee consented to any organization access to or use of the non-employee's information.

Federal, state, and foreign data protection laws may protect the personal information of a device's owner. For example, under the Electronic Communications Privacy Act (ECPA), personal communications made via BYOD devices may not be accessed without valid authorization. Similarly, any disputes about ownership of the device or the data stored on it may complicate questions about who has standing to provide "authorization" to access the device and implicate protections afforded under the Computer Fraud and Abuse Act (CFAA). Similarly, evolving individual state laws may also create protections for personal information such as social media content stored on devices used by employees.

Principle 3: Employee-owned devices that contain unique, relevant ESI should be considered sources for discovery.

Comment 3.a. Factors to determine whether ESI on an employee-owned device is discoverable include: whether the ESI is within the employer's possession, custody, or control; whether the ESI is unique; and whether the discovery of the ESI is proportional to the needs of the case.

It should come as no surprise that ESI that falls within the scope of discovery is often stored on mobile devices.[17] Organizations cannot ignore their discovery obligations merely because a device containing unique, relevant ESI is also used for personal purposes.[18] That said, several courts have noted "significant concerns regarding the intrusiveness of the request and the privacy rights of the individuals to be affected."[19] Whether

17. *See* FED. R. CIV. P. 26(b)(1), 26(b)(2)(B)–(C); *see also* Ewald v. Royal Norwegian Embassy, No. 11-CV-2116, 2013 WL 6094600, at *10 (D. Minn. Nov. 20, 2013) (quoting the Magistrate Judge in the case: "It is not a surprise to any of the parties in this case that there were tablets, text messages, cell phones, and laptops involved. All of these devices were known prior to the initiation of litigation, and it is common knowledge that ESI is contained on all of these devices.").

18. *E.g.*, Alter v. Rocky Point School Dist., No. 13-1100 (JS)(AKT), 2014 WL 4966119 (E.D.N.Y. Sept. 30, 2014) ("to the extent school district employees had documents related to this matter, that information should have been preserved on whatever devices contained the information (e.g., laptops, cellphones, any personal digital devices capable of ESI storage.)"); H.J. Heinz Co. v. Starr Surplus Lines Ins. Co., No. 2:15-cv-00631-AJS, 2015 WL 12792025 (W.D. Pa. Jul. 31, 2015).

19. Kickapoo Tribe of Indians of Kickapoo Reservation in Kan. v. Nemaha Brown Watershed Joint Dist. No. 7, 294 F.R.D. 610, 619 (D. Kan. 2013); *see also* Bakhit v. Safety Marking, Inc., No. 3:13CV1049 (JCH), 2014 WL 2916490, at *3 (quoting Riley v. California, 134 S. Ct. 2473, 2478–79 (2014) (regarding the

and how that device may become an appropriate data source for discovery in litigation is subject to numerous considerations, including the way ESI is stored on a BYOD device; whether that ESI is duplicative of other ESI on the organization's systems; and how effectively segregated that ESI is from the user's personal information.

BYOD devices and apps can pose unique discovery challenges as the technology behind them is evolving and discovery tools may not yet exist or be mature enough to handle this type of ESI efficiently and effectively. Counsel has the responsibility to conduct adequate BYOD discovery process due diligence. This due diligence will be the basis for a defensible process and counsel's representations to the court and opposing counsel regarding the discovery process. This is one area where counsel should consider engaging experts with the appropriate technical knowledge, competence, and experience.[20]

An organization's duty to preserve or produce such content will often depend on whether the employer is deemed to have possession, custody, or control of either the ESI or the device, or both, under Rule 34 of the Federal Rules of Civil Procedure (or its state equivalent), and whether the ESI is both relevant and unique (or if instead there is other ESI that is more readily available from other sources), and whether the requested discovery is proportional to the needs of the case. We discuss each of these issues in turn.

---

implication of the individual defendants' privacy interests and the qualitative impact of the volume and variety of data that can be stored on a modern-day cell phone)).

20. *See The Sedona Conference, Commentary on Defense of Process: Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process,* Principle 2, THE SEDONA CONFERENCE (Sept. 2016 Public Comment Version), https://thesedonaconference.org/publication/sedona-conference-commentary-defense-process-public-comment-version-september-2016.

Comment 3.b. An organization's BYOD program can impact whether the organization has possession, custody, or control over ESI on employee-owned devices, but the legal test may vary widely by jurisdiction.

Three different legal standards have developed and been applied in the federal courts to determine whether discovery is in the possession, custody, or control of a responding party generally: the legal right standard, the legal right plus notification standard, and the practical ability standard. A far more detailed examination of these three standards can be found in The Sedona Conference *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* but generally speaking, the legal right standard evaluates a party's control based on their legal right to obtain the documents or ESI in question.[21] The legal right plus notification standard builds on the previous standard by further obligating responding parties who do not have a legal right to the ESI to notify the requesting party of the third parties who have possession, custody, or control of the information requested.[22] Finally, the practical ability standard evaluates control based on whether the responding party has the practical ability to obtain the documents and ESI, regardless of whether or not it has the legal right to do so.[23]

The *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control"* advocates for universal adoption of the legal right standard.[24] The Sedona Conference believes this is particularly

21. *The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," supra* note 1, at 482–518.

22. *Id*.

23. *Id*.; *see also In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007).

24. The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," supra* note 1 at 537–45.

true in the case of BYOD, where it is often unclear whether the organization has the "practical ability" to demand the device from its employees. Under any of these tests, organizations should not be compelled to terminate or threaten employees who refuse to turn over their devices for preservation or collection. It should be emphasized, however, that, at present, the legal right standard has not been unanimously adopted by all federal courts and therefore it is crucial to consider the standard applied in the applicable jurisdiction.

In the BYOD context, the concept of "control" can be particularly murky and ripe for disputes due to the overlap of personal and business information on the device, as well as the physical possession and ownership of the device by the employee, who may be an uninterested third party to the litigation. There is limited case law on possession, custody, or control in the BYOD context although a few courts have held in legal right jurisdictions that organizations do not have possession, custody, or control over BYOD devices where there was no contention that the employer had any legal right to obtain employees text messages on demand.[25]

A "consent" or "acknowledgement" or other agreement that the employee signs and that recognizes that the organization owns or controls the ESI would likewise give the organization possession, custody, or control of the ESI, and the resulting obligation to consider the device when meeting its discovery obligation. Thus, organizations should carefully consider how a

25. *Id.*; Matthew Enterprise, Inc. v. Chrysler Grp. LLC, No. 13-cv-04236-BLF, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015); Ewald v. Royal Norwegian Embassy, No. 11-CV-2116, 2013 WL 6094600, at *10 (D. Minn. Nov. 20, 2013) (refusing to order production of text messages from content from personal mobile devices because plaintiff did not make any showing that she is entitled to personal devices and she "has had ample opportunity to conduct that discovery").

policy that asserts ownership may increase the likelihood that a court will find that an organization does indeed have legal control over such information, thereby increasing discovery-related obligations.[26]

Courts and parties should also consider the practical implications of commanding employees to turn over devices that the employees bought and paid for. Even if an organization has possession, custody, or control over a device, the organization should not be required to use a threat of termination to force the employee to turn over the device. Such a rule would impose too heavily on the relationship between employees and their employer. On the other hand, employers should advise opposing counsel if they are practically unable to collect from employee-owned devices ESI that is within the scope of discovery (i.e., the ESI is relevant, unique, proportional, and within the possession, custody, or control of the employer).

Comment 3.c. Even if ESI on a mobile device is relevant, the ESI is not within the scope of discovery if it can be collected from a more accessible source.

Under many BYOD programs, a significant amount of content on employee-owned devices is duplicative of ESI stored by the organization in other places. Further, the duplicate ESI stored by the organization is typically more accessible than the content stored on the device. In determining whether to preserve or produce ESI content stored on BYOD devices, an organization should evaluate whether the BYOD device is likely to

26. *See* H.J. Heinz, Co. v. Starr Surplus Lines, Ins. Co., No. 2:15-cv-00631-AJS, 2015 WL 12791338, at *4 (W.D. Pa. July 28, 2015) (finding Heinz had possession, custody, and control of BYOD device based on Heinz BYOD policy that indicated Heinz owns the property on the devices and that it can delete content from devices in its sole discretion).

contain relevant, unique content—for example, through interviews or sampling. Organizations may also rely on their BYOD program and their Information Governance program to reach reasonable conclusions about whether relevant ESI on employee-owned devices is likely to be unique.

As explained in Comment 8.a. of *The Sedona Principles*, organizations should first look to more accessible sources of relevant ESI before going to less accessible sources:

> The primary sources of information for the responding party should be those that are routinely accessed in the ordinary course through ordinary means. Once those primary sources are exhausted, the responding party arrives at a "phase gate" or "decision gate," where it must consider whether additional, unique, and discoverable ESI exists within less readily accessible sources and, if so, whether the preservation and potential production of that information through extraordinary means is consistent with the proportionality requirement of Rule 26(b)(1).[27]

Applying this concept to mobile devices, organizations may look to ESI from more accessible sources (e.g., company servers) before collecting ESI from mobile devices.

At least one court has found that a public official's private phone contained public records subject to an open records request, where it was shown that the phone contained government business communications, the township was reimbursing the employee for the use of the phone, and the employee could

27. *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, Cmt. 8.a. (2018).

not "privatize his public correspondence."[28] A trend appears to be growing among state legislators to treat as public records any messages on officials' or government employees' personal devices concerning government business.[29] Even so, public employees' communications on personal devices may be subject to Constitutional protections.[30]

Comment 3.d. The concept of proportionality also limits the scope of discovery of ESI on employee-owned devices.

BYOD greatly expands the opportunities for an organization's users to create and retain ESI in ways that may be well suited for the individual user's needs, but that render preservation and collection for discovery laborious, disruptive, and expensive. As discussed in Comment 3.c., discoverable ESI found on BYOD devices may be duplicative of ESI stored in more accessible sources and, as noted under Principle 1, some of the unique or duplicative content may contain the user's personal information and, potentially, the personal information of third parties. The confluence of these issues can be found in an organization's everyday business activities.

> *Example i.* The chief executive officer (CEO) of ABC Corporation receives an email from her assistant with an attached draft presentation. Using her smartphone, the

28. Paint Township v. Clark, 109 A.3d 796, 809 (Pa. Commw. Ct. 2015); *but see* City of San Jose v. Superior Court, 169 Cal. Rptr. 3d 840, 856 (6th Dist. 2014), *review granted and opinion superseded,* City of San Jose v. S.C. (Smith), 326 P.3d 976 (2014) (holding that the California Public Records Act did not impose an affirmative duty to search devices and accounts of its employees and officials for messages relating to City business).

29. *See, e.g.*, TEX. GOV'T CODE § 552.002(a-1) and (a-2), TEX. LOC. GOV'T CODE § 201.003(8).

30. *See* City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010).

> CEO composes an email forwarding the presentation to the chief financial officer (CFO). The CFO receives the email on his smartphone as his flight is about to depart and downloads and saves the presentation file. During the flight, he edits the presentation, saves the revised version on his smartphone, and composes an email explaining his revisions and attaching the edited presentation file. On landing, he sends the email to the CEO, who then opens the email and attachment on her tablet for viewing on a larger screen. She saves the file to her tablet, makes further edits to the presentation, and then emails the edited file back to the CFO. The two smartphones and tablet are each of different manufacturers and use different operating systems, and each is synchronized to a separate personal cloud account for file storage and backup that is owned and controlled by the individual. The CEO is careful to use a personal email account for family correspondence, but her personal email synchronizes to both her smartphone and tablet and her cloud storage accounts. Her personal emails include the college transcript of her adult daughter, an evaluation from her minor son's therapist, and correspondence with an attorney regarding her role as the legal guardian and trustee of her elderly mother's trust. Applying the proportionality factors, the burden of collecting the various drafts from the various sources likely outweighs the benefit, unless the presentation is so central to the case that drafts of the presentation are extremely important in resolving the issues in the case.

In the above example, an exchange of just three emails between executives created numerous copies of potentially non-identical files stored on multiple devices and accounts and commingled with communications implicating the privacy interests

of third parties who have not previously consented, and may be unwilling or unable to consent, to disclosure of their sensitive personal information to ABC Corporation's counsel. In the first decade of discovery, the paradigmatic example of disproportionate discovery burdens was disaster-recovery-tape backups. ESI on backup tapes was equally inaccessible and required great effort and expense to restore, whether for the organization's ordinary business needs or for discovery. For example, locating a single email message on a backup tape was equally burdensome to accomplish, whether the reason for locating that email was to satisfy business needs or satisfy discovery obligations in litigation. The problem with accessing ESI on mobile devices is often different, in that individual employees can access the ESI for their own business uses (e.g., the CEO in the above example can easily access the draft presentation), but the organization cannot easily access the same information from all the various sources for discovery.[31] Thus, device content can be accessible for business needs in this context, and still not be proportional for purposes of discovery. This distinction may be critical to a proportionality analysis for discovery of ESI on personally-owned devices.[32]

---

31. As another example, some BYOD ESI is not readily accessible to the organization in the course of regular business, such as deleted text messages that may reside on the device but cannot be accessed by a lay user, but only through forensic acquisition.

32. "Free" solutions may fail to properly preserve text messages on cell phones. For example, using cell phone operating system software to sync cell phones with a computer hard drive may not copy all unique ESI from the cell phone, and the process may not store the ESI in a sound manner that can be used for discovery purposes. Further, syncing features may be inadequate, or may be changed by the software provider. Additionally, such processes are not always scalable or user-friendly. "Free" does not necessarily equate with "proportional" or "reasonable."

The proportionality analysis should look beyond the discovery costs in any single case, and consider the impact that discovery will have on the organization's BYOD program. As stated in Comment 3.d. of The Sedona Conference *Commentary on Proportionality in Electronic Discovery*, an effective information governance program should help organizations reduce discovery costs and risks, and, conversely, organizations should not benefit from a poor information governance program that results in large quantities of unique, relevant ESI residing in locations that are difficult to access for discovery:

> Information retention policies may also affect the proportionality analysis. Where a party's information retention policies serve reasonable organizational or commercial purposes, burden, expense, or delay attributable to such policies should not be held against the party claiming burden. Conversely, where information retention policies do not serve such purposes, associated arguments of burden, expense, or delay should be discounted.[33]

Applying proportionality in this manner will incentivize organizations to align their management of BYOD usage with their discovery obligations. Moreover, it will incentivize organizations to address discovery costs when considering adoption of BYOD and the design and operation of their IT systems relating to BYOD.

Implicit in this basic policy argument is an assumption that reliable, practicable methods for managing BYOD presently exist and may be implemented at a reasonable cost.

---

33. The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141, Cmt. 3.d. (2017).

Comment 3.e. Organizations should consider their employees' privacy interests before collecting ESI from employee-owned devices.

As both a legal and practical matter, employees' expectations of privacy are generally greater for devices that they own than for devices that their employer provides. Organizations may have to balance varying privacy obligations with discovery obligations in the different jurisdictions in which it does business, with sometimes conflicting legal standards.[34] Often, the determination of which country's data privacy laws apply to the data stored on a BYOD device must be made on a case-by-case basis. Organizations can work with outside privacy counsel and local counsel to analyze factors such as whether data privacy rights are based on the citizenship of the employee or the physical location of the device. *See* Appendix B, *infra*, for a discussion regarding country specific considerations.

If a BYOD device contains unique, relevant data, but is subject to data protection laws, several opportunities to balance data protection with U.S. discovery obligations exist, including: (1) limiting the scope of discovery to only relevant and necessary protected data; (2) establishing a stipulation or protective order regarding protected data; (3) planning for phased discovery and collecting data from easily accessible sources first; and (4) potentially planning an in-country collection and review in order to minimize the transfer of protected data outside of the country.

Organizations also face an inconsistent and complex landscape of court rulings that increase their risk of potential liability to employees when the organization accesses BYOD devices to collect unique, relevant content. For example, in the context of

34. *See* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397 (2016).

employer-provided devices, courts have recognized public sector employees' privacy expectations in personal text messages,[35] and private sector employees' privacy expectations in attorney-client emails sent via employee-owned webmail accounts.[36] In contrast, other courts have found employees' expectations of privacy waived when using the computer systems owned by their employer.[37]

Many organizations attempt to require broad privacy waivers from users as a condition of the organization's consent to BYOD usage. This approach may be inconsistent with local law in some jurisdictions. Even if such broad user privacy waivers are enforceable, commingled BYOD ESI may include information implicating the privacy rights of third parties not bound by the waiver. The example of the CEO using her tablet and smartphone in Comment 3.d., *supra*, illustrates how the personal communications of a user may intersect with multiple, distinct legal and ethical relationships, raising privacy concerns for each.

---

35. *Quon*, 560 U.S. at 760 (acknowledging city employee's "reasonable expectation of privacy" in text message communications sent via a cell phone issued by the municipality in the context of a Fourth Amendment search and seizure claim; however, the Court did not resolve the parties' disagreement over Quon's privacy expectations).

36. *See, e.g.*, Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 663 (N.J. 2010).

37. *See, e.g.*, Order, *In re* Grand Jury Subpoenas Dated May 14, 2014 & January 13, 2015, No. 1:15-mc-02227-JBW (E.D.N.Y. Dec. 3, 2015) (unsealed) (Weinstein, S.J.) ("The employee was warned by the company that the documents created during employment were company property. . . . As company documents they would not be subject to a privilege between the employee and an attorney acting for the employee and also for the company."); Holmes v. Petrovich Dev. Co., L.L.C., 191 Cal. App. 4th 1047, 1071 (Cal. Ct. App. 2011) (plaintiff had no expectation of privacy in personal email sent on a work computer when plaintiff was notified in writing that her employer could inspect her computer at any time at its discretion).

Principle 4: An organization's BYOD policy and practices should minimize the storage of—and facilitate the preservation and collection of—unique, relevant ESI from BYOD devices.

Comment 4. Organizations should proactively manage employee-owned devices.

Proactive BYOD management can reduce discovery costs by limiting or excluding unique ESI from the BYOD device (where practical), and striving to ensure that all organization ESI transmitted, received, or stored on the BYOD device is also captured and retained on the organization's network servers or other centralized storage locations under the organization's control, where preservation and search functions can be addressed in a targeted and efficient manner.

Eliminating the BYOD device as a relevant storage location for discovery, to the extent reasonably feasible, would require a combination of technology, policy, and user training solutions. Avoiding retention of unique emails sent or received on the user's organization email account is a common practice whereby there is complete synchronizing of transmitted and deleted email between the device and the network, and the retention period is the same on both the corporate email server and on the device. At least in theory, implementing these account settings—i.e., prohibiting use of personal email and cloud accounts for organization ESI, and prohibiting users from saving organization files locally on the BYOD device—may substantially reduce the relevance of the BYOD device for discovery of business information. However, in practice, an organization may need to rely primarily on technology safeguards to implement and enforce these restrictions by "locking down" the device settings and using MDM security software applications, as discussed in Comment 2.d., *supra*. User training complements

such technology solutions. The goal of user training is not simply to communicate the organization's policy, but also to persuade users to support the policy. Sophisticated users will find opportunities to "work around" BYOD restrictions and frustrate the organization's BYOD management unless they accept these restrictions as valid and credible.

Again, policy, technology, and training offer viable solutions to substantially reduce the problem of commingled personal data and organization ESI on BYOD devices. For example, several software developers market partitioning applications[38] to segregate personal data on BYOD devices. Many of the same solutions that an organization may rely upon to aggregate organization ESI on a corporate network or other centralized storage location may also be used to exclude personal data—such as using separate email accounts for personal and business communications, or excluding business files from local storage on the BYOD device so that, in theory, the only unique files saved locally to the device are personal user content. In the context of managing personal data, training is especially important to inform users of how to use the BYOD device in a manner that does not compromise their personal privacy. Such training may mitigate the need for broad organization-imposed privacy waivers.

Reasonable measures to regulate BYOD usage should be considered by an organization. What constitutes reasonable may vary among organizations depending upon the size and complexity of the organization or the frequency with which the organization is a discovery respondent. Within a particular organization, different approaches may be appropriate for different users based upon their organization roles and their degree of sophistication as IT consumers. BYOD may be inappropriate

38. For example, Google's "Android for Work" and AT&T's "Toggle" provide partitioning functionality.

for some users because it is prohibited by law or regulations. For example, some employees may be prohibited from using personal devices while performing certain functions to protect public safety (e.g., railroad locomotive engineers) or to prevent criminal or fraudulent schemes (e.g., traders on the securities markets). Comment 3.e., *supra,* discusses the extent to which local law protecting user privacy rights may impact an organization's ability to implement effective BYOD management.

An important part of proactive BYOD management is developing regularly recurring processes for documenting and validating the organization's methods. As a discovery respondent, the organization may be required to defend its reliance on these methods to define the scope of its preservation and collection. Well-documented processes may be essential for the organization to actually enjoy the benefits of its investment in careful BYOD management.

Principle 5: Employee-owned devices that do not contain unique, relevant ESI need not be considered sources for discovery.

Comment 5.a. Responding parties should make reasonable efforts to determine whether mobile devices contain unique, relevant ESI.

As explained in Principle 3, *supra*, efforts related to discovery of BYOD devices should target the unique, relevant ESI on such devices. It is now well-accepted that discovery of relevant information is limited in scope to exclude duplicate copies of otherwise responsive ESI, as long as none of the copies have independent value. Thus, if there is a reasonable basis to believe that personally-owned devices do not contain unique, relevant information, the organization should not be required to preserve or collect ESI from those devices.

The existence of a "reasonable basis" can be shown many ways, including the following:

- An interview of key custodians determines none of the custodians used their mobile devices to communicate about issues relevant to a case, and, where this may be in dispute, none of the ESI created by the communications was unique to the devices.
- Critical evidence in a case is formulae in a spreadsheet stored on a computer and, therefore, have absolutely nothing to do with any data that could be uniquely stored on a cell phone.
- The only communications about the issues or events involved in a case are through an email application that fully synchronizes with the organization's servers; the email can be collected from the servers and not from the BYOD devices.
- The organization has in place a BYOD policy or technology controls reasonably designed, with due care and in good faith, to prevent the storage of unique, relevant ESI on BYOD devices. Where this is the case, the organization should preserve and collect the most accessible copy of such ESI from non-BYOD sources, such as active email files or a designated legal hold archive of such email files (if an organization has such a system in place).

As with other potential sources of ESI, the concept of proportionality applies to dictate what steps an organization must take to determine whether the devices contain unique, relevant ESI.[39]

39. *See supra* Comment 3.d.

Comment 5.b. BYOD programs can give organizations a reasonable basis to believe that employee-owned devices do not contain unique, relevant ESI.

Where an organization relies on its BYOD policy to avoid preservation or collection of ESI from BYOD devices, cooperative discussion and non-privileged information exchange with opposing counsel regarding what ESI is (and is not) stored on the BYOD devices, and what other sources of data are reasonably available, may reduce or eliminate formal discovery or motion practice.

> *Example i.* An organization has a BYOD device policy or protocol that ensures all email sent from and received on the BYOD device is also stored on the email server, all deletions made in Outlook synchronize to the device, and the retention period is the same in Outlook and the device. After reasonable inquiry, the organization can reasonably conclude that unique, business-related ESI is not stored on the device. Absent any other showing, the organization should be relieved of the burden of preserving and collecting ESI from the device.

As many courts have opined, Rule 26(b)(1) and (g) impose a reasonableness standard for discovery, and do not require perfection.[40] Extending this to the realm of preservation of BYOD

40. Reinsdorf v. Skechers U.S.A., Inc., 296 F.R.D. 604, 615 (C.D. Cal. 2013) ("[W]hile parties must impose a reasonable construction on discovery requests and conduct a reasonable search when responding to the requests, the Federal Rules do not demand perfection. *See, e.g., Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 618–19 (D. Colo. 2007) (parties have 'an obligation to construe . . . discovery requests in a reasonable manner'); *Metropolitan Opera Ass'n, Inc. v. Local 100, Hotel Employees and Restaurant Employees Int'l Union*, 212 F.R.D. 178, 223 (S.D.N.Y. 2003) (Rule 26(g) requires a 'reasonable inquiry under the circumstances'); *Moore v. Publicis Groupe*, 287 F.R.D. 182, 188 (S.D.N.Y. 2012) ('[T]he Federal Rules of Civil Procedure do

devices, it may always be a possibility that due to a technology bug or loophole, or to a user's activities, instances of unique, relevant ESI on a BYOD device may go undetected—despite an organization's reasonable efforts. The mere possibility or existence of such ESI, in the absence of a compelling need or showing, should not require an organization to take additional steps to preserve and collect ESI on BYOD devices.

> *Example ii.* The organization in the example above advises that users of BYOD devices can download attachments from email messages to their devices and those downloads are not synchronized to the organization's systems. If, after reasonable inquiry, the organization determines that such downloads are infrequent and that the attachments are not significant to the issues in the case (e.g., custodian interviews demonstrate that no custodians regularly used the download feature to organize relevant information into meaningful compilations), the organization is not required to preserve or collect ESI from such devices.
>
> *Example iii.* An organization has in place a BYOD program reasonably designed, with due care and in good faith, to prevent the storage of unique, business-related ESI on BYOD devices. If the organization takes reasonable steps to confirm that its employees comply with its program, that organization need not preserve or collect ESI from BYOD devices.

---

not require perfection.'); *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of America Securities, LLC,* 685 F. Supp. 2d 456, 461 (S.D.N.Y. 2010) . . . 'The reasonableness of the inquiry is measured by an objective standard. . . .' *National Ass'n of Radiation Survivors v. Turnage,* 115 F.R.D. 543, 555 (N.D. Cal. 1987).").

Example iv. An organization makes reasonable inquiry during custodian interviews to confirm that the custodians comply with the BYOD program, which therefore provides the organization with a reasonable belief that unique, relevant ESI does not exist on BYOD devices. At a later deposition, however, a key custodian discloses that she used her BYOD device to store relevant ESI, in contravention of the organization's BYOD policy. If that ESI is proportional to the needs of the case, the organization should collect ESI from the device and produce non-privileged relevant information. The organization should also take reasonable steps to determine whether other employees with relevant ESI also violated the BYOD policy. If the organization fails to produce non-privileged relevant information from the device of the custodian who originally disclosed violation of the BYOD policy, a challenging party could then move to compel discovery of this device and the court may reasonably grant such a motion where a compelling need is shown, though it should not make *post hoc* judgments about preservation of the device based on information not previously known to the organization. Additionally, the court could allow limited discovery on the issue of whether other key custodians similarly used their devices in contravention of the policy, whether the information stored on their BYOD devices is material and unique, and whether the burden of obtaining the ESI is proportional to the needs of the case.

Comment 5.c. Parties and courts should take reasonable steps to protect business information in cases where the organization is not a party.

The above comments address the situation where the organization is a party and some of the organization's ESI is relevant

in the litigation, but personal information is not. Sometimes, however, the roles are reversed and the employee is a litigant, but the organization is not. In those cases, the organization's data is not relevant, but the employee's information is. Where a BYOD device is a target of discovery solely for the personal information on the device, a court should allow an organization to remove from the device, or otherwise exclude from discovery, any ESI it can demonstrate is non-relevant, business information. In such situations, the organization would benefit from clauses in its BYOD policy that give it the right to be notified and to remove or otherwise protect any such business information prior to collection. The objective is to ensure that the organization's non-relevant data is not subject to discovery. In the absence of a third-party request or other similar obligation to preserve such ESI, an organization does not have a duty to preserve or collect personal ESI stored on BYOD devices.

> *Example i.* In a domestic dispute involving an employee, discovery is taken from the employee's BYOD device. In the absence of a compelling need or showing otherwise, the parties should notify the organization and work with it to ensure that document collection from the device excludes organization information, or allow the organization to remove non-relevant business information from the device (subject to other preservation requirements that may be in place).

APPENDIX A: DEPARTMENTAL COLLABORATION GUIDE

Collaboration among departments or people of various disciplines should be undertaken when organizations develop a BYOD policy and BYOD practices ("BYOD program"). Collaboration is not a legal requirement, but rather an aspirational best practice. When developing a BYOD program, consider consulting with these departments: Finance, Human Resources (HR), Information Governance (IG), Information Technology (IT), Legal/Compliance, and Security. Smaller organizations may not have all of these departments, or they may have combined or outsourced some functions. Furthermore, an organization's structure and purpose may necessitate consulting with people in other specialty areas not included here. Below is a chart outlining the potential benefits of consulting with departments in each specialty area and questions to address to each, but the chart's primary purpose is to help guide organizations identify which specialty areas to include when developing a BYOD program.

Specialty Areas to Include When Developing a BYOD Program

	Benefits of Consulting	Questions to Ask
Finance	• Understand financial issues for BYOD program, including indirect or hidden costs • Coordinate potential employee reimbursement for BYOD	• How will BYOD devices be financed (purchase, lease, or rental)? • Are there any agreements that govern the provision of BYOD devices or data/phone services? • How will costs increase or decrease if there is a change to the BYOD program?
Human Resources (HR)	• Understand employment issues • Articulate HR objectives for BYOD program • Coordinate with existing HR policies and procedures • Determine roles for HR in implementation and enforcement • Identify state and country laws that may impact BYOD program	• How does HR currently handle BYOD devices? • How does HR handle use of technology and communication in its various policies? • How does HR handle technology training? • Will BYOD program include employees and contractors or organization agents? • How will the BYOD program be rolled out to employees? • Should all employees be eligible for the BYOD program? • How will HR exit-interview processes incorporate questions about BYOD?

	Benefits of Consulting	Questions to Ask
Information Governance (IG)	• Determine how BYOD will affect management and governance of data	• Do any information management policies or processes need to be revised? • How will BYOD affect data governance and record retention?
Information Technology (IT)	• Understand IT objectives and requirements for BYOD program • Coordinate with IT to enable elements of the BYOD program • Determine roles for IT in implementation and enforcement • Create proprietary apps for use on BYOD devices	• How does IT currently handle BYOD devices? • How does IT handle remote access? • What types of devices will be included? • What geography is included? • How does IT handle technology training? • How will IT handle BYOD devices when an employee leaves the organization?

	Benefits of Consulting	Questions to Ask
Legal/ Compliance	• Identify state and country laws that may impact BYOD program • Understand impact on preservation and litigation, and other disclosure mandates • Understand impact on third-party requests for information • Consider employment issues that arise from BYOD • Identify and assess relevant record retention requirements	• How will risk increase and decrease if there is a change to the BYOD program? • How will BYOD affect identification, preservation, collection, and all other discovery steps? • How will compliance with the BYOD program be reviewed? • How will Legal/Compliance exit-interview processes incorporate questions about BYOD, particularly as related to any information that may be under preservation?

	Benefits of Consulting	Questions to Ask
Security	• Understand security risks • Establish security risk tolerances • Implement security requirements • Identify processes for protecting confidential and private information	• How will BYOD devices be secured? • How will BYOD devices access organization systems? • How will BYOD devices be locked out of or removed from accessing organization systems?

Many of the items suggested for consideration impact multiple specialty areas within an organization that may, and hopefully will, bring different perspectives to the table for discussion. For example, when an organization is determining the scope of a BYOD program, and which employees or contractors should be eligible for BYOD, Finance will be interested because of the cost and ability to charge back to a business unit, while HR may be interested in the issues with rolling out different policies for different roles or departments. Below is a chart that suggests which areas may need to be consulted regarding common topics confronted by an organization implementing a BYOD program.

Topics for Multiple Specialty Areas within an Organization to Consider

	Finance	HR	IG	IT	Legal/ Compliance	Security
Eligible Employees	X	X	X	X	X	X
Eligible Data			X	X	X	X
Eligible Devices	X			X	X	X
Security Requirements	X			X	X	X
Eligible Apps	X			X	X	X
Training		X		X	X	X
Compliance Monitoring	X	X		X	X	X
Notice to and Consent from Third Parties			X		X	
Device Tracking	X			X	X	X
Budget	X	X	X	X	X	X
Types of ESI on BYOD Devices		X	X	X	X	X

Consultation with its various departments can help the organization consider implications and risks identified by each area and in theory will result in a more robust and well-planned BYOD program. It is important to have a clear project plan with timelines and a project manager that can shepherd the various

organizational departments through the creation, implementation, and initial compliance audit for the BYOD program.

APPENDIX B: BYOD IN THE INTERNATIONAL CONTEXT

There are unique legal challenges to the successful implementation of a BYOD program, particularly in the international context and due mainly to data privacy and data protection laws. In the European Union and many other jurisdictions, data privacy is considered a human right. Therefore, when developing a BYOD program, organizations should consider and understand the various data protection laws and regulations in the countries that they operate, especially those laws that apply to BYOD and the workplace, including concepts such as employee monitoring.

Employers will also face unique legal challenges due to international data privacy and data protection regulations that may impact discovery. The Sedona Conference *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)* (hereinafter "*International Litigation Principles*") provides guidance for navigating such global discovery challenges.[41] The *International Litigation Principles* contains discovery obligations for the employer, which include striving to show due respect to the data protection laws of any foreign sovereign, operating under a standard of good faith and reasonableness, limiting scope of preservation and discovery of protected data, using a stipulation or court order to protect protected data, demonstrating that appropriate data protection safeguards are in place, and retaining protected data only as long as necessary to satisfy business or legal needs.[42]

---

41. The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, THE SEDONA CONFERENCE (January 2017), https://thesedonaconference.org/publication/International%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection.

42. *Id*.

Organizations should contact both local counsel and local data protection authorities when considering instituting global BYOD programs. Individual countries may have specific and nuanced definitions of personal data and regulatory bodies may have commented specifically on BYOD best practices. For example, the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), released BYOD guidelines in early 2015 that detail best practices for BYOD in France.[43] In 2013, the German Federal Office for Information Security (BSI) published guidance on BYOD issues.[44] In 2013, the Information and Privacy Commissioner of Ontario, Canada, partnered with a telecom organization to issue a whitepaper on BYOD policies and development strategies.[45] Also in 2013, the United Kingdom's Information Commissioner's Office (ICO) issued guidance regarding the UK Data Protection Act of 1998 and its application to BYOD policies.[46] These are a few examples of a broad array of guidance on BYOD that has been issued from various regulatory agencies across the globe.

---

43. CNIL, *BYOD: quelles sont les bonnes pratiques?* (Feb. 19, 2015), https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques (unofficial translation *available at* http://www.hldataprotection.com/2015/03/articles/international-eu-privacy/cnil-releases-byod-guidelines).

44. Hunton & Williams LLP, *German Federal Office for Information Security Issues Guidance on Consumerization and BYOD*, PRIVACY & INFO. SECURITY L. BLOG (Feb. 7, 2013), https://www.huntonprivacyblog.com/2013/02/07/german-federal-office-for-information-security-issues-guidance-on-consumerization-and-byod.

45. Ann Cavoukain, OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, & TELUS, BYOD (BRING YOUR OWN DEVICE): IS YOUR ORGANIZATION READY?, PRIVACY BY DESIGN, at 1 (December 2013), *available at* https://www.ipc.on.ca/wp-content/uploads/2013/12/pbd-byod.pdf.

46. UNITED KINGDOM'S INFORMATION COMMISSIONER'S OFFICE (ICO), BRING YOUR OWN DEVICE (BYOD), *available at* https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf (last visited November 25, 2017).

THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES FOR ADDRESSING DATA PROTECTION IN CROSS-BORDER GOVERNMENT & INTERNAL INVESTIGATIONS: PRINCIPLES, COMMENTARY & BEST PRACTICES

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

Author:

The Sedona Conference

Editors-in-Chief:

Denise E. Backhouse
Taylor M. Hoffman
Peggy Kubicz Hall
David C. Shonka

Contributing Editors:

Natascha Gerlach
Jeane Thomas

Contributors:

Lara Ballard
Michael Flanagan
Michael Becker
Jennifer Hamilton
Craig Earnshaw
David Moncure

Staff Editors:

Susan M. McClain
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views 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, click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> 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).

PREFACE

Welcome to The Sedona Conference *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices* (*"International Investigations Principles"*), 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 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 *International Investigations Principles* is effectively a companion publication to The Sedona Conference *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)* (*"International Litigation Principles"*). Whereas the *International Litigation Principles* addresses cross-border transfers of data in the context of U.S. civil litigation and legal actions, the *International Investigations Principles* addresses cross-border transfers of data in the context of Government and Internal Investigations. The *International Investigations Principles* represents the collective effort of numerous WG6 members who, over the course of five years of dialogue, review, and revision, have developed a consensus-based set of principles and associated commentary.

I particularly thank Editors-in-Chief Denise E. Backhouse, Peggy Kubicz Hall, Taylor M. Hoffman, and David C. Shonka for their leadership and significant commitments in time and attention to this project. I also thank Natascha A. Gerlach and Jeane Thomas who served as contributing editors, as well as Lara Ballard, Michael Becker, Craig Earnshaw, Michael Flana-

gan, Jennifer Hamilton, and David Moncure for their contributions. And finally, I thank David Wallace-Jackson, Megan Walsh, and X. Kevin Zhao from the Greene Espel P.L.L.P. law firm; Leeanne Mancari from the DLA Piper LLP (U.S.) law firm; Kimberly J. Duplechain of Littler Mendelson, P.C.; and Shelley O'Hara from the U.S. Federal Trade Commission's (FTC) Office of General Counsel for their assistance with this publication in its various iterations.

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.

Craig Weinlein
Executive Director
The Sedona Conference
May 2018

FOREWORD

In 2011, The Sedona Conference, through its Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6) issued its *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery of Protected Data in U.S. Litigation* (*"International Litigation Principles"*).[1] In it, WG6 identified six principles to guide Organizations navigating the competing demands of U.S. discovery and European data protection regulations. These six principles were accompanied by commentary, suggested best practices, and model practice materials.

The *International Litigation Principles* offers helpful guidance to practitioners and courts in reconciling U.S. Litigation discovery rights with data privacy rights.[2] However, as noted in the commentary herein, the *International Litigation Principles* is not always useful, or even available, in the context of investigations. Accordingly, WG6 formed a committee to study Government and Internal Investigations, in order to explore how to best

1. Originally issued for public comment in a European Union edition in 2011, the publication was revised and reissued in 2017 to incorporate received comments and to reflect intervening developments in international data protection and U.S. civil procedure rules and case law. *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%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection [hereinafter *International Litigation Principles*].

2. The *International Litigation Principles* defines U.S. Litigation as "civil proceedings requiring the discovery of relevant information whether in federal, state, or other U.S. fora" and specifically excludes "criminal proceedings or any other government investigations." *See id*. at Sec. II, Definition 6 (incorporated into the *International Investigations Principles* in Definition 11).

guide practitioners in addressing the unique issues often present in those matters.

This version of The Sedona Conference *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices* (*"International Investigations Principles"*) is the culmination of a five-year effort by The Sedona Conference and WG6 to develop practical guidelines and principles to help Organizations, regulators, courts, and other stakeholders when they must deal with civil Government Investigations or Internal Investigations that necessitate the transfer of Protected Data across national borders.[3] The *International Investigations Principles* was conceived as a result of dialogue that began in 2013 in Zurich, where The 5th Annual Sedona Conference International Programme ("International Programme") and a WG6 Meeting were held, and where WG6 recognized that processes that work for handling Protected Data in litigation do not always work in investigations. The general content of the *International Investigations Principles* was discussed at the International Programme and WG6 Meeting in London in July 2014 (then in the form of a paper identifying the differences between litigation and investigations and calling for more dialogue on these issues) and at The Sedona Conference "All Voices" Meeting in New Orleans in November 2014 (then in the advanced form of a paper proposing modifications to the *International Litigation Principles*). Taking into account feedback from WG6 members, the WG6 Steering Committee then directed that the paper be developed into this standalone set of principles with commentary, which was the focus of additional dialogue at the International Programme

3. The *International Investigations Principles* does not address cross-border data transfers in connection with criminal law enforcement investigations, which are governed by different laws, treaties, and protocols from civil (non-criminal) Government Investigations.

and WG6 Meeting in Hong Kong in June 2015. A few months after Hong Kong, the European Union Court of Justice invalidated the U.S.-EU "Safe Harbor" program, which has since been replaced with the EU-U.S. Privacy Shield framework ("Privacy Shield"). Developments related to the Privacy Shield proposals then prompted a close review of the *International Investigations Principles* to ensure that it remains consistent with current law in the EU and elsewhere. These developments prompted further review of the draft commentary, and those changes were in turn the subject of additional dialogue at the International Programme and WG6 Meeting in Berlin in June 2016. The *International Investigations Principles* was developed during a tumultuous period in the evolution of EU-U.S. data protection relations, spanning the revelations of Edward Snowden in 2013, the decision of U.K. voters in June 2016 to leave the EU, and the passage into law of the General Data Protection Regulation (GDPR)[4] in May 2016 and taking effect in May 2018. These last two developments were largely, but not perfectly, anticipated in time for Berlin; and, consequently, the public comment version of this paper was ready for discussion at the International Programme and WG6 Meeting in Dublin in June 2017.

The resulting *International Investigations Principles* is a standalone document that provides guidance to Organizations, regulators, courts, and other stakeholders when they must deal

4. The General Data Protection Regulation [hereinafter GDPR] is a single, binding EU-wide legislation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN), effective May 2018. The GDPR replaces 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) 31, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 [hereinafter the EU Data Protection Directive].

with civil Government Investigations or Internal Investigations that necessitate the transfer of Protected Data across national borders. While the Privacy Shield, The Asia-Pacific Economic Cooperation (APEC) Framework, The Hague Convention, and other intergovernmental arrangements, where available, all establish procedures that Organizations may—or should—follow, the eight principles herein are intended to guide Organizations in planning for and responding to Government and Internal Investigations while ensuring that Protected Data is safeguarded at all times against avoidable risks of disclosure. Accordingly, these Principles do not provide legal advice for complying with various legal regimens, nor do they purport to tell Investigating Authorities or courts how they should respond in particular cases. Rather, they provide guidance for safeguarding Protected Data while working within established legal regimens no matter where, or what, they are.

The *International Investigations Principles* is organized as follows: The Introduction is followed by Part I which highlights key differences between litigation on the one hand and civil Government Investigations and Internal Investigations on the other. Part II sets out the eight guiding international principles for addressing data protection in cross-border Government and Internal Investigations, and provides comments on each.

TABLE OF CONTENTS

THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES FOR ADDRESSING DATA PROTECTION IN CROSS-BORDER GOVERNMENT & INTERNAL INVESTIGATIONS

1. Organizations doing business across international borders, in furtherance of corporate compliance policies, should develop a framework and protocols to identify, locate, process, transfer, or disclose Protected Data across borders in a lawful, efficient, and timely manner in response to Government and Internal Investigations.

2. Data Protection Authorities and other stakeholders should give due regard to an Organization's need to conduct Internal Investigations for the purposes of regulatory compliance and other legitimate interests affecting corporate governance, and to respond adequately to Government Investigations.

3. Courts and Investigating Authorities should give due regard both to the competing legal obligations, and the costs, risks, and burdens confronting an Organization that must retain and produce information relevant to a legitimate Government Investigation, and the privacy and data protection interests of Data Subjects whose personal data may be implicated in a cross-border investigation.

4. Where the laws and practices of the country conducting an investigation allow it, the Organization should at an early stage of a Government Investigation engage in dialogue with the Investigating Authority concerning the nature and scope of the investigation and any concerns about the need to produce information that is protected by the laws of another nation.

5. Organizations should consider whether and when to consent to exchanges of information among Investigating Authorities of different jurisdictions in parallel investigations to help minimize conflicts among Data Protection Laws.

6. Investigating Authorities should consider whether they can share information about, and coordinate, parallel investigations to expedite their inquiries and avoid, where possible, inconsistent or conflicting results and minimize conflicts with Data Protection Laws.

7. Courts and Data Protection Authorities should give due regard to the interests of a foreign sovereign seeking to investigate potential violations of its domestic laws.

8. A party's conduct in undertaking Internal Investigations and complying with Investigating Authorities' requests or demands should be judged by a court, Investigating Authority, or Data Protection Authority under a standard of good faith and reasonableness.

DEFINITIONS

The following definitions apply to the Principles, Commentary, and associated guidance:[5]

1. "Data Controller" is the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means for the Processing and transfer of Protected Data.[6]
2. "Data Protection Authority" refers to a local, national, or other government entity authorized to implement and enforce Data Protection Laws.
3. "Data Protection Laws" include any law or regulation, including U.S. laws and regulations, that restricts the usage or disclosure of data, requires safeguarding data, or imposes obligations in the event of compromises to the security or confidentiality of data. The *International Investigations Principles* is intended to apply broadly wherever Data Protection Laws, regardless of national origin, conflict with obligations pertaining to Government Investigations (as defined herein) and Internal Investigations,

5. Many of the definitions used in the *International Investigations Principles* parallel the terms used in the GDPR. We use these definitions intentionally in order to establish a common platform of understanding. It should be noted, however, that the *International Investigations Principles* is agnostic relative to the national origin of any Data Protection Law, and the usage of similar terminology should not be construed as recognition or acceptance of any particular interpretation given to those terms by others, either now or in the future.

6. Under the GDPR, a Data Processor who is not also a Data Controller may nevertheless become subject to a similar level of accountability as a Data Controller, or subject to potential joint liability for Processing performed on behalf of a Data Controller.

whether those laws take the form of privacy regulations, blocking statutes, specific industry protections (e.g., banking privacy), labor laws, trade secret protections, or other protections.

4. "Data Subject" is any person or entity whose Protected Data is or may be processed, transferred, or disclosed.

5. "Government Investigation" is used broadly to include any inquiry by a duly authorized government entity to acquire information for a purpose other than the investigation or prosecution of a crime or suspected criminal activity. Although a Government Investigation may lead to the filing of civil claims in judicial or administrative courts (considered U.S. Litigation), as used herein, Government Investigation refers only to the pre-filing investigative stage of proceedings.

6. "Internal Investigation" includes any inquiry into relevant facts undertaken by an Organization for the purpose of determining whether conduct attributable to it is or has been consistent with its legal or ethical obligations or whether others are or have been engaged in conduct that is harmful to the Organization.

7. "Investigating Authority" refers to the duly authorized government entity, other than a court, undertaking the Government Investigation at issue or demanding the production of information, but does not include Data Protection Authorities.

8. "Organization" as used herein shall have its ordinary meaning and may include any entity or group of entities that are related whether by ownership or by agreement.

9. "Processing" includes any operation or set of operations, activity, use, or application performed upon Protected Data by automatic or other means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, transfer, or disclosure or otherwise making available.

10. "Protected Data" is any data irrespective of its form (e.g., paper, electronically stored information (ESI), images, etc.) that is subject to Data Protection Laws.[7]

11. "U.S. Litigation" includes civil proceedings requiring the discovery of information whether in federal, state, or other U.S. fora. For the purposes of these Principles, "U.S. Litigation" does not include criminal proceedings or pre-lawsuit Government Investigations.[8]

7. The use of the word "data" in the *International Investigations Principles* is intended to convey that the Principles, Commentary, and associated guidance apply to all data, from its lowest level of abstraction to any assembly into information and its recordation on any media.

8. For specific guidance concerning U.S. Litigation implicating cross-border data transfers, *see International Litigation Principles*, *supra* note 1.

INTRODUCTION

Cross-border production of documents in civil litigation must account for the data protection and privacy regulations of the countries where documents and custodians reside. Practitioners understand that the demands of litigation potentially conflict with parties' obligations under Data Protection Laws in jurisdictions where they operate, and practitioners have become more adept at balancing these competing demands. The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6) has published a set of principles, provided commentary, and suggested best practices to assist practitioners in addressing these competing concerns. Less work has been done, however, to build consensus around best practices for handling Protected Data, particularly personal data,[9] in the context of Government Investigations and Internal Investigations.[10] The Sedona Conference *International Principles for Addressing Data Protection in*

9. For example, the EU defines "personal data" broadly to encompass virtually any information relating to an identified or identifiable natural person ('data subject'), reaching even location data and online identifiers. *See* GDPR art. 4(1).

10. In recent years, legal scholars and practitioners have addressed the unique challenges presented by cross-border investigations. *See, e.g.*, Lucian E. Dervan, *International White Collar Crime and the Globalization of Internal Investigations*, 39 FORDHAM URB. L.J. 361, 373 (2011) ("The starting place for any internal investigation is the collection of relevant documentary evidence for review and analysis. . . . In the international context, however, collection, review, and transfer of documentation can present unique challenges to counsel because of the growing prevalence of data protection laws around the globe."); George J. Terwilliger III, *Transnational Practice in Preventing and Addressing Corruption Cases*, INTERNATIONAL WHITE COLLAR ENFORCEMENT: LEADING LAWYERS ON UNDERSTANDING INTERNATIONAL DEVELOPMENTS, COMPLYING WITH FCPA INVESTIGATIONS, AND ESTABLISHING EFFECTIVE CORPORATE COMPLIANCE PROGRAMS 95 (2011 Ed.), 2010 WL 5312204, at *2 ("Procedural differences among nations also affect the ability of a company

Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices (*"International Investigations Principles"*) was developed to help fill that gap.

The following three examples illustrate realistic investigative situations and demonstrate the need for a set of principles and best practice guidelines for practitioners involved in international data Processing and transfer in the context of civil Government and Internal Investigations.

Example 1: A publicly traded global corporation based in the U.S. has operations in the U.K.; the U.K. corporation has a Brazilian subsidiary that is overseen by the U.K. corporation's Spanish subsidiary. If the Brazilian subsidiary engages in a foreign bribery scheme, the U.S. ultimate parent could simultaneously be subject to a Foreign Corrupt Practices Act (FCPA) investigation in the U.S., a U.K. Bribery Act investigation, and potentially two additional corruption investigations, one in Brazil and one in Spain. Relevant documents might be located in Spain and subject to Spanish Data Protection Laws. Other documents could be subject to Brazil's Data Protection Laws. As is common in the U.S., the ultimate-parent corporation, upon learning of the corruption and conducting an Internal Investigation, may decide to notify the U.S. Department of Justice (DOJ) and the U.S. Securities and Exchange Commission (SEC), which would expect the corporation to conduct an Internal Investigation, and then share the results with the agencies in order to obtain credit for cooperation and avoid criminal charges or reduce potential fines and penalties. The ultimate parent may also decide to share the results with the U.K. Serious Fraud Office (SFO) for the same reasons. To conduct the investigation,

---

to address suggestions of internal wrongdoing. . . . That does not make doing internal investigations impossible, but adhering to the requirements of local data privacy laws and restrictions in conducting internal investigations can add significantly to their cost and duration.").

the corporation would collect relevant documents and data and conduct interviews in multiple jurisdictions. Materials might potentially be produced to the DOJ/SEC, the SFO, and to Brazilian and Spanish anticorruption authorities. Complicating the corporation's defense and response is the potential for a "dawn raid" in the country where the corruption is alleged—here, Brazil. One major issue, among many facing the corporation, is how it can effectively and efficiently collect and review relevant materials and negotiate its response with multiple countries' enforcement agencies while giving due respect to each country's Data Protection Laws.[11]

11. This example is not fanciful. *See* Lindsay B. Arrieta, *How Multijurisdictional Bribery Enforcement Enhances Risks for Global Enterprises*, BUSINESS LAW TODAY (June 2016), http://www.americanbar.org/publications/blt/2016/06/08_arrieta.html (describing the "recurring and ongoing investigations and enforcement actions" against French corporation Alstom S.A. in multiple jurisdictions including the U.S., U.K., Switzerland, and Brazil: in 2011, Swiss authorities fined Alstom approximately $40 million for bribery charges; in 2014, the corporation pled guilty to FCPA violations with penalties of over $772 million in the U.S.; the SFO charged Alstom with bribery in Lithuania and arrested seven executives on criminal charges; Alstom also was subject to a corruption probe in Brazil); *see also* U.S. Dep't of Justice Press Release, Alstom Sentenced to Pay $772 Million Criminal Fine to Resolve Foreign Bribery Charges (Nov. 13, 2015), https://www.justice.gov/opa/pr/alstom-sentenced-pay-772-million-criminal-fine-resolve-foreign-bribery-charges (outlining bribery charges in connection with state-owned entity projects in Indonesia, Egypt, Saudi Arabia, the Bahamas, and Taiwan). Commenting on the increased collaboration among various agencies in transnational enforcement activities, one practitioner observed: "[T]he Justice Department's Criminal Division and the SEC work together with the Serious Fraud Office in the U.K., the Investigating Magistrates in France, and other authorities in Germany and elsewhere in Europe. In the future, it is likely that there will be increased cooperation in corruption and fraud cases with the authorities in Asia, with China currently being somewhat of a question mark." Terwilliger, *supra* note 10, at *10.

Example 2: A multinational corporation intends to acquire another multinational corporation and the proposed transaction is subject to merger-clearance procedures in multiple jurisdictions. If the deal is subject to U.S. pre-merger review and either antitrust agency makes a "second request,"[12] within a very short period the corporation may need to provide a broad scope of information about the proposed transaction, the affected lines of commerce, and the likely competitive effects of the proposed transaction, including emails and other business records maintained by individual custodians. Because the target corporation does business in multiple jurisdictions outside the U.S., information may need to be collected, reviewed, and produced promptly in order to meet critical financing or business deadlines—and there may be great business pressure to complete the regulatory work necessary to proceed with the deal.[13] These business pressures could lead a corporation to take data privacy protection shortcuts in order to "clear the deal."

Example 3: Corporations have a vital interest in protecting their reputations, ensuring that their resources are not being misused or attacked, and ensuring that they are in compliance

12. *See* Fed. Trade Comm'n, *Merger Review*, FED. TRADE COMM'N, http://www.ftc.gov/news-events/media-resources/mergers-and-competition/merger-review (last visited May 16, 2018) (describing process of merger review including potential for second requests).

13. *See* Melissa Lipman, *5 Tips for Deal Makers to Smooth the 2nd Request*, LAW360 (Mar. 17, 2014), http://www.law360.com/articles/519230 (subscription required). Lipman's five tips are: (1) narrow the scope of the second request by asserting an appropriately narrow market or product definition; (2) hand over information quickly; (3) acknowledge a problem if it exists; (4) know how far your client will go to fix it; and (5) remember an adverse staff recommendation isn't the end. Of course, knowing whether a client has a problem that should be disclosed to regulators requires a quick yet thorough investigation of the products and markets at issue while under the pressure of the second request response deadline.

with their legal, moral, and social obligations. Indeed, this is one area in which their civil interests have the potential to overlap with criminal law violations. For example, under the U.S. Federal Sentencing Guidelines, a corporation may receive a reduction in fines of up to 95 percent if it has implemented an effective compliance program.[14] Multinational corporations often design corporate compliance programs to meet the requirements of those guidelines. To be effective, a compliance program must include a means of investigating potential misconduct and auditing and monitoring the program itself.[15] To achieve these objectives, corporations may monitor certain types of employee

---

14. *See* Paula Desio, *An Overview of the Organizational Guidelines*, U.S. SENTENCING COMM'N, http://www.ussc.gov/sites/default/files/pdf/training/organizational-guidelines/ORGOVERVIEW.pdf (describing the impact of compliance programs on sentencing).

> [W]hen the Commission promulgated the organizational [sentencing] guidelines, it attempted to alleviate the harshest aspects of this institutional vulnerability by incorporating into the sentencing structure the preventive and deterrent aspects of systematic compliance programs. The Commission did this by mitigating the potential fine range—in some cases by up to 95 percent—if an organization can demonstrate that it had put in place an effective compliance program. *This mitigating credit under the guidelines is contingent upon prompt reporting to the authorities and the non-involvement of high level personnel in the actual offense conduct.*

Id. (emphasis added). To self-report and show that high-level personnel were not involved in the criminal offense, an Organization must be able to investigate wrongdoing, identify who was involved, and provide evidence supporting its conclusion to the relevant prosecuting agency.

15. An effective compliance program must include "[r]easonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal . . . [and] [r]easonable steps to respond to and prevent further similar offenses upon detection of a violation." *Id.*; *see also* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1, U.S.

conduct worldwide to help prevent and detect violations of the corporation's business conduct policies, whether the conduct relates to fraud, conflicts of interest, embezzlement, corruption, harassment, treatment of confidential information, or other behaviors that could violate corporation policies and the law. As monitoring tools become more sophisticated, it is reasonable to assume that the corporation may review Protected Data as part of its compliance monitoring functions and that a surveillance program may conflict with data protection and other laws.[16]

The bottom line is this: Government or Internal Investigations raise issues that are not solved by strategies designed to balance the tension between discovery and privacy considerations in civil litigation. To appreciate why this is so, we must consider the procedural and legal differences between civil litigation and both Government and Internal Investigations. We examine the differences, *infra.*

SENTENCING COMM'N (2015), http://www.ussc.gov/guidelines/2015-guidelines-manual/2015-chapter-8.

16. *See, e.g.*, Délibération n° 2014-042 du 30 janvier 2014 modifiant l'autorisation unique n° 2005-305 du 8 décembre 2005 n° AU-004 relative aux traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle [Deliberation n° 2014-042 of 30 January 2014 modifying the single authorization n° 2005-305 of 8 December 2005 n° AU-004 relating to automated Processing of personal data implemented within the framework of warning devices], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANCAISE [J.O.][Official Gazette of France], Feb. 11, 2014, https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=656E3F9168B3D0B618C7903416BB718B.tpdjo04v_2?cidTexte=JORFTEXT000028583464&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000028583033/ (regarding the 2014 amendments to whistleblower hotline requirements in France).

I. INVESTIGATIONS DIFFER FROM LITIGATION IN IMPORTANT WAYS

A. Public Policy Considerations

Processing data when there are broad prohibitions against doing so is challenging, even when there appear to be exceptions that permit it. For example, the General Data Protection Regulation (GDPR)[17] allows the Processing of otherwise Protected Data where the Data Controller has a "legitimate interest" that is not overridden by the "fundamental rights" of Data Subjects; to determine whether the exception applies a party must balance the interests and rights of all concerned parties.[18]

---

17. GDPR art. 6(f).

18. Previously, the Article 29 Working Party provided guidance on this issue under a parallel provision in the EU Data Protection Directive, Article 7. *See* Article 29 Data Protection Working Party, *Working Document 1/2009 on Pre-Trial Discovery for Cross-Border Civil Litigation*, at 8–9, 00339/09/EN/WP 158 (Feb. 11, 2009), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf [hereinafter WP 158]. In its *Opinion 06/2014 on the Notion of legitimate interest of the data controller under Article 7 of the Directive 95/46/EC*, 19844/14/EN/WP 217 (Apr. 9, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, the Article 29 Data Protection Working Party expanded further on this balancing analysis.

> It is also important to emphasise that [Directive] Article7(c) refers to the laws of the European Union or of a Member State. Obligations under the laws of third countries (such as, for example, the obligation to set up whistleblowing schemes under the Sarbanes-Oxley Act of 2002 in the United States) are not covered by this ground. To be valid, a legal obligation of a third country would need to be officially recognised and integrated in the legal order of the Member State concerned, for instance under the form of an international agreement. On the other hand, the need to comply with a foreign obligation may represent a legitimate interest

Although commentators have explored that balance in the context of civil litigation, much of their analysis is inapplicable to Government and Internal Investigations.[19] Determining the appropriate balance requires exploring and weighing a range of public policy issues that are not necessarily present in litigation.

In litigation, the primary public policy objective is fair determination of party rights. Practitioners understand that the approach to litigation varies significantly between the U.S. and the EU, and those variations, especially the concept of broad discovery in the U.S., account in part for the tension related to cross-border data transfers in that context. In Government Investigations, other important government and public (versus private) considerations are at stake, including the means by which governments enforce national policies (e.g., enforcement of compe-

---

> of the controller, but only subject to the balancing test of [Directive] Article 7(f), and provided that adequate safeguards are put in place such as those approved by the competent data protection authority.

Id. at 19 (citation omitted).

19. Close to the time of publication of the *International Investigations Principles*, the Article 29 Working Party provided guidance on transfer derogations under GDPR art. 49 indicating that a derogation may be available for certain investigations. *See* Article 29 Data Protection Working Party, *Guidelines on Article 49 of Regulation 2016/679* (Feb. 6, 2018), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614232 [hereinafter WP 262]. Public comments were invited until March 26, 2018). While stressing that derogations must be narrowly construed, this preliminary version of WP 262 notes that the GDPR art. 49(1)(e) derogation for transfers necessary for the establishment, exercise, or defense of legal claims may cover an administrative investigation in a third country including, for example, antitrust law, corruption, and insider trading investigations; or for obtaining a reduction or waiver of a fine in, for example, an antitrust investigation; or for seeking approval for a merger.

tition policy, government regulation of corporate financial matters, financial regulation of banking institutions, anticorruption enforcement, money laundering, and so forth).

In the case of Government Investigations, nations have an obvious substantial interest in protecting their economies, the flow of commerce within their borders, and the health, safety, and welfare of their citizens and residents, both human and corporate. Statutes, regulations, and court decisions reflect the societal values and beliefs of the countries that create them. They are among the principal means by which a government establishes national social and economic policy and standards of conduct for its citizens, resident aliens, and Organizations that do business directly or indirectly in the country. A nation's law enforcement actions generally, and its law enforcement investigations in particular, are an important means by which it advances the public interest, ensures that its values and principles are honored, and ensures that its citizens and Organizations are protected from those who do not share the same values and principles, or are unwilling to abide by them.[20]

In the case of Internal Investigations, the primary public policy objective is to ensure that corporations engage in appropriate corporate governance both to protect their shareholders, employees, and other stakeholders and to protect their own ability to do business, especially where their licenses or operating permits depend on their compliance with local law. Corporate governance public policy considerations differ markedly between

20. *See, e.g.*, U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR INTERNATIONAL ENFORCEMENT AND COOPERATION ¶ 1 *et seq.* (Jan.13, 2017), https://www.justice.gov/atr/internationalguidelines/download ("To protect U.S. consumers and businesses from anticompetitive conduct in foreign commerce, the federal antitrust laws have applied to 'commerce with foreign nations' since their inception.") (citation omitted) [hereinafter ANTITRUST GUIDELINES].

the U.S. and Europe. In the U.S., principles of corporate governance have developed through a combination of statutes; the Federal Sentencing Guidelines; rules of the Securities and Exchange Commission; rules of the various stock exchanges, including the New York Stock Exchange Governance Rules; regulations under federal contracting law; banking regulations; and development of the common law of fiduciary duty.[21] Today, it is well accepted in the U.S. and a few other countries, such as the U.K. and the Netherlands, that corporations must have business-conduct policies and associated internal procedures designed to prevent, detect, and remediate employee and corporate misconduct in all aspects of a corporation's global operations: financial, human resources, manufacturing, sales, promotion, and more.[22] In contrast, "[i]n Europe, the emphasis

21. *See generally* RICHARD M. STEINBERG, GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE: IT CAN'T HAPPEN TO US—AVOIDING CORPORATE DISASTER WHILE DRIVING SUCCESS (2011); ANTHONY TARANTINO, GOVERNANCE, RISK, AND COMPLIANCE HANDBOOK: TECHNOLOGY, FINANCE, ENVIRONMENTAL, AND INTERNATIONAL GUIDANCE AND BEST PRACTICES (2008); Contractor Code of Business Ethics and Conduct, 48 C.F.R. § 52.203–13 (2015); ABA SECTION OF PUBLIC CONTRACT LAW, GUIDE TO THE MANDATORY DISCLOSURE RULE: ISSUES, GUIDELINES, AND BEST PRACTICES (2010).

22. *See generally Responsible Business,* INT'L CHAMBER OF COMM., https://iccwbo.org/global-issues-trends/responsible-business/ (last visited Apr. 3, 2018) (**"**[M]ore and more businesses are bolstering their principles and policies relating to transparency, ethics and risk management—not just for legal compliance but as an integral element of good management. Enterprises doing business with integrity are more likely to attract and retain motivated employees and attract investors who put their own reputation on the line."); *Corporate Responsibility*, INT'L CHAMBER OF COMM., https://iccwbo.org/global-issues-trends/responsible-business/corporate-responsibility/ (last visited Apr. 3, 2018) ("Companies today are increasingly approaching corporate responsibility as part of their overall policy to manage activities.").

is on voluntary internal controls rather than enforcement of controls by statutes."[23] Likewise, the scope of potential corporate liability differs in Europe; and the potential for corporations to be held liable for the acts of non-senior management is much lower in Europe than in the U.S.[24] Arguably, such differences in

---

23. *Is Corporate Governance Better Across the Atlantic?*, VALUE WALK (Jan. 11, 2013, 12:55 PM), http://www.valuewalk.com/2013/01/is-corporate-governance-better-across-the-atlantic/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+valuewalk%2FtNbc+%28Value+Walk%29; *see also* Global Corporate Governance Forum, *The EU Approach to Corporate Governance: Essentials and Recent Developments*, INTERNATIONAL FINANCE CORPORATION (Feb. 2008), http://www.ifc.org/wps/wcm/connect/f515ff804af4fc7da869b9b94e6f4d75/IFC_EUApproach_Final.pdf?MOD=AJPERES.

24. *See* Clifford Chance LLP, *Corporate Liability in Europe* (Jan. 2012), http://www.cliffordchance.com/content/dam/cliffordchance/PDFs/Corporate_Liability_in_Europe.pdf.

> In all jurisdictions where the concept of corporate, or quasi-corporate, criminal liability exists, it is, with the exception of the UK and the Netherlands, a relatively new concept. Those countries apart, France was the first European country to introduce the concept of corporate criminal liability in 1994, followed by Belgium in 1999, Italy in 2001, Poland in 2003, Romania in 2006 and Luxembourg and Spain in 2010. In the Czech Republic, an act creating corporate criminal liability has just become law as of 1 January 2012. Even in the UK where criminal liability for corporate entities has existed for decades, many offences focusing on corporate criminal liability have been created in recent years. In the Netherlands, until 1976 only fiscal offences could be brought against corporate entities. The movement towards criminal liability for corporate entities is likely to continue. . . . The basis or proposed basis of liability for corporate entities within those countries where liability exists (or is proposed) rests on the premise that the acts of certain employees can be attributed to a corporate entity. The category of employees which can trigger corporate liability is limited in some jurisdictions to those with management responsibilities and the act must

governance policy may cause U.S. multinational corporations to engage in Internal Investigations and to assess whether corporate governance obligations require the self-reporting of misconduct to regulators, where EU corporations might not. The point is simply this: corporate governance—as that concept is understood by U.S.-based multinationals—requires review of business documents in order to manage the corporation and to identify and remediate inappropriate behaviors.

For example, every FCPA investigation of a multinational Organization necessarily includes a cross-border component requiring collection and review of data from employees in countries alleged to be involved—and these multijurisdictional investigations are increasing.[25] As one commentator explains:

> With the rollout of a new agency to combat corruption in France and the implementation of anti-corruption legislation in Brazil, it appears that the landmark UK Bribery Act and the U.S. Foreign Corrupt Practices Act (FCPA) are paving the way for legal reforms across the globe. These two statutes, with which corporate counsel and compliance officers have become intimately acquainted, have long been regarded as the pinnacles of anti-corruption legislation. For years they stood alone,

---

> generally occur within the scope of their employment activities. The act must also generally be done in the interests of or for the benefit of the corporate entity.

Id. at 2.

25. Matthew Villmer, *4 Practice Areas Generating Big Billable Hours*, LAW360 (Apr. 24, 2014), http://www.law360.com/competition/articles/524698?nl_pk=a0916a62-52d3-4f6b-a766-229071168fb0&utm_source=newsletter&utm_medium=email&utm_campaign=competition (subscription required) (discussing practice areas such as investigations under the Foreign Corrupt Practices Act that are "growing by leaps and bounds").

> but now in addition to France and Brazil, a dozen countries are planning to follow suit with their own legislation.[26]

U.S. regulators often expect Organizations to conduct Internal Investigations and provide the results to the SEC and DOJ in order to earn "cooperation" credit.[27] Whether an Organization receives cooperation credit will depend, in part, on its providing authorities with relevant evidence and identifying relevant actors inside and outside of the Organization. This form of cooperation often requires the Processing, transfer, and disclosure of Protected Data.[28]

---

26. *See* Amit Katyal, *Anticorruption Laws Sweeping Across the Globe*, LAW.COM (Feb. 24, 2014), http://www.law.com/sites/articles/2014/02/24/anti-corruption-laws-sweeping-across-the-globe/ (subscription required).

27. According to the U.S. Department of Justice:

> Under DOJ's *Principles of Federal Prosecution of Business Organizations*, federal prosecutors consider a company's cooperation in determining how to resolve a corporate criminal case. Prosecutors consider whether the disclosure was made voluntarily and timely, as well as *the company's willingness to provide relevant information and evidence and identify relevant actors inside and outside the company, including senior executives*. In addition, prosecutors may consider a company's remedial actions, including efforts to improve an existing compliance program or *appropriate disciplining of wrongdoers*. A company's remedial measures should be meaningful and illustrate its recognition of the seriousness of the misconduct, for example, *by taking steps to implement the personnel, operational, and organizational changes necessary* to establish an awareness among employees that criminal conduct will not be tolerated.

U.S. DEP'T OF JUSTICE, CRIMINAL DIVISION AND U.S. SECURITIES AND EXCHANGE COMM'N, A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT, 54 (Nov. 14, 2012) (emphases added).

28. *Id*.

The regulatory and corporate governance underpinnings of Government Investigations and Internal Investigations make clear that the policy considerations affected by cross-border data transfers in those contexts differ from considerations in the litigation context.

B. Specific Considerations: Government Investigations

From the perspective of Investigating Authorities, the foremost consideration for government-initiated civil investigations is to ensure that the government gains access to information needed to exercise regulatory responsibilities;[29] they will object if Organizations appear to use Data Protection Laws to stonewall investigations.[30] Investigating Authorities prefer to obtain

---

29. The *International Investigations Principles* addresses only those situations in which an Investigating Authority requires the Organization to provide information and documents, and the Organization must determine how best to cooperate while still complying with relevant Data Protection Laws. Consequently, the *International Investigations Principles* does not address how an Organization should respond to a search warrant or a dawn raid, Mutual Legal Assistance Treaty (MLAT) arrangement, or the exercise of police powers generally. Article 8(5) of the EU Data Protection Directive states: "Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards." *See* Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, 2008 O.J. (L 350) (defining "'competent authorities' [as Member State] agencies or bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union, as well as police, customs, judicial and other competent authorities of the Member States that are authorized by national law to process personal data within the scope of this Framework Decision").

30. For example, China's State Secrets Law was invoked in an attempt to block the SEC from obtaining documents in a securities fraud investigation

Organization cooperation and not to resort to other means of obtaining relevant information. U.S. regulators' requests for information and documents are initiated by agencies pursuant to their statutory authority.[31] Investigating Authorities have a number of tools available for obtaining information, including administrative subpoenas, civil investigative demands, access letters, special orders, and turn-over demands. The time al-

---

of the Chinese affiliates of BDO and the "Big Four" accounting firms—Ernst & Young, KPMG, Deloitte Touche Tohmatsu, and PricewaterhouseCoopers. In 2011 and 2012, the SEC sought documents and audit papers from the Chinese affiliates of these accounting firms to investigate suspected securities fraud by certain China-based issuers. Citing China's State Secrets Law and express directions from the China Securities Regulatory Commission (SCRC), the accounting firms refused to produce the requested documents. After negotiations reached an impasse, the SEC commenced administrative proceedings against the accounting firms, alleging violations of Section 106 of Sarbanes-Oxley Act. In January 2014, an administrative law judge issued a 112-page decision, concluding that the accounting firms had violated § 106 by willfully refusing to comply with the SEC's demands. As a sanction, the judge banned the firms from practicing before the SEC for six months. *See, In re* BDO China Dahua et al., Admin. Proc. Nos. 3-14872, 3-15116, Initial Decision (Jan. 22, 2014), https://www.sec.gov/alj/aljdec/2014/id553ce.pdf. The matter was finally resolved in early 2015. *See, In re* BDO China Dahua et al., Admin. Proc. Nos. 3-14872, 3-15116, Settlement Order (Feb. 6, 2015), https://www.sec.gov/litigation/admin/2015/34-74217.pdf. *See also* SEC Press Release, SEC Imposes Sanctions Against China-Based Members of Big Four Accounting Networks for Refusing to Produce Documents (Feb. 6, 2015), *available at* www.sec.gov/news/pressrelease/2015-25.html (Under the settlement with the SEC, the SCRC will act as a conduit, enabling the SEC to gain access to Chinese firms' audit documents.).

31. *See* David C. Shonka, *Responding to the Government's Civil Investigations,* 15 SEDONA CONF. J. 1 (2014). Certain government investigative requests are voluntary, others judicially enforceable, and still others somewhere between voluntary and compulsory in that the recipient is not "compelled" to provide information, but is forbidden from taking certain actions unless it provides whatever information may be required. *Id.* at 3–5.

lowed to respond may be significantly compressed in the Government Investigation context. And some Organizations accordingly believe that regulators do not understand the conflicting obligations placed on Organizations when regulators issue broad requests for information, including Protected Data, "wherever it may be."

In contrast, non-U.S. regulators may more often turn to police-like powers to collect information, resorting in particular to "dawn raids" in the context of competition law and corruption investigations.[32] To support collection of evidence in that context, EU investigators may rely on legal authorities that are not available either to the Organization under investigation or to foreign investigators.[33]

---

32. *See, e.g.*, Caroline Binham, *Big increase in SFO raids signals tougher tactics,* FINANCIAL TIMES (June 9, 2013), https://www.ft.com/content/21ae857a-cf9a-11e2-a050-00144feab7de (subscription required) (reporting that the SFO conducts raids at the investigation stage to collect evidence); Jack Ewing and Bill Vlasic, *German Authorities Raid U.S. Law Firm Leading Volkswagen's Emissions Inquiry*, N.Y. TIMES (Mar. 16, 2017), https://www.nytimes.com/2017/03/16/business/volkswagen-diesel-emissions-investigation-germany.html; Practical Law Competition, *Investigations and Dawn Raids by the CMA: A Quick Guide*, PRACTICAL LAW, https://uk.practicallaw.thomsonreuters.com/6-380-1599?__lrTS=20170427190502429&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1&ignorebhwarn=IgnoreWarns (last visited May 15, 2018) (noting the UK Competition and Market Authority's "wide powers of inspection" include conducting dawn raids); Bloomberg, *HK's anti-corruption body raids JPMorgan CEO's office*, BUSINESS STANDARD (Mar. 31, 2014), http://www.business-standard.com/article/international/hk-s-anti-corruption-body-raids-jpmorgan-ceo-s-office-114033100012_1.html (describing example of a local jurisdiction implementing a dawn raid in the context of a multi-country, anti-corruption investigation).

33. Regulation (EC), No. 45/2001, which has to be adapted to Article 2(2)(b) and 2(3) of the GDPR, governs data protection by EU institutions that does not fall under Chapter 2 of Title V of the Treaty on European Union (TEU). GDPR, art. 2(2)(b) and 2(3).

Organizations accordingly must develop protocols that address their production of information to government agencies within reasonable timeframes and mitigate the privacy impact on affected Data Subjects. Best practices should reflect, among other things, the following realities differentiating investigations from litigation:

- Government Investigations are conducted in a confidential manner in order to protect the integrity of the investigation and the privacy interests of the subjects. Once the government files a case in court, protective orders are routinely sought to protect sensitive personal data and other confidential information from public disclosure.[34] In addition, rules of procedure provide for the sealing of personal and other confidential information.[35]
- Government Investigations often are not confined to conduct that occurred within one nation's boundaries.
- Government Investigations may occur in parallel with other countries' investigations (criminal or civil) and such parallel proceedings may or may not be cooperative undertakings.
- Government Investigations may extend over a lengthy period and change scope over time.
- Government Investigations may be broad in scope and appear to have few limits.
- Because Investigating Authorities are typically not required to set out a specific claim or legal theory when

34. *See* FED. R. CRIM. P. 16(d), 49.1; FED. R. CIV. P. 26(c).

35. *See* FED. R. CRIM. P. 49.1(d); FED. R. CIV. P. 26(c).

they request data, it may be difficult for an Organization to assess the relative importance of documents covered by a data request. However, recipients of government demands are typically informed of the general nature of the conduct under investigation and the potential statutory violations. For example, by statute, each Civil Investigative Demand (CID) issued by the DOJ or the Federal Trade Commission (FTC) must state the nature of the conduct or activities under investigation and the law pertaining to such conduct or investigation.[36] Further, the CID statutes require that documents be described with "such definiteness and certainty as to permit such material to be fairly identified."[37]

- Government Investigations are not usually the subject of judicial supervision, but some statutes allow the recipient of a government demand to file a motion with the court to quash or modify the demand. The grounds for doing so, however, are limited. For example, the recipient of a CID from the DOJ may seek to quash or modify a demand on the grounds of burden, relevance, or privilege.[38] In contrast, the recipient of a subpoena or a CID from the FTC may only proceed administratively to quash or limit process and may not seek "pre-enforcement review" from a

36. 15 U.S.C. §§ 57b-1(c)(2), 1312(b)(1); *see* 16 C.F.R. § 2.6.

37. 15 U.S.C. §§ 57b-1(c)(3)(A), 1312(b)(2)(A); *see* 16 C.F.R. § 2.7(b).

38. 15 U.S.C. §§ 1312, 1314(b); *see also* FED. R. CIV. P. 26(b), 45(d); FED. R. CRIM. P. 17(c)(3); ANTITRUST DIV., DEP'T OF JUSTICE, ANTITRUST DIVISION MANUAL, Chapter III, Part E.8., 69–72 (5th ed., last updated Apr. 2015), https://www.justice.gov/atr/file/761141/download.

court.[39] However, regulatory demands are not always self-enforcing; and if an Organization refuses to comply with an agency request (except when statutory or automatic penalties attach to noncompliance), the Investigating Authority must seek judicial intervention to enforce its requests. Only at that point might a court provide even limited oversight.

- Investigating Authorities may assess cooperation credit based on an Organization's willingness to provide information and identify employees and others involved in the matter under investigation.
- Investigating Authorities may use a combination of police powers and civil information requests to gather evidence.

Courts are not always available to assist Organizations in their attempt to balance their regulatory-disclosure obligations with their obligations under Data Protection Laws. In the U.S., for example, agencies enjoy broad powers to seek information from Organizations they regulate, and judicial supervision of agency requests is very limited. Investigating Authorities may request information even if there is no certain legal violation "because of the important governmental interest in the expeditious investigation of possible unlawful activity."[40] For example, in assessing a challenge to an FTC administrative subpoena, U.S. courts have observed that "[a]lthough the court's function

39. *See* 16 C.F.R. § 2.7. Under Commission Rule 2.7, a party may raise objections to an FTC subpoena by filing a petition to limit or quash. Such petitions may be resolved by a designated Commissioner, and the designated Commissioner's ruling may thereafter be appealed to the full Commission.

40. FTC v. Texaco, Inc., 555 F.2d 862, 872 (D.C. Cir. 1977) (en banc) (internal citation omitted).

is 'neither minor nor ministerial,'"[41] it is "strictly limited"[42] to determining whether the FTC can demonstrate that the subpoena is "'within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant'" to the matter under investigation.[43]

Not only is government authority broad and court review limited, but it also may not serve an Organization's interest to seek judicial supervision over production disputes with Investigating Authorities. From a defense point of view, government investigative requests are often challenging. Timing may be crucial. The Organization may not want to force the Investigating Authority to turn to a court when an impasse appears because the Organization may not want to irritate the authority with a legal challenge to its request. Any party that pushes the agency into court to seek judicial enforcement runs the risk of damaging its working relationship with the authority and reducing any cooperation credit it might otherwise receive. It also runs the risk of adverse publicity from not cooperating with a Government Investigation. Thus, judicial oversight of data requests is unlikely. Although judicially supervised protective orders are a best practice regularly used in litigation to govern the use and disclosure of documents and information produced during discovery, they are rarely, if ever, available in Government or Internal Investigations. Various statutes, however, may provide protections regarding the use and disclosure of information provided to the government.[44]

---

41. *Id.* (quoting Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 217 (1946)).

42. *See id*. at 872.

43. *See id*. (quoting United States v. Morton Salt Co., 338 U.S. 632, 652–53 (1950)).

44. *See* ANTITRUST GUIDELINES, *supra* note 20, at ¶¶ 5.1.2, 5.1.4; *see, e.g.*, FED. R. CRIM. P. 6(e); 15 U.S.C. §§ 18a(h), 46(f), 57b-2, 1313(c)–(d), 1314(g); *see also* 5 U.S.C. §§ 552a(b), 552(b)–(c).

Further, when disputes arise over what information and documents the Organization should provide in response to a government request, the government may be in a particularly strong negotiating position. For example, in a merger-related second request, Organizations have a strong incentive to "get the deal done." Similarly, if the Organization faces potential criminal exposure because of employee misconduct, the consequences of complying with Investigating Authority requests may be more important to the Organization than they would be in private litigation. There may be a sense of greater seriousness, with the Organization wanting to ensure that it does the right thing (in terms of both compliance and public perception). Tactical considerations often shape the response to a government request.

In some jurisdictions, particularly the U.S., Organizations may be able to engage in arm's length, candid discussions with the Investigating Authority seeking to focus the investigation and limit productions to only the most necessary and relevant data and information, especially as the Organization may be concerned that produced materials may be disclosed in subsequent civil lawsuits (e.g., a damages suit following an antitrust investigation).[45] Statutory time limits, limited budgets, and heavy workloads also create incentives for Investigating Authorities to respond to legitimate, reasoned, and well-supported requests to limit an investigation. Despite these incentives, authorities are not obligated to cooperate. Further, one might think that if an Organization is being investigated by a U.S. authority and wants to cooperate, it should obtain the cooperation of a Data Protection Authority in the relevant country. However, some fear that such cooperation during an ongoing investigation might come at the price of triggering an investigation in

45. *See* Shonka, *supra* note 31, at 8–9.

that country for the same conduct under investigation in the U.S., or may otherwise compromise the confidentiality that often surrounds such investigations or trigger a separate investigation relating to violation of Data Protection Laws in connection with complying with the U.S. investigation.

Conversely, some Investigating Authorities have expressed concern about the potential for tactical abuse of Data Protection Laws in Government Investigations. Investigating Authorities may be concerned that an Organization may be more inclined to use Data Protection Laws as a defense to production in the government context. An Organization's tactical decisions about whether—and to what extent—to cooperate may depend on its business and legal interests, the type and importance of data requested, whether the matter will resolve quickly or slowly, and the probability that the investigation might otherwise resolve (with or without cooperation) before any data is produced. However, delay does not usually result in avoidance of producing data to the Investigating Authority. To the contrary, it may prolong the investigation by forcing the government to seek judicial enforcement, thus forgoing opportunities to narrow the scope of the investigation through candid discussions. In addition, expenses increase, given the costs of court enforcement actions.

Similarly, to the extent Data Protection Laws give Data Subjects legal rights and remedies, such as rights to access, correction, and deletion, those laws may potentially give Data Subjects the ability to prevent or at least delay the ability of their employers or an Investigating Authority to obtain relevant but incriminating or embarrassing documents. An employee may attempt

to use these laws to subvert or delay justified adverse employment action or even criminal prosecution.[46] Such attempts interfere with the ability of Organizations to cooperate with the government in detecting and ending wrongdoing, and ultimately harm the Organization, consumers, and society.

Organizations responding to agency requests for information must also consider the potential for obstruction of justice charges. Such cases are usually predicated on willful loss or destruction of evidence, interference with potential witnesses, or affirmative obstruction of an investigation. A failure to produce all relevant non-privileged documents could result in an obstruction of justice charge against the Organization or its lawyers—even if the Organization maintains a good-faith belief that the information can be legally withheld.[47] Of course, this

46. Other legal obligations may affect the employees' responsibility to cooperate with Internal Investigations in European countries. For example, certain European labor laws impose regulations as to how investigations may proceed, but a discussion of such laws is beyond the scope of this paper. *See* David C. Shonka, *Producing Information from the EU to U.S. Government Agencies,* DIGITAL DISCOVERY & E-EVIDENCE (December 21, 2017) [hereinafter *Producing Information*].

47. For example, a corporate lawyer was indicted, in part, for failing to produce documents she concluded were not required to be produced based on advice of outside counsel. *See DOJ Failed Case against GSK Staff Lawyer Lauren Stevens: Lessons Learned*, POLICY AND MEDICINE (last updated May 6, 2018), http://www.policymed.com/2012/01/doj-failed-case-against-gsk-staff-lawyer-lauren-stevens-lessons-learned.html#sthash.XcFe8TXJ.dpuf ("In *Stevens*, the judge specifically relied on favorable evidence found in house counsel's correspondence with outside counsel. The documents showed that outside counsel was intimately involved with GSK's document production that triggered Steven's [sic] indictment. For example, the judge pointed to letters and emails between in house counsel and outside counsel that showed that in house counsel was diligently relying on outside counsel's advice."). The lawyer was subsequently acquitted, but the issue remains of concern to in-house counsel. Imagine that in-house counsel locates incriminating documents as part of an internal FCPA investigation but decide not to disclose

presents a dilemma for an Organization if the mere preservation of data is considered to be "Processing" within the meaning of applicable Data Protection Laws.

Complicating matters further, multiple countries' Investigating Authorities may be involved in an area of investigation. Unlike discovery in the U.S. court or administrative litigation context, where the typical pattern involves cross-border transfers to the U.S., Government Investigations may involve reciprocal sharing amongst countries, each with different laws governing such exchanges. When one government becomes interested, others may follow.[48] This often appears in the context of antitrust review of mergers, as well as in the context of other antitrust and anticorruption investigations. Such matters require the subject Organization to manage cross-border, document-transfer issues in multiple jurisdictions and thus raise complex and challenging issues of case management, document Processing, review, transfer, and coordination. Indeed, an Organization may find itself in the awkward position of submitting different sets of documents to different Investigating Authorities in order to comply with different countries' Data Protection Laws. And if regulators in one country, especially outside the U.S., use search warrants to collect evidence and then share that evidence with other involved governments, the Organization's ability to collect (and use in its defense) the very

---

them to the DOJ/SEC because of relevant Data Protection Laws. The Organization (and its counsel) are thus in a worse position as a result of attempting to cooperate.

48. An interesting example of international cooperation is the provision in the U.S. SAFE WEB Act, 15 U.S.C. § 46(j) that allows the FTC to provide non-U.S. law enforcement agencies with investigation assistance. *See In re* FTC, No. MJG-13-mc-524, 2014 WL 3829947, at *4 (D. Md. Aug. 4, 2014) (enforcing a subpoena issued under 28 U.S.C. § 1782 to permit the FTC to obtain information on behalf of the Canadian Competition Bureau).

documents that Investigating Authorities have already obtained may be hindered, or even defeated.

Many of the issues involved in Government Investigations simply do not arise in the context of litigation-related transfers. Developing and implementing a sound framework and following best practices for investigations are important to global business operations and compliance functions.

C. Specific Considerations: Internal Investigations

As set out previously, Organizations that implement effective compliance programs are entitled—under certain circumstances—to reductions in fines that would otherwise be assessed for criminal conduct. As a result, Organizations place great weight on "finding and fixing" compliance-related issues. U.S. hotline reports, whistleblower allegations, and the SEC's Dodd-Frank rules require prompt investigations to permit Organizations to manage their compliance obligations. In addition, various U.S. whistleblowing, labor, employment, and civil rights laws protect employees' rights in the workplace and require employers to protect those rights. Similarly, other countries also have "leniency programs" for Organizations that self-report violations of laws, including laws protecting workers', and other, rights. Programs like these provide Organizations strong incentives to monitor internal behavior and report any misconduct they find. Of course, such internal policies further important government and social interests in promoting lawful conduct and sanctioning wrongdoers, while conserving government resources.

However, satisfying this corporate governance obligation requires corporations to investigate employee misconduct and analyze otherwise Protected Data to determine whether misconduct has occurred—conduct that often involves serious, and potentially criminal, matters such as allegations of competition

law violations, tender violation issues, export control issues, fraud, embezzlement, international corruption, and many others.

Investigative needs might often conflict with the underlying principles of consent and transparency incorporated into Data Protection Laws. Indeed, if abused and improperly used as a shield, such laws have the potential to stymie the Organization or counsel advising the Organization. The Organization or its counsel may be prevented from conducting a thorough, meaningful Internal Investigation or from providing full and meaningful advice to management. For example, it makes no sense to give notice to an employee before investigating potential wrongdoing by that employee. Conceivably, counsel could be exposed to a malpractice suit by a client Organization if he or she does not conduct a thorough Internal Investigation or provides inappropriate advice based on an incomplete investigation.[49] Accordingly:

- Organization investigators generally seek to maintain secrecy regarding the subject matter of an Internal Investigation to prevent interference with the investigation or destruction of evidence, or when required by law;
- it may be prudent for Organization investigators to issue broad preservation notices in order to accomplish preservation without alerting alleged bad actors to the nature and targets of the Internal Investigation;

49. *See* Sections of Antitrust & Int'l Law, A.B.A., Comments Of The American Bar Association Sections of Antitrust Law And International Law On The Proposed Regulation Of The European Parliament And Of The European Council On The Protection of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, at 7 (Nov. 20, 2012), http://www.americanbar.org/content/dam/aba/administrative/antitrust_law/at_comments_eu_privacy.authcheckdam.pdf.

- it might be in the interest of the Organization for collection to occur simultaneously with the issuance of a preservation notice (an internal "dawn raid") to preserve evidence at the moment the Organization receives notice of the matter in order to avoid the potential for destruction of evidence;
- notice may not be given at all or may be delayed until the moment of collection because an employee may destroy evidence or confer with other involved employees in an attempt to initiate a cover-up;[50]
- employees may object upon receiving notice if they distrust the employer or think they may be subject to discipline or termination if the investigative findings disclose misconduct, a lapse in judgment, or even mere negligence;
- the Organization may need to disclose the investigation and its results as part of a self-report to an Investigating Authority in order to obtain cooperation credit for the Organization;
- because the Organization will not know what the investigation may uncover, the Organization may be unable to tell employees how the information will be used or how long it will be retained; and

50. For all the reasons given with respect to Government Investigations, consent is not a viable option in Internal Investigations. Moreover, in some countries, obtaining consent after the fact will not excuse a violation of the Data Protection Laws. For example, under German law, consent must be sought in advance of transfer and use. There are different legal terms for consent ("Einwilligung") and assent after the fact ("Genehmigung"). Assent after the fact is not a remedy for a previously-absent consent. *See* BÜRGERLICHES GESETZBUCHES [BGB] [CIVIL CODE], §§ 183,184(1)–(2) (Ger.), *translation at* http://www.gesetze-im-internet.de/englisch_bgb/index.html.

- disclosures may need to be made in countries that do not have laws that provide the same protections as those in the country from which the documents were collected.

In conclusion, cross-border transfers of data in Government Investigations and Internal Investigations may require an approach that differs from that taken in litigation.

II. STATEMENT OF PRINCIPLES FOR ADDRESSING DATA PROTECTION IN CROSS-BORDER CIVIL GOVERNMENT AND INTERNAL INVESTIGATIONS

Principle 1

Organizations doing business across international borders, in furtherance of corporate compliance policies, should develop a framework and protocols to identify, locate, process, transfer, or disclose Protected Data across borders in a lawful, efficient, and timely manner in response to Government and Internal Investigations.

Comment 1a: In the investigation context, a meaningful Principle 1 process should begin before a specific investigation enters the realm of possibility or, in the case of compliance monitoring, before the monitoring starts. Many problems can be avoided by setting up appropriate policies, procedures, and processes beforehand. Apart from data protection, labor, and other laws (including works council rights, bargaining agreements, and the secrecy of telecommunications) can, under some circumstances, delay or even prohibit use of employee, customer, or other personal data. Having in place appropriate policies can help an Organization navigate these issues and demonstrate respect for applicable local laws.

Information Technology (IT) policies should be drafted concisely and clearly with explicit rules regarding the appropriate use of major IT assets and the employer's right of access. Apart from policies for active employees, off-boarding policies should set out what may happen to a former employee's data in the case of an investigation. Departing employees not subject to a legal hold may also be invited to delete—under supervision—any non-business, purely personal communications and documents that they stored in the assets of the Organization. In certain countries, labor laws require employee body representatives to

be involved in the drafting and approval of such policies or, at the very least, to be informed of the policies. In some countries, whistleblower hotlines may need to be approved by the Data Protection Authority. In most circumstances, it is good practice to bring relevant stakeholders to the table to set standards.

The careful design of an investigation plan is a necessary ingredient for complying with data protection requirements. Concise policies put in place before any investigation occurs provide the building blocks and necessary transparency for Data Subjects. Nevertheless, policies should allow for flexibility in individual matters, particularly when specific decisions are documented and are accordingly considered in light of facts and circumstances known at the time.

Comment 1b: An Organization may be able to earn good will with an Investigating Authority if it gains the investigators' trust and is cooperative. One way to do this is to have strong compliance and ethics policies in place along with a framework and protocols that anticipate the possibility of an investigation before any actual investigation materializes. Such advance preparation enables an Organization to come forward, meet, and discuss issues with the Investigating Authority promptly. In order to be in this position, Organizations should consider developing a framework or guidelines that address how they will conduct Internal Investigations and respond to Government Investigations so as to pay due respect to relevant Data Protection Laws and the privacy rights of persons subject to such laws, as well as the needs of the Organization and Investigating Authority to detect wrongful conduct. Preparing such a framework or guidelines in advance of Government Investigations and Internal Investigations helps ensure timely responses and consistent and defensible practices for addressing these potentially conflicting interests.

In addition to what follows this comment, this means that the Organization should: (a) have a solid grasp of where its data is collected and stored; and (b) have a response team that is prepared to deal with production requests on short notice and understands its business and legal interests and priorities.[51]

Comment 1c: In developing a framework or guidelines for Internal Investigations, an Organization should anticipate potential disclosure to third parties. Most Internal Investigations conclude as purely internal matters without third-party involvement. Stakes for data protection in this context are comparatively low as Data Protection Law exceptions may apply and any third-party involvement and cross-border data transfer is under the Organization's direct control. However, when an investigation uncovers activity that triggers a reporting duty or that may lead to government action, the data protection stakes increase as the Organization must anticipate broader data preservation obligations, cross-border data transfers, and third-party disclosures, all of which raise heightened data protection concerns.

Comment 1d: When an Internal Investigation reaches a point where the need for third-party disclosure becomes likely, the Organization should consider the potential need to demonstrate the reasonableness and good faith of its decision-making processes in the event they are challenged. The Organization should also position itself to explain data protection issues to the Investigating Authority and to propose limitations and alternative sources of data. The Organization is in the best position to determine the appropriate scope of its initial investigation; whether, when, and how to escalate the investigation; and

51. The GDPR's requirements of data protection by design and by default (GDPR art. 25) facilitate this further.

what measures to take to maximize compliance with Data Protection Laws throughout this process.

Comment 1e: Organizations that regularly conduct business in certain jurisdictions—and thus may face Government Investigations in those jurisdictions—may consider including in their framework or guidelines country-specific information to help ensure consistent and defensible practices. This has the practical benefit of providing an Organization with a clear plan of action instead of having to start anew for each matter. An Organization may also determine which jurisdictions in which it does business raise the most significant compliance concerns and then allocate resources to address data protection issues according to the assessed costs and benefits.

Comment 1f: An Organization addressing a specific cross-border investigation should begin by identifying relevant jurisdictions and relevant Data Protection Laws governing the Processing and cross-border transfer of information, and identifying a resource skilled in applying such laws. It is probably impractical for Organizations to retain legal counsel in every jurisdiction but, if faced with an investigation, Organizations should be advised by individuals knowledgeable on the laws of the specific jurisdictions.

Comment 1g: Appropriate protocols should include consideration of invoking specific confidentiality protections when disclosing or producing Protected Data to Investigating Authorities. In the U.S. for example, the U.S. Freedom of Information Act (FOIA) contains a specific exemption prohibiting the government from disclosing in response to public requests "records or information compiled for law enforcement purposes [that] . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy."[52] In addition to this broad,

52. 5 U.S.C. § 552(b)(7)(C).

general prohibition, certain U.S. agency investigations are conducted pursuant to authorizing statutes that afford even stronger confidentiality provisions. For example, the Antitrust Civil Process Act, which authorizes the DOJ to investigate potential antitrust violations, contains a specific provision prohibiting the government from disclosing any material produced pursuant to that authority without the consent of the producing party.[53] Similar protections are provided under the False Claims Act,[54] Hart Scott Rodino Act,[55] and other statutes that authorize specific types of Government Investigations. In other types of investigations, statutes and regulations allow producing parties to request that the government provide confidential treatment under FOIA.[56] These types of confidentiality protections should be referenced in cover letters accompanying productions, production agreements, and if possible on the face of individual documents in order to draw attention to the fact that Protected Data is being produced and is subject to heightened confidentiality protection.

Principle 2

Data Protection Authorities and other stakeholders should give due regard to an Organization's need to conduct Internal Investigations for the purposes of regulatory compliance and other legitimate interests affecting corporate governance, and to respond adequately to Government Investigations.

Comment 2a: Organizations have legal, regulatory, and governance duties that may at times conflict with data protection obligations. When such interests conflict, an Organization may

53. 15 U.S.C. § 1313(c)(3).

54. 31 U.S.C. § 3733(i)(2)(C).

55. 15 U.S.C. § 18a(h).

56. *See, e.g.*, 17 C.F.R. § 200.83 (regarding SEC investigations).

need to balance the rights of Data Subjects against the Organization's legitimate interests in complying with those duties. In assessing an Organization's conduct, Data Protection Authorities and those who implement and enforce Data Protection Laws should recognize these competing imperatives.

Comment 2b: This Principle applies where a Data Protection Authority is evaluating whether an Organization has complied with relevant Data Protection Laws in response to either a Government or an Internal Investigation. Although there are many substantial differences, similar public policies underlie both civil regulatory enforcement and corporate governance. Both seek to detect, appropriately punish or discipline, and prevent unlawful conduct and promote lawful conduct. Organizations whose data is sought, as well as the jurisdictions in which they reside, have interests in promoting lawful conduct and detecting, eliminating, and punishing unlawful conduct.[57]

This Principle describes a standard that Data Protection Authorities, Investigating Authorities, and works councils may use to determine whether Organizations are responding appropriately to Investigating Authorities' requests or in conducting Internal Investigations. Courts and Data Protection Authorities should consider good faith, reasonableness, and proportionality in judging either an Organization's Internal Investigations or its

57. *See* EUROPEAN COMMISSION & DIRECTORATE-GENERAL FOR COMPETITION, COMPLIANCE MATTERS: WHAT COMPANIES CAN DO BETTER TO RESPECT EU COMPETITION RULES 9, 20 (2012) ("The prime responsibility for complying with the law, as in any other field, lies with those who are subject to it. EU competition rules applying to undertakings are a fact of daily business life that has to be reckoned with. . . . The Commission welcomes and supports all compliance efforts by companies as they contribute to the firm rooting of a truly competitive culture in all sectors of the European economy."), http://bookshop.europa.eu/en/compliance-matters-pbKD3211985/?CatalogCategoryID=8BYKABstR7sAAAEjupAY4e5L.

responses to Government Investigations. And in judging an Organization's responses to Government Investigations—particularly in the U.S.—best practices should recognize that Investigating Authorities require great flexibility in requesting data in order to accurately detect the full scope of unlawful conduct. Those requests are generally made without judicial supervision, and Organizations respond to them with limited recourse to court intervention prior to the government's filing of a court action against the Organization. During a Government Investigation, determining whether an Organization's response to an information request is sufficient rests primarily in the hands of the Investigating Authority making the request, due to the nature of investigatory work. In the case of Internal Investigations, it rests primarily in the hands of those undertaking the investigation on behalf of the Organization.

Comment 2c: Data Protection Authorities and other stakeholders should be mindful of an Organization's self-governance needs, recognizing the societal and economic benefits that accrue from an Organization keeping a clean house and complying with its regulatory obligations. Data Protection Laws and blocking statutes should not be used as a shield to prevent the detection of unlawful conduct. Unlawful conduct often causes widespread and long-term damage, harming Organizations, innocent employees, customers, and societies and economies as a whole. Undetected malfeasance sometimes spans years or even decades. Maintaining lawful conduct and detecting and eliminating unlawful conduct benefits Organizations, their customers, their employees, and society, and is generally a common international public interest. Conversely, undetected and unpunished malfeasance often multiplies and replicates when employees escape detection and then recruit co-workers and

competitors into their schemes and carry their unlawful conduct to new jobs in the same or different industries.[58]

Principle 3

Courts and Investigating Authorities should give due regard both to the competing legal obligations, and the costs, risks, and burdens confronting an Organization that must retain and produce information relevant to a legitimate Government Investigation, and the privacy and data protection interests of Data Subjects whose personal data may be implicated in a cross-border investigation.

Comment 3a: Every investigation that requires data to move across borders implicates the interests of multiple parties and countries. At a national level, the country conducting an investigation has a vital interest in securing the information it needs to protect its societal and economic interests. The country in which the information sought is located has, at a minimum, an interest in asserting its authority over the data located there and, to the extent the data relates to Data Subjects within its jurisdiction, it also has an interest in ensuring that those Data Subjects are treated fairly and consistently under its laws. The country

58. *See generally Position Paper: Business Compliance With Competition Rules*, BUSINESSEUROPE (Nov. 28, 2011), http://ec.europa.eu/competition/antitrust/compliance/businesseurope_compliance_en.pdf ("Abiding by antitrust rules is fundamental for creating and sustaining a competitive economy. . . . Being compliant with rules and maintaining a strong reputation are fundamental matters for every enterprise. . . . [C]ompliance action brings the following benefits: . . . [b]eing seen as a progressive and ethical business[,] . . . [a]ttracting ethically conscious consumers and investors[,] . . . attracting and retaining ethically conscious talent[,] . . . [and] [r]educing the risk of fines, or benefiting from competition authorities' settlement or leniency procedures . . . . The code of conduct of the company must make it absolutely clear that violation of any law, including competition law, will not be tolerated and will lead to disciplinary action[.]").

from which the data originated also has an interest in helping to uncover unlawful conduct committed by entities within its borders; ensuring that Organizations residing within it are responsible corporate citizens; and ensuring that employees of Organizations residing within it are obeying the law.

At the sub-national level, every Data Subject whose information is sought has a significant interest in having his or her information protected from misuse, as well as in having unlawful conduct committed against him or her uncovered and punished. Similarly, the Organization that is the subject of the investigation not only has a critical legal interest in the outcome of the investigation, but it also has a significant economic interest—even if not always legally cognizable[59]—in minimizing its costs and burden in producing information, in minimizing any resulting penalties, in cleaning house to uncover any unlawful conduct, in taking appropriate disciplinary action against offending employees, in preventing future violations that could result in even greater costs, and in having a say in whether information produced in one investigation is provided to a different jurisdiction. It also has a significant interest in not having its good-faith compliance with one set of investigative demands result in an investigation by a different jurisdiction concerning its conduct in responding to the first investigation, as would happen if responding to a Government Investigation triggered an inquiry by Data Protection Authorities in another jurisdiction.

Each of these varied interests might best be balanced if all interested courts and Investigating Authorities recognize both

59. At least in the U.S., the expense of defending a legal proceeding brought by the government is a cost of doing business and not a legally cognizable injury.

the potential conflicts that may result from variance in legal regimens and the common interests that may result from convergent public policies.

Comment 3b: Due regard for conflicting interests is especially warranted when the Organization is cooperating with the Investigating Authority and demonstrating a good-faith effort to produce relevant information in a timely manner. Although Investigating Authorities may not always "reward" good behavior in an investigation by "forgiving" law violations or even granting leniency, they nonetheless may be able to reward good-faith conduct by working with the Organization to find workable solutions to problems encountered because of conflicting legal obligations. Such cooperation on the part of the Investigating Authority may ultimately facilitate production of requested information and hasten the investigation while minimizing the Organization's expense and burden of compliance. More importantly, a record of working with Organizations that manifest good faith and cooperate in investigations will encourage other parties to cooperate in future investigations.

Comment 3c: One way in which Government Investigations differ fundamentally from private litigation is that Government Investigations focus on events, acts, or practices and the Investigating Authority's theories and perceptions may change as it gathers more information. Accordingly, the scope of an investigation may expand over time or become more focused. Moreover, a Government Investigation does not end until the Investigating Authority determines not to pursue the matter further, or initiates a formal challenge.

As a consequence, when the country hosting relevant information has strict Data Protection Laws, issues of data Processing (including preservation) present one of the most vexing problems for Investigating Authorities and Organizations

whose information is requested in cross-border investigations. This is so for Investigating Authorities because they may be unable to "release" an Organization from its data preservation obligations until they know with certainty that they no longer need certain information. It is so for the subject Organizations because their efforts to satisfy the investigative needs of one jurisdiction may require them to risk breaking the laws of another.

The difficulties that confront Investigating Authorities and subject Organizations in this regard can best be addressed through a dialogue in which the Organization is mindful of the Investigating Authority's legitimate need for information and the Investigating Authority is mindful of the legal obligations of the Organization and the interests of Data Subjects whose information may be implicated in the investigators' requests. In many instances, the Investigating Authority should consider whether its needs might be met through alternative mechanisms, such as phased productions, or receipt of aggregated or redacted/anonymized/pseudonymized information. Nevertheless, an Investigating Authority should demonstrate due regard by releasing an Organization from its data preservation obligations once it can appropriately do so.

Comment 3d: Investigating Authorities should retain Protected Data only so long as they are legally obliged to do so. In this regard, there generally is no difference in best practice between a litigation context and investigation context, except that in the context of investigations it may not be as clear to parties when a legal obligation to retain Protected Data preserved for the investigation ends. In litigation, the obligation ends no later than when the litigation and any appeals and related litigation end. In investigations, the endpoint may be less clear, particularly given the real risk of follow-on litigation, and parties may need to make appropriate inquiries to Investigating Authorities

to determine the status of an investigation.[60] In responding to inquiries about the status of an investigation, Investigating Authorities should bear in mind the interests and policies of the host country and those of any Data Subjects. One objective should be to "release" parties from their preservation obligations as soon as possible, consistent with the needs of the investigation.[61]

Principle 4

Where the laws and practices of the country conducting an investigation allow it, the Organization should at an early stage of a Government Investigation engage in dialogue with the Investigating Authority concerning the nature and scope of the investigation and any concerns about the need to produce information that is protected by the laws of another nation.

Comment 4a: U.S. experience has shown that there is real value in early and frequent engagement between the Investigating Authority and the party being requested to produce information. When the parties are candid and forthright with investigators, and investigators are willing to listen and engage with

60. *See International Litigation Principles*, *supra* note 1, at 25 (Principle 6).

61. Some authorities have a practice of notifying entities that have submitted data of the conclusion of an investigation and arranging for the return or destruction of the data held by the authority. Those authorities, however, make exceptions to the return or destruction of the data, for example, if the data is relevant to another investigation by the authority or if a document has become a court exhibit, such as in a grand jury proceeding, and thus must be retained in an official government internal file. To address situations in which parties may not know that an investigation has concluded, the Federal Trade Commission has adopted a Rule of Practice that "relieves" a party of its preservation obligations with respect to the investigation if the party has not received any written communication from the agency regarding the investigation for a period of one year. *See* 16 C.F.R. § 2.14(c).

the parties, investigations can be focused and concluded efficiently at reduced cost to both the government and the parties. Especially in the absence of civil procedures that can be leveraged to advance data protection goals (including the meet-and-confer process, discovery and case management by a judge, rules limiting discovery and jurisdiction, and court-ordered data protection), an Organization should look for opportunities to proactively alert Investigating Authorities to potential legal conflicts and propose measures designed to protect data. In jurisdictions where Investigating Authorities will entertain it, early discussions regarding scope may allow the Organization to limit potential conflicts with Data Protection Laws and to address those that exist while showing regulators good faith and transparency.

Comment 4b: Even in the absence of formal or informal mechanisms that facilitate frequent dialogue between the Investigating Authorities and the parties, in some investigations there may be opportunities to use certain protective mechanisms outlined in the *International Litigation Principles*, including: phased disclosure; sampling; substitution of data; redaction, anonymization and pseudonymization (where viable); and physical and organizational security measures including encryption, access-rights management, and access-request notification.[62]

Comment 4c: The issues under investigation may evolve over time as leads are followed and threads of information are developed more fully until resolved—favorably or unfavorably. Investigating Authorities must be able to go where the evidence leads. In many ways, these needs are antithetical to the trans-

62. *See International Litigation Principles*, *supra* note 1, at 14–19 (Principle 3).

parent, staged, targeted, specific collection, Processing, and production strategies contemplated by Principle 3 of the *International Litigation Principles*.

Comment 4d: Some steps in investigations may help demonstrate substantial compliance with Data Protection Laws. In keeping with principles of data accuracy and proportionality,[63] any investigation should follow a carefully designed process ensuring that only data sources with relevance to the investigation are processed, that the Processing is limited to that purpose, and that end-of-matter data disposition policies are followed. In accordance with GDPR Articles 24(1), 25, and 28(1), appropriate technical and organizational measures must be adopted to ensure the security and confidentiality of the processed data. In-country evaluation by a local entity versus immediate cross-border transfer and disclosure should be considered.[64] Notice should be given to the Data Subject as soon as practicably and appropriately possible, recognizing that providing notice can, for instance, undermine an investigation and may have to be delayed.[65]

Comment 4e: In disclosing information about global operations and educating Investigating Authorities regarding potential data protection issues, Organizations should be prepared to

63. *See, e.g.*, GDPR art. 5(b)–(d).

64. *See, e.g.*, WP 158, *supra* note 18, at 9–16 (discussing whistleblowing schemes).

65. Note that exceptions are provided in GDPR art. 14(5)(b) where providing notice would "seriously impair" the objective of the Processing; *see also* Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679*, at 28, 17/EN/WP260 (Dec. 12, 2017), *available at* http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50057. Moreover, there are limits on how far an Investigating Authority will go (or can be expected to go) in protecting the rights of Data Subjects. *See Producing Information, supra* note 46.

explain how proposed measures to limit and channel disclosure meant to minimize Data Protection Law conflicts are compatible with, and not intended to impede, investigation objectives.

Principle 5

Organizations should consider whether and when to consent to exchanges of information among Investigating Authorities of different jurisdictions in parallel investigations to help minimize conflicts among Data Protection Laws.

Comment 5a: To encourage and facilitate cooperation in Government Investigations and voluntary compliance with requests for information by Investigating Authorities, governments sometimes enact laws that limit use of information obtained. For example, the U.S. Internal Revenue Service generally may not share tax-related information with other agencies; the Department of Commerce may not share census information; both the DOJ and the FTC generally may not share with others any information they obtain under pre-merger notification laws; and the FTC may share information it receives with other federal or state agencies only if the other agencies certify that they will use the information solely for law enforcement purposes and maintain confidentiality.

Exceptions to these rules tend to be limited. For example, in very limited circumstances, the FTC can share information with non-U.S. law enforcement agencies under the U.S. SAFE WEB Act. [66] That law allows the FTC to share information with non-U.S. agencies in consumer protection cases upon request if: (1)

66. Undertaking Spam, Spyware, And Fraud Enforcement with Enforcers beyond Borders Act of 2006 ("U.S. SAFE WEB Act"), Pub. L. No. 109-455, 120 Stat. 3372, extended by Pub. L. No. 112-203, 126 Stat. 1484, codified at 15 U.S.C. §§ 41 *et seq*.

the requesting agency seeks the information for law enforcement purposes; (2) the law it is enforcing is analogous to one enforced by the FTC; and (3) the requesting agency will reciprocate in cooperating with requests by the FTC.[67]

Despite the limitations on their ability to share information, governments often investigate conduct or transactions that cross borders or even span the globe.[68] Some matters may pique the interests of other nations. Examples of non-criminal matters include mergers involving large international Organizations or other competition cases involving monopolistic or other anti-competitive practices that cross international borders. Although Investigating Authorities often develop cooperative relations with their foreign counterparts, frequently embodied in Memoranda of Understanding or even Mutual Assistance Treaties, such arrangements in civil matters often limit the authorities to generalized discussions about legal theories and investigative strategies because authorization statutes preclude sharing actual information about the entities and subject matter of investigations.

Comment 5b: The inability of Investigating Authorities to share information has consequences for Organizations subject to investigation by more than one government for conduct involving common facts or transactions. Such Organizations must often deal with overlapping, burdensome, and redundant demands for information. Some Government Investigations may begin much later than others; some progress more swiftly than

67. *See* 15 U.S.C. § 46(j)(1)–(4).

68. Investigations into the manipulation of London Interbank Offered Rate (LIBOR) and currency exchange rates are a good example: *see, e.g.*, DOJ Division Update Spring 2016, https://www.justice.gov/atr/division-operations/division-update-2016/ (noting international enforcement cooperation across multiple jurisdictions in foreign currency exchange manipulation investigations).

others. At the conclusion, Organizations may be subject to inconsistent or even mutually exclusive results that leave them in a position of having to disobey one country's orders in order to comply with another's. One strategy for avoiding, or at least minimizing, these risks, is for the Organization to authorize governments to share information about the subjects of their investigations to the extent they have the authority to do so. By allowing such sharing and information transfers, Organizations may be able to coordinate the timing of investigations and lessen their burden of producing information to multiple Investigating Authorities. Most importantly, by encouraging coordination and cooperation among Investigating Authorities, the Organization may minimize the risk that it will be subject to inconsistent or mutually exclusive orders.

Comment 5c: Significantly, coordination among countries may be the one aspect of a Government Investigation that an Organization can best control. In many instances, only the Organization can authorize governments to share information that they otherwise could not share.[69] Also, in some instances the Organization may be the only entity aware of multiple investigations. In many situations, there may be no reason why investigators in one country should know of a similar or related investigation in another country. In such situations, the Organization should consider whether its interest may, consistent with applicable Data Protections Laws (*see* Comment 5e, *infra*), best be served by granting waivers to encourage and facilitate cooperation and coordination among Investigating Authorities. An important factor for the Organization to consider is that once enforcement actions in one jurisdiction are filed against a mul-

69. The Organization's ability to authorize such further disclosure may, however, be subject to obtaining appropriate Data Subject input.

tinational Organization, or a subject makes required public disclosures, such as under the securities laws, other jurisdictions will become aware of the investigation if they are not already aware. If the Organization has proactively granted a waiver and cooperated with other jurisdictions, its cooperation has the potential to reduce penalties.

Comment 5d: Assuming an Organization decides to grant waivers that allow countries to share information, it should carefully consider the scope of any waiver it grants, and especially whether it will allow Investigating Authorities to share information protected by a legally-recognized privilege or applicable blocking statute. In this regard, U.S. law generally recognizes that communications between an Organization's managers and in-house attorneys, as well as communications between the Organization's managers and other select employees, may be privileged. Not all countries recognize such privileges. Accordingly, when granting waivers to Investigating Authorities, Organizations may wish to consider whether to limit the waivers to information and communications that are not privileged under the laws of one or more interested jurisdictions.[70] Similarly, by their very nature, dawn raids may result in the capture of more information than the Investigating Authorities need for their investigation. Indeed, dawn raids may result in the acquisition of information that is wholly irrelevant to the matter or beyond the scope of the investigation. In those cases, assuming the subject of the investigation has a chance to allow sharing among multinational investigators, the Organization

70. Both U.S. antitrust agencies have expressly adopted a model waiver for use in civil investigations. *See* Fed. Trade Comm'n Press Release, Federal Trade Commission and Justice Department Issue Updated Model Waiver of Confidentiality for International Civil Matters and Accompanying FAQ (Sept. 25, 2013), https://www.ftc.gov/news-events/press-releases/2013/09/federal-trade-commission-justice-department-issue-updated-model.

should carefully identify the scope of the information that may be shared, taking special care to protect irrelevant Protected Data.

Comment 5e: To the extent that an Organization considers granting waivers allowing authorities in different countries to share information, it should also consider the impact of Data Protection Laws on the scope of the waiver. On the one hand, a cooperative effort may facilitate adherence to data protection principles (for example, by ensuring greater control over the process, allowing the Organization to negotiate limits on data Processing, and minimizing data Processing and transfer in a single effort). At the same time, such an effort may raise Data Protection Law concerns (for example, under EU law, considerations for transferring data within the EU are entirely different from those raised by transferring data to a non-approved country such as the U.S.; here, there may also be issues regarding notice and consent requirements and Processing data for a single purpose).

Principle 6

Investigating Authorities should consider whether they can share information about, and coordinate, parallel investigations to expedite their inquiries and avoid, where possible, inconsistent or conflicting results and minimize conflicts with Data Protection Laws.

Comment 6a: Governments do not enforce each other's laws, but may nonetheless share common interests, values, and goals with respect to certain non-criminal matters. Thus, where possible, dialogue and cooperation among and between foreign Investigating Authorities may, consistent with Data Protection Laws, generate good will and understanding among nations and advance global commerce and welfare. Nations create law

enforcement agencies to enforce domestic laws, and thereby advance and protect the nation's societal and economic interests. They may also advance common interests with other nations either by entering into bilateral or multilateral treaties or by authorizing enforcement authorities to enter into Memoranda of Understanding and other cooperative arrangements with their foreign counterparts. Authorities may sometimes have opportunities to engage in informal discussions with foreign counterparts, although in civil matters such discussions often must remain at higher levels of generality. Cooperation and coordination may help a law enforcement agency leverage scarce resources. It may also benefit business entities subject to bilateral or multilateral investigations by reducing their expense and burden of dealing with multiple overlapping investigations and the risk of inconsistent orders.[71]

Comment 6b: Given the potential benefits, Investigating Authorities should carefully consider opportunities to engage in dialogue and cooperation with their foreign counterparts on matters of mutual interest and concern. This may be particularly important when Organizations that manifest good-faith efforts to cooperate in an investigation offer to facilitate the flow of information between governments. By acceding to such offers, Investigating Authorities may help reduce the subject's costs of compliance with investigative demands and thereby encourage cooperation by other subjects in future investigations. A more immediate benefit is that all concerned Investigating Authorities may gain access to more complete information and proceed with confidence that they are all working from the same factual basis. At least in principle, when nations share common goals and work with common facts, their legal and economic analysis of information should tend to converge and investigations

71. *See* ANTITRUST GUIDELINES, *supra* note 20, at ¶¶ 5.1.3, 5.1.4.

should reach results that are approximately consistent, if not identical.

Principle 7

Courts and Data Protection Authorities should give due regard to the interests of a foreign sovereign seeking to investigate potential violations of its domestic laws.

Comment 7a: The U.S. Supreme Court in *Aérospatiale* held that "international comity compels 'due respect' for the laws of other nations and their impact on parties in U.S. Litigation subject to, or entitled to benefits under, those laws."[72] As a corollary, the *International Litigation Principles* cautions that "Data Protection Laws should not be advanced for improper purposes or to delay preservation or discovery absent a good faith belief that Data Protection Laws conflict with U.S. preservation or discovery requirements."[73] As noted earlier, Government and Internal Investigations implicate the law enforcement interests of foreign sovereigns, and may involve the specter of significant corporate exposure. Accordingly, the stakes may be high for both the country conducting the investigation and the Organization that is the subject of the investigation (the public interest and the collateral consequences of civil law enforcement proceedings can be far reaching). The Organization's decisions of whether and how intensely to assert any conflicts-of-laws may be difficult. An interesting question is how courts and Data Protection Authorities should treat the issue of comity in the context of regulatory enforcement where the conduct being investigated has the potential to support law enforcement actions, as

72. *See International Litigation Principles*, *supra* note 1, at 9 (citing Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522, 546 (1987)).

73. *Id.* at 10.

there is an accepted exception to the application of comity principles when the strong public policies of the forum are in actual conflict with the laws of a foreign jurisdiction.[74] Seemingly, such conflicts should be rare because common public interest and welfare of the citizens of all interested nations are furthered when legitimate investigations can be conducted concerning possible improper behavior, such as bribery, theft, dishonesty, deception, and anticompetitive activities by corporations or by individual employees.[75]

Comment 7b: Law enforcement actions differ fundamentally from private actions. Because investigations are an exercise of sovereign power, they represent the means by which nations assert authority over conduct that occurs within their borders or that has a substantial effect within their borders, and help ensure adherence to national values. Because laws set out national values and policies, they express the public interest as identified and defined by the national legislature. Although private litigation often reflects national values and the public interest, law enforcement actions presumptively attempt to implement and protect the public interest and advance public welfare.

When a government decides to seek documents covered by foreign Data Protection Laws, "the government balances the need for the information sought and the public interest in the investigation against the interests of the foreign jurisdictions

74. *Id.* at 10 n.30.

75. *See* ANTITRUST GUIDELINES, *supra* note 20, at ¶ 4.1; Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party at 15, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation (No. 17-2), 2017 WL 6383224, https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf [hereinafter EU Microsoft Amicus].

where the information is located and any potential consequences for [its] foreign relations."[76] Thus, a U.S. "government request for production . . . reflects the Executive Branch's conclusion, in the exercise of its responsibility for both foreign affairs and the enforcement of [criminal and civil] laws requiring production, that disclosure would be consistent with both the domestic public interest and international comity concerns."[77] As reflected in bilateral and multilateral agreements between nations, "many sovereigns recognize that government [law enforcement] document requests reflect important sovereign interests and should be dealt with cooperatively when possible."[78] As already noted, nations do not enforce each other's civil laws. However, absent fundamental irreconcilable conflicts in values, they should respect each other's laws. Principles of comity suggest that nations should respect each other's legislative, executive, and judicial acts, at least where such respect is reciprocated. In the context of law enforcement investigations, comity suggests that courts and regulators of a country hosting information needed for an investigation in another country should give due regard to the laws (and interests) of the country conducting the investigation and seek to accommodate those interests where possible. They should also consider the extent to which the investigation reflects, or even furthers, the public, legal, and societal values of their own jurisdiction. Similarly, countries conducting investigations should make reasonable efforts to limit demands for Protected Data to that which they truly need.[79]

---

76. Brief for the United States as Amicus Curiae at *12, Arab Bank, PLC v. Linde, 134 S. Ct. 2869 (2014) (No. 12-1485), 2014 WL 2191224 (citing American Ins. Ass'n v. Garamendi, 539 U.S. 413–15 (2003)).

77. *Id.* at *12–13.

78. *Id*. at *13.

79. *See* EU Microsoft Amicus at 12–16, *supra* note *73*.

Principle 8

A party's conduct in undertaking Internal Investigations and complying with Investigating Authorities' requests or demands should be judged by a court, Investigating Authority, or Data Protection Authority under a standard of good faith and reasonableness.

Comment 8a: While Principle 7 addresses the deference and regard that governments should exercise when considering the legitimate law enforcement needs of another sovereign, Principle 8 primarily addresses the standard governments should apply when considering the legitimate governance needs of Organizations in conducting Internal Investigations and echoes and paraphrases Principle 2 of the *International Litigation Principles*. That Principle provides guidance to parties who must attempt to meet both obligations, and to Data Protection Authorities, Investigating Authorities, and courts that may be required to evaluate the parties' actions. In these situations, a standard of good faith and reasonableness should apply, particularly when guidance is unavailable, vague, or inconsistent. Data Protection Authorities assessing the conduct of an Internal Investigation should recognize the substantial benefits that accrue to the Organization and to society when Organizations detect, stop, prevent, and punish illegal conduct by their employees. When conflicts of law do arise, Organizations should make good-faith and reasonable efforts to mitigate risk, recognizing that full compliance with conflicting obligations may not be possible. Conversely, when called upon to evaluate party actions and responses, Data Protection Authorities, Investigating Authorities, and courts should consider the conflicting obligations and base their judgments on consideration of the Organization's reasonable and good-faith efforts made under the circumstances that existed at the time and proportionate to the matters at issue.

For example, a Data Controller must necessarily make determinations regarding the applicability of Data Protection Laws and what data is actually protected. Depending on which country's law applies and the specific circumstances of the matter under investigation, factors including the Protected Data's country of origin and the relevant Data Subject's residency or nationality may also be considered in assessing how to proceed. The Data Controller must ultimately make decisions about how to effectuate Processing and potential transfer and disclosure of Protected Data. Often these determinations must be made early, before the circumstances and scope of the investigation are known and before there is opportunity to consult with Investigating Authorities or Data Protection Authorities. Under Principle 8, the parties' actions—and later judgment of those actions—should be viewed, not in hindsight, but in light of the facts known and the circumstances that existed at the time the action was taken, and governed by a good-faith and reasonableness standard.[80]

Comment 8b: There may be situations in which courts, Data Protection Authorities, or others may be called upon to evaluate an Organization's compliance efforts in a Government Investigation that the host country finds do not adequately support its

80. For a discussion of the standard of "good faith" in U.S. Litigation, *see International Litigation Principles, supra* note 1, at 11–13 (Principle 2, Comment); for a discussion of preservation and legal hold duties in the context of Government Investigations, *see* The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265 (2010), *passim* and Guideline 1, Illustration iii ("An organization learns of a report in a reputable news media source that includes sufficient facts, consistent with information known to the organization, of an impending Government Investigation of a possible violation of law by the organization stemming from the backdating of stock options given to executives. Under these circumstances, a Government Investigation (and possibly litigation) can reasonably be anticipated and a preservation obligation has arisen.").

values and in which it believes the document demands conflict with the host country's Data Protection Laws. Here too, Principle 8 counsels that the Organization's actions should be viewed, not in hindsight, but in light of the facts known and the circumstances that existed at the time the action was taken, in light of the competing if not conflicting demands, and governed by a good-faith and reasonableness standard.

Comment 8c: Organizations can—even when acting in good faith and reasonably—still make mistakes in the view of the Data Protection Authority or Investigating Authority. Investigating Authorities should view these perceived shortcomings in light of overall efforts of complying with conflicting regulatory schemes. Good faith and reasonableness includes a range of interpretations and judgments of how to comply with Data Protection Laws. Thus, two Organizations may approach the same inquiry differently but still reasonably. There is no one-size-fits-all assessment, and the same Organization may respond to regulatory inquiries differently but still reasonably and in good faith. Across cases, the outcome of the legal analysis of complying with Data Protection Laws may differ for valid reasons.

TRADE SECRET "TRIGGERS": WHAT FACTS WARRANT LITIGATION?

William Lynch Schaller, Russell Beck** & Randall E. Kahnke****

INTRODUCTION

A confluence of factors, including multiple high-profile prosecutions and civil actions for trade secret thefts, passage of the federal Defend Trade Secrets Act (DTSA), and uncertainty over patent protection, have brought trade secret issues to the forefront of American business concerns.[1] Whether old-fashion insider theft or ultra-modern computer hacking, trade secret theft knows no bounds "in an era of digitalization, global markets, and mobile workers."[2] Recent, illustrative examples can be found in the Cisco-Arista router trade secret litigation, in which

* Retired Partner, Baker & McKenzie, Chicago, Illinois. The views herein do not necessarily reflect the views of Baker & McKenzie or its clients. Mr. Schaller is no longer a partner, employee, or agent of Baker & McKenzie in any way.

** Partner, Beck Reed Riden, Boston, Massachusetts.

*** Partner, Faegre Baker Daniels, Minneapolis, Minnesota.

1. Maressa A. Frederick & Clara N. Jiménez, *Are the Crown Jewels Really Safe?: Considerations for Building a Strong Trade Secret Portfolio in Today's Market*, A.B.A. LANDSLIDE, Vol. 9, No. 4, March/April 2017, at 14 ("In the past year, the passage of the Defend Trade Secrets Act in the United States and the Trade Secrets Directive in the European Union, coupled with the perceived uncertainty surrounding patent procurement and enforcement, have increased the attractiveness of trade secrets as tools to protect intellectual property.").

2. *Id*.

a key executive left Cisco to lead Arista in head-to-head competition,[3] and the Equifax cyberhacking disaster, in which 143 million Americans may face identity theft.[4] Others, like the high-profile Google/Waymo-Uber self-driving car lawsuit, involved elements of both: Anthony Levandowski, a former engineer with Google's driverless car unit Waymo, allegedly "colluded with Uber to steal 14,000 confidential documents from Waymo––even before he left Waymo to jump-start Uber's self-driving car efforts."[5] His actions resulted initially in expedited discovery and a preliminary injunction barring Levandowski from participating in Uber's driverless car technology[6] and ended later in Levandowski's termination,[7] a permanent injunction against Uber, and a $245 million settlement by Uber.[8] Federal Judge Wil-

3. *See* Rachel King, *Cisco's Costly Feud: CEO's Former Protégé Joins Startup, Builds Rival Networking Business*, WALL ST. J., Aug. 18, 2017, at A1 (reporting business and litigation aspects of the fight between Cisco CEO John Chambers and his former colleague, Arista CEO Jayshree Ullal).

4. Brad Stone, *Hurricane Equifax Is a Category 5 Breach*, CHI. TRIB., Sept. 12, 2017, § 1, at 15 (discussing the Equifax breach from a personal perspective, as one notified that his most sensitive information may have been breached).

5. Jack Nicas, *Uber Appeared Wary Before Deal: Alphabet Offers Evidence that Rival Anticipated Suit Over Purchase of Startup*, WALL ST. J., April 13, 2017, at B3.

6. *See* Greg Bensinger & Jack Nicas, *Uber Takes Hit in Car-Tech Fight: Judge Gives Alphabet Unit Broad Leeway to Exam Evidence from Ride-Hailing Firm*, WALL ST. J., May 16, 2017, at B1.

7. *See* Mike Isaac & Daisuke Wakabayashi, *Uber Fires Former Google Engineer at Heart of Self-Driving Dispute*, N.Y. TIMES (May 30, 2017), https://www.nytimes.com/2017/05/30/technology/uber-anthony-levandowski.html ("Uber has pressured Mr. Levandowski to cooperate for months, but after he missed an internal deadline to hand over information, the company fired him.").

8. Kif Leswing & Rob Price, *Uber and Waymo Have Reached a $245 Million Settlement in Their Massive Legal Fight Over Self-Driving-Car Technology*,

liam Alsup of the Northern District of California in San Francisco also referred the case to the Justice Department for criminal investigation.[9]

These cases reflect the speed and intensity of trade secret actions, and they underscore the need for prompt and thorough investigations at the outset. When investigating a trade secret misappropriation case under pressure, however, it's all too easy to skip the first and most basic question: What are the facts that constitute "triggers" warranting legal action? As Ken Vanko has noted, "Trade secret cases pose unique challenges for plaintiff's counsel, particularly since the elemental trigger facts lie squarely within the client's control and may deal with obtuse, technical concepts."[10] Ironically, in tougher cases, the trigger facts may actually rest solely within the defendant's control. The consequences of getting this "trigger" question wrong can be severe for all counsel,[11] given how quickly these cases can mushroom into major litigation.[12]

BUSINESS INSIDER (Feb. 9, 2018), https://www.businessinsider.com.au/uber-settles-with-waymo-in-self-driving-lawsuit-2018-2 (reporting settlement, including non-use agreement).

9. Greg Bensinger & Jack Nicas, *supra* note 6.

10. Kenneth J. Vanko, *Trade Secrets: Proving Bad Faith in Trade Secret Cases*, ILL. B. J., Vol. 105, No. 6, June 2017, at 40, 42.

11. *See* Charles S. Fax, *The Perils of Appearing Pro Hac Vice*, A.B.A. LITIG. NEWS, Vol. 42, No. 4, Summer 2017, at 20 (noting that local counsel may sign a complaint prepared by *pro hac vice* counsel, only to find some factual or legal assertions in the filing are not the result of reasonable inquiry or otherwise violate Rule 11's requirements: (1) no improper purpose; (2) warranted by existing law or non-frivolous argument to modify law; (3) factual contentions have or will likely have evidentiary support; and (4) denials of factual contentions are warranted).

12. *See, e.g.*, Wolters Kluwer Financial Services, Inc. v. Scivantage, 525 F. Supp. 2d 448 (S.D.N.Y. 2007) (100-page opinion excoriating trade secret litigation tactics of plaintiff's counsel, starting with elementary fact that the accused former employees never had access to the secret computer source code

Broadly speaking, all trade secret cases involve allegations that information was a trade secret and *wrongfully* acquired, used, or disclosed. While all cases involve some amount of wrongful conduct, it is the quality of the wrongful conduct that presents the "trigger" factual inquiry.

In some cases, trigger facts are the subject of direct evidence and hence relatively straightforward. For example, there are virtually no circumstances in which outsiders can legitimately hack into someone else's password-protected computer system, and occasionally employees are caught on camera or tell others of their bad acts. But most trade secret cases rely on more circumstantial evidence and thus require more thought.[13]

Below, we treat the three most common scenarios—jumping ship, inevitable disclosure, and failed deals—by reviewing cases decided before the DTSA. We then turn to how federal pleading standards may play out under the new DTSA with respect to trigger facts, including federal court jurisdictional facts and the potential unavailability of the inevitable disclosure doctrine under the DTSA.

JUMPING SHIP

Although cyber intrusions like the Equifax disaster make headlines, most trade secret cases start more modestly, with

in question); *In re* Kristan Peters, 748 F.3d 456 (2d Cir. 2014) (affirming seven-year suspension from federal court practice of law for lead plaintiff's counsel in the *Scivantage* case).

13. *See* Sokol Crystal Products, Inc. v. DSC Communications Corp., 15 F.3d 1427, 1429 (7th Cir. 1994) ("While there was no direct evidence that anyone at DSC used Sokol's confidential information in the making of its own VCXO, the jury apparently inferred from the fact that DSC had access to Sokol's confidential information and from the similarity between the two devices that DSC misappropriated Sokol's trade secret and that the AFD VCXO was derived from that trade secret.").

partners, executives, employees, or consultants ending one relationship to start another—invariably with a competitor. Indeed, many believe with some justification that job-hopping is the only way to secure a significant raise,[14] and others argue that worker mobility is central to economic growth.[15] While the data is still inconclusive,[16] an underlying question remains: Does the mere fact that a person switches sides, without more, justify a trade secret lawsuit?

The answer to this narrow but simple question should be "no," yet surprisingly few appellate cases directly and thoroughly address this question at the pleadings stage. As a result, innocent defendants are forced to endure full-blown trade secret litigation through summary judgement and then have no recourse for bad faith or simply deficient pleading.

---

14. *See, e.g.*, Cassie Walker Burke & Sabrina Gasulla, *Is Job-Hopping the Only Way to Get Ahead in Chicago?*, CRAIN'S CHI. BUS., April 3, 2017, at 15 ("Out of 650-plus Chicago-area men and women we surveyed in January [2017], 62 percent—nearly 2 out of 3—said changing jobs was necessary for advancement in the local job market."); Vanessa Fuhrmans, *The Case for Saying Goodbye*, WALL ST. J., April 19, 2017, at B7 ("Young professionals are among today's biggest job-hoppers: A 2016 LinkedIn survey found millennials have worked at roughly four companies in their first decade after college, compared with 2.5 companies for the generation before them.").

15. *See, e.g.*, Omri Ben-Shahar, *How Chicago Can Lure Amazon: Ban Noncompete Agreements*, CHI. TRIB., Sept. 12, 2017, § 1, at 13 ("[T]he evidence strongly suggests that the [complete noncompete] ban proposed by [Illinois Governor Bruce Rauner] would support economic growth, technological startups and innovation."); Ronald J. Gilson, *The Legal Infrastructure of High Technology Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. REV. 575 (1999) (arguing that California's statutory ban on noncompete agreements—resulting in increased employee mobility—played a critical role in the rise of Silicon Valley).

16. Norman D. Bishara & Evan Starr, *The Incomplete Noncompete Picture,* 20 LEWIS & CLARK L. REV. 497, 497–546 (2016).

A case in point at the district court level is *Glenayre Electronics, Ltd. v. Sandahl*.[17] In this bruising fight, Joel Sandahl and six other employees departed Glenayre to form a rival paging system firm, Complex Systems. They continued to provide consulting services to Glenayre for the next six months, but the parties eventually landed in arbitration over an alleged noncompetition agreement violation relating to the design of Complex Systems' new paging system called C-NET. During a pretrial conference in connection with the arbitration, Sandahl said an attorney had compared C-NET's paging system patent application with a patent application Glenayre had filed for its new Omega Gold paging product and had found Omega Gold was a "clone" of C-NET. This caused Glenayre to conclude that Complex Systems had somehow improperly obtained confidential information about Omega Gold.

Extensive discovery, a preliminary injunction,[18] and an interlocutory appeal ensued,[19] but the case culminated in summary judgement for the defense seventeen months after the initial complaint was filed. The district court carefully parsed the evidence and arguments before ruling that Glenayre's circumstantial evidence did not raise a reasonable inference of trade secret misappropriation. Among other things, the court rejected Glenayre's assertion that Omega Gold must have been misappropriated just because Complex Systems came up with C-NET quickly and "out of thin air," noting Glenayre cited no documents or other evidence in support of this notion. The court also

17. 830 F. Supp. 1149 (C.D. Ill. 1993).

18. Glenayre Electronics, Ltd. v. Sandahl, 811 F. Supp. 388 (C.D. Ill. 1993) (noting the court's prior order dated June 3, 1992, granting a preliminary injunction preventing defendants' use of information obtained from Glenayre, but allowing both parties to continue to pursue their respective patent applications on the pager technology at issue).

19. *In re* Sandahl, 980 F.2d 1118 (7th Cir. 1992).

ignored Sandahl's "cloning" remark at the arbitration, calling it "a misunderstanding, not misappropriation,"[20] in light of the patent attorney's testimony that he had never seen the Omega Gold patent application. The court then deconstructed the claim that Michael Tanner, another ex-Glenayre employee who joined Complex Systems, must have misappropriated Omega Gold because he accepted a higher paying position with Complex and subsequently waited five days before resigning from Glenayre. The evidence, however, showed that Omega Gold was not underway until after Tanner left.

When all was said and done, the triggers of mass departures, substantial similarity, and suspicious timing were simply not enough, especially since it appeared none of the defendants had access to Glenayre's secrets. The court had "no doubt that the gentlemen who left Glenayre's employment are highly knowledgeable and experienced regarding paging system technology,"[21] but this by itself did not establish a colorable trade secret misappropriation case against them. Yet, despite their lack of wrongful conduct, the defendants spent seventeen months in litigation that was arguably baseless from the outset.

The absence of trigger facts produced a similar pro-defense outcome at the pleadings stage in another district court case, *Accenture Global Services GmbH v. Guidewire Software, Inc*.[22] In this case, strictly speaking, employees did not jump ship; instead, the customer did. Specifically, rival firm employees worked for the same customer, CNA Insurance, on overlapping insurance claims handling automation projects under nondisclosure agreements. Accenture later alleged that competitor Guidewire

20. *Glenayre Electronics, Ltd.*, 830 F. Supp. at 1152.

21. *Id*. at 1153.

22. 581 F. Supp. 2d 654 (D. Del. 2008).

"somehow" and "somewhere" gained access to Accenture's insurance claims processing software secrets because Guidewire quickly produced software that had taken Accenture years to develop: "[W]e believe that their product development trajectory was just too fast to result in the kind of product that they have, which looks fairly similar to ours. From our view that's too much of a coincidence, so there has to be a trade secret violation here, in our opinion."[23]

The district court was unimpressed and dismissed these conclusory allegations on a Rule 12(b)(6) motion. Under the United States Supreme Court's governing standards in *Bell Atlantic Corp. v. Twombly*,[24] the district court noted, "more than labels and conclusions" are necessary; "a formulaic recitation of the elements of a cause of action will not do."[25] Instead, "a well-pleaded complaint must contain enough facts to state a claim to relief that is plausible on its face"—a standard that "does not impose a probability requirement at the pleading stage."[26] The district court's sensitive application of these principles is worth quoting:

> It is not common for a trade secret misappropriation plaintiff to know, prior to discovery, the details surrounding the purported theft. That being said, a court may be asked to strike a balance between the notice required by Rule 8 with the reality that a trade secret misappropriation plaintiff may have minimal facts available to it at the pleading stage.

23. *Id*. at 659.

24. 550 U.S. 554 (2007).

25. *Accenture*, 581 F. Supp. 2d at 660 (quoting *Twombly*, 550 U.S. at 545).

26. *Accenture*, 581 F. Supp. 2d at 660–61 (quoting *Twombly*, 550 U.S. at 545).

> It is the court's opinion that the complaint at bar, however, presents nothing more than "conclusions" and a "formulaic recitation of elements of a cause of action." With respect to the theft of its trade secrets, Accenture states only the following: Accenture worked with CNA, during which time it learned about Guidewire; Accenture installed ACCS software on CNA's computers in late 2002; CNA informed Accenture in 2003 that its bid had lost; and Accenture later learned that Guidewire had the winning bid. (D.I. 1 at ¶¶ 20–25) Accenture assumes, based upon what it feels was "a surprisingly quick development trajectory," that Guidewire has "somehow" obtained and used Accenture's trade secrets. (*Id*. at ¶¶ 24, 25, 31) The balance of Accenture's complaint recites only the remainder of the misappropriation elements, namely, that Guidewire acted with knowledge, and that its acts constitute harm to Accenture. (*Id*. at ¶¶ 33–34)
>
> To support its trade secrets claim, Accenture was required to plead certain facts, namely, that Guidewire obtained its trade secrets by improper means or, alternatively, an improper use or disclosure. 6 Del. C. § 2001(2)(a) & (b). Accenture states only that Guidewire "somehow gained access to Accenture trade secrets in creating its software and services." (*Id*. at ¶ 25) This paragraph implies that Guidewire possessed the trade secrets in question. There is no allegation, however, that Guidewire obtained the information by improper means, or the nature of such means. Accenture's

> use of the word "somehow" in describing Guidewire's acquisition of its trade secrets emphasizes this point. (*Id*.) Notably, there is no specific allegation that Guidewire gained access to ACCS through CNA.
>
> Secondly, there is no allegation that Guidewire either disclosed or used the secrets in developing Guidewire Insurance Suite, only that Guidewire "seemed to" develop its product "surprisingly quick[ly]" in Accenture's opinion, which is of no import. Accenture is not entitled to conduct a fishing expedition based upon such bare allegations; its DUTSA claim is dismissed. *See Knights Armament Co. v. Optical Systems Technology, Inc.*, 568 F. Supp. 2d 1369, 1377 (M.D. Fla. 2008) (dismissing UTSA counterclaim under *Twombly* where defendant stated that plaintiffs had access to the secrets through business dealings, but "[gave] no further details as to how [they] allegedly used the trade secrets."); *compare Savor, Inc. v. FMR Corp.*, 812 A.2d 894, 895, 897 (Del. Supr. 2002) (trade secret misappropriation pled where Savor alleged a purportedly unique combination of marketing strategies and processes for a rebate program, and that it provided the program to defendant under cover that the enclosed materials were "protected by various copyrights, patents pending, and trademark registrations").[27]

Access "somehow"? Access "somewhere"? A "similar" product? A "coincidence"? These allegations were no better

27. *Accenture*, 581 F. Supp. 2d at 662–64 (footnotes omitted).

than the allegations of *en masse* employee departures, product similarity, and suspicious timing in *Glenayre*. Yet, these might be the only trigger facts available to the plaintiff at the pleading stage. If so, filing an action would be premature and plaintiff's investigation should continue.

It is also noteworthy, however, that trade secrets cases are very fact intensive and many courts have found a sufficient basis for trade secrets claims on limited trigger facts. Indeed, direct evidence of misappropriation need not be alleged, nor even proven at trial. As the Eighth Circuit stated in affirming a trial verdict finding misappropriation where the plaintiff presented no direct evidence thereof, "direct evidence of industrial espionage is rarely available and not required."[28] Other courts have issued similar holdings to the effect that access plus subsequent development of similar products states a plausible misappropriation claim that can survive summary judgment as well as post-trial challenges. [29]

---

28. Pioneer Hi-Bred Int'l v. Holden Found. Seeds, 35 F.3d 1226, 1239 (8th Cir. 1994) (quotation omitted).

29. *See* Stratienko v. Cordis Corp., 429 F.3d 592, 600–01 (6th Cir. 2005) (stating it is sufficient for trade secret plaintiffs to present evidence that "(1) the misappropriating party had access to the secret and (2) the secret and the defendant's design share similar features," and reasoning that "[p]ermitting an inference of use from evidence of access and similarity is sound because misappropriation and misuse can rarely be proved by convincing direct evidence") (quotation omitted); Sokol Crystal Prods. v. DSC Commc'ns Corp., 15 F.3d 1427, 1432 (7th Cir. 1994) (affirming jury verdict because "once the jury concluded that (1) DSC had access to Sokol's trade secrets, and (2) DSC's product was similar to Sokol's, it was entirely reasonable for it to infer that DSC used Sokol's trade secret"); Leggett & Platt, Inc. v. Hickory Springs Mfg. Co., 285 F.3d 1353, 1361 (Fed. Cir. 2002) (showings of "access and similarity" of products "may support a trade secret misappropriation claim"); Contour Design, Inc. v. Chance Mold Steel Co., 2010 DNH 11, at *27–28 (D.N.H. 2010) (showings of "access and similarity—may support a trade secret misappropriation claim because they suggest that the defendant derived its product

INEVITABLE DISCLOSURE

Faced with the conundrum the district court acknowledged in *Accenture*—the trade secret plaintiff does not "know, prior to discovery, the details surrounding the purported theft"—plaintiffs increasingly pursue another option to establish trigger facts: the doctrine of inevitable disclosure. In inevitable disclosure cases, the court examines the same circumstances deemed defective in *Glenayre* and *Accenture*, yet finds a viable claim based upon certain additional facts, usually head-to-head competition by an executive or employee who cannot avoid drawing on his past employer's secrets to do his new job.[30] In other words, these circumstances dispense with the need for direct proof of misappropriation, a "no proof" approach (critics would

---

from the plaintiff's trade secret, rather than from an independent source") (quotation omitted); Bro-Tech Corp. v. Thermax, Inc., 651 F. Supp. 2d 378, 412 n.240 (E.D. Pa. 2009) (trade secret plaintiffs "may establish use or disclosure through inference, by showing that the defendant had access to plaintiff's trade secret, and that there are 'substantial similarities' between defendant's product and plaintiff's secret information"); PRG-Schultz Int'l, Inc. v. Kirix Corp., 2003 WL 22232771, at *7 (N.D. Ill. Sept. 22, 2003) (where defendants had access to trade secret during employment with plaintiff and thereafter created a similar software program, "a reasonable jury could conclude that the individual defendants misappropriated a trade secret from plaintiffs"*);* USA Power, LLC v. PacifiCorp, 235 P.3d 749, 761 (Utah 2010) (holding that "a jury can infer misappropriation . . . if presented with circumstantial evidence that shows access to information similar to the trade secret at issue").

30. *See* C & F Packing Co., Inc. v. IBP, Inc., 1998 WL 1147139, at *8–9 (N.D. Ill. Mar. 16, 1998) (quoting deposition testimony of former C & F Packing employee McDaniel in denying defense summary judgement motion in "inherent disclosure" case: "Q: Did you draw on your experience at C & F with the Italian sausage toppings to help solve problems at IBP? A: I tried to keep things separate. Whether I did it unknowingly or not, I cannot say.").

say) that has gained traction in other legal fields such as copyright and employment discrimination.[31] Indeed, inevitable disclosure claims have become *de rigueur*, with 100 appearing in published opinions by 2004.[32] This theory has antecedents dating back over a century,[33] but it did not really gain wide-spread acceptance until the Seventh Circuit's seminal 1995 decision in *PepsiCo, Inc. v. Redmond*.[34] Not all courts subscribe to this "no

31. *See* Robert Kirk Walker, *Ghosts in the Machine: Musical Creation and the Doctrine of Subconscious Copying*, A.B.A. LANDSLIDE, Vol. 9, No. 4, March/April 2017, at 48 (reviewing difficulty in separating "subconscious copying" from "independent creation" in copyright cases in light of the unlimited access to copyrighted material the Internet provides); Nancy Gertner, *Loser's Rules*, 122 YALE L.J. ONLINE 109, 110 (2012) ("In effect, today's plaintiff stands to lose unless he or she can prove that the defendant had explicitly discriminatory policies in place or that the relevant actors were overtly biased. It is hard to imagine a higher bar or one less consistent with the legal standards developed after the passage of the Civil Rights Act, let alone with the way discrimination manifests itself in the twenty-first century."); Annika L. Jones, Comment, *Implicit Bias as Social-Framework Evidence in Employment Discrimination*, 165 U. PA. L. REV. 1217 (2017) (arguing "implicit bias" and "unconscious discrimination" can be proven through social science research and can overcome *Daubert* challenges); Mark Newman, *When "Culture Fit" Is Really a Bias Cover: Assessment Not Always a Valid One for Job Candidates*, CHI. TRIB., May 22, 2017, § 2, at 3 ("Unconscious bias and the natural tendency to gravitate toward people similar to us can play out in hiring decisions.").

32. *See* William Lynch Schaller, *Trade Secret Inevitable Disclosure: Substantive, Procedural & Practical Implications of an Evolving Doctrine*, 86 J. PAT. & TRADEMARK OFF. SOC'Y 336 (2004) (collecting cases).

33. *See* Harrison v. Glucose Sugar Refining Co., 110 F. 304, 311 (7th Cir. 1902) ("Under the circumstances it would require something more than his mere denial to convince us that in the manufacture of glucose he would not employ the secrets of the business of appellee which had been confidentially communicated to him. He could not do otherwise. He was employed the rival for that purpose.").

34. 54 F.3d 1262 (7th Cir. 1995).

evidence" view, and some—notably courts in California, as exemplified by *Cypress Semiconductor Corp. v. Maxim Integrated Products, Inc.*[35]—reject the inevitable disclosure doctrine as a matter of policy.[36]

Comparing *PepsiCo* with *Cypress* illuminates the power and danger of the inevitable disclosure doctrine. In *PepsiCo*, the defendant William Redmond, who served as the General Manager of PepsiCo's California region (part of the Pepsi-Cola North America division, or "PCNA"), began interviewing with Quaker Oats to become the latter's Vice President of On-Premise Sales of Gatorade. In that position, Redmond would be responsible for defeating the very marketing plans he had prepared for PepsiCo for its competing products, including its All Sport drink. Redmond's secret interviews spanned five months and began with Quaker Oats' Gatorade division head, Donald Uzzi, himself a recent PepsiCo executive. Redmond eventually revealed his Quaker Oats opportunity to his superiors at PepsiCo, but he misstated his contemplated Quaker Oats position as "Chief Operating Officer" of the combined Gatorade and Snapple operations, even though his new position was more modest. He then waited two days, apparently in the hope of receiving a counter offer from PepsiCo, before telling his PepsiCo superiors that he had accepted the Quaker Oats position. PepsiCo immediately initiated litigation, and the district court—on the authority of the inevitable disclosure doctrine—granted a five-month

35. 236 Cal. App. 4th 243, 186 Cal. Rptr. 3d 486 (2015) (noting California courts' rejection of inevitable disclosure and awarding fees for "bad faith" trade secret litigation).

36. *See, e.g.*, Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443, 1458, 125 Cal. Rptr. 2d 277, 290–94 (2002) (rejecting *PepsiCo* as contrary to California public policy embodied in Section 16600 of the California Business and Professions Code, the California statute generally prohibiting noncompete agreements).

injunction barring Redmond from working for Quaker Oats and a permanent injunction prohibiting Redmond from using or disclosing PepsiCo's trade secrets or confidential information.

The Seventh Circuit offered a nuanced view of the situation in affirming the district's injunction order. Because the inevitable disclosure doctrine seems more controversial than the Seventh Circuit's narrow holding, we quote the Court of Appeals at length:

> The ITSA [Illinois Trade Secrets Act], *Teradyne*, and *AMP* lead to the same conclusion: a plaintiff may prove a claim of trade secret misappropriation by demonstrating that defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets. *See also* 1 Jager, *supra*, § 7.02[2][a] at 7–20 (noting claims where "the allegation is based on the fact that the disclosure of trade secrets in the new employment is inevitable, whether or not the former employee acts consciously or unconsciously"). The defendants are incorrect that Illinois law does not allow a court to enjoin the "inevitable" disclosure of trade secrets. Questions remain, however, as to what constitutes inevitable misappropriation and whether PepsiCo's submissions rise above those of the *Teradyne* and *AMP* plaintiffs and meet that standard. We hold that they do.
>
> PepsiCo presented substantial evidence at the preliminary injunction hearing that Redmond possessed extensive and intimate knowledge about PCNA's strategic goals for 1995 in sports drinks and new age drinks. The district court concluded

on the basis of that presentation that unless Redmond possessed an uncanny ability to compartmentalize information, he would necessarily be making decisions about Gatorade and Snapple by relying on his knowledge of PCNA trade secrets. It is not the "general skills and knowledge acquired during his tenure with" PepsiCo that PepsiCo seeks to keep from falling into Quaker's hands, but rather "the particularized plans or processes developed by [PCNA] and disclosed to him while the employer-employee relationship existed, which are unknown to others in the industry and which give the employer an advantage over his competitors." *AMP*, 823 F.2d at 1202. The *Teradyne* and *AMP* plaintiffs could do nothing more than assert that skilled employees were taking their skills elsewhere; PepsiCo has done much more.

Admittedly, PepsiCo has not brought a traditional trade secret case, in which a former employee has knowledge of a special manufacturing process or customer list and can give a competitor an unfair advantage by transferring the technology or customers to that competitor. *See, e.g., Glenayre Electronics, Ltd. v. Sandahl*, 830 F. Supp. 1149 (C.D. Ill. 1993) (preliminary injunction sought to prevent use of trade secrets regarding pager technology); *Stampede Tool Warehouse, Inc. v. May*, 1995 WL 121439 (Ill. App. 1st Dist. March 22, 1995) (preliminary injunction sought to prevent use of customer lists); *Colson*, 155 Ill. Dec. at 473, 569 N.E.2d at 1082 (same); *Television Telecommunication Systems, Inc. v. Saindon*, 169 Ill. App. 3d 8, 119 Ill. Dec. 500, 522

N.E.2d 1359 (2d Dist.) (preliminary injunction sought to prevent use of trade secrets regarding analog circuity in a wake-up call device), *appeal denied*, 122 Ill.2d 595, 125 Ill. Dec. 238, 530 N.E.2d 266 (1988). PepsiCo has not contended that Quaker has stolen the All Sport formula or its list of distributors. Rather PepsiCo has asserted that Redmond cannot help but rely on PCNA trade secrets as he helps plot Gatorade and Snapple's new course, and that these secrets will enable Quaker to achieve a substantial advantage by knowing exactly how PCNA will price, distribute, and market its sports drinks and new age drinks and being able to respond strategically. *Cf. FMC Corp. v. Varco Int'l, Inc.*, 677 F.2d 500, 504 (5th Cir. 1982) ("Even assuming the best of good faith, Witt will have difficulty preventing his knowledge of FMC's 'Longsweep' manufacturing techniques from infiltrating his work."). This type of trade secret problem may arise less often, but it nevertheless falls within the realm of trade secret protection under the present circumstances.

***

The district court also concluded from the evidence that Uzzi's actions in hiring Redmond and Redmond's actions in pursuing and accepting his new job demonstrated a lack of candor on their part and proof of their willingness to misuse PCNA trade secrets, findings Quaker and Redmond vigorously challenge. The court expressly found that:

> Redmond's lack of forthrightness on some occasions, and out and out lies on others, in the period between the time he accepted the position with defendant Quaker and when he informed plaintiff that he had accepted that position leads the court to conclude that defendant Redmond could not be trusted to act with the necessary sensitivity and good faith under the circumstances in which the only practical verification that he was not using plaintiff's secrets would be defendant Redmond's word to that effect.

The facts of the case do not ineluctably dictate the district court's conclusion. Redmond's ambiguous behavior toward his PepsiCo superiors might have been nothing more than an attempt to gain leverage in employment negotiations. The discrepancy between Redmond's and Uzzi's comprehension of what Redmond's job would entail may well have been a simple misunderstanding. The court also pointed out that Quaker, through Uzzi, seemed to express an unnatural interest in hiring PCNA employees: all three of the people interviewed for the position Redmond ultimately accepted worked at PCNA. Uzzi may well have focused on recruiting PCNA employees because he knew they were good and not because of their confidential knowledge. Nonetheless, the district court, after listening to the witnesses, determined otherwise. That conclusion was not an abuse of discretion.

***

> Thus, when we couple the demonstrated inevitability that Redmond would rely on PCNA trade secrets in his new job at Quaker with the district court's reluctance to believe that Redmond would refrain from disclosing these secrets in his new position (or that Quaker would ensure Redmond did not disclose them), we conclude that the district court correctly decided that PepsiCo demonstrated a likelihood of success on its statutory claim of trade secret misappropriation.[37]

Head-to-head competition and slight dishonesty carried the day in *PepsiCo*, but *PepsiCo* itself has not fared so well in California, as *Cypress* reflects. Just as Quaker Oats pursued multiple PepsiCo employees before filling the position Redmond ultimately accepted, Maxim pursued multiple Cypress employees to fill two touchscreen technology positions, one of which Cypress "Employee 60XX" initially accepted. Employee 60XX later declined the Maxim position after a war of words broke out between Cypress president T.J. Rodgers and Maxim president Tunc Doluca over Maxim's targeting of Cypress employees. Even though Employee 60XX was deterred, Cypress, in order to prevent trade secret theft, still sued for an injunction prohibiting Maxim from recruiting Cypress employees. After months of wrangling over whether Cypress had any actual trade secrets, Cypress suddenly and voluntarily dismissed its suit without prejudice. Cypress' about-face didn't work; Maxim prevailed on its claim for "bad faith" in spite of Cypress' *volte-face*.

37. 54 F.3d at 1269–71 (footnotes omitted).

The California Court of Appeal affirmed the trial court's bad faith findings and fee award of approximately $181,000. The appellate court made its views clear: mere solicitation of a rival's employees is not actionable, and inevitable disclosure claims cannot be used to change this outcome in California. The Court of Appeal held:

> The second theory on which Cypress sought to claim misappropriation of a trade secret is that Maxim was seeking to hire Cypress employees "in order to acquire and use Cypress's confidential information in an effort to catch up . . . in the development of touchscreen products." This allegation is repeated several times in slightly variant forms, i.e., that "Maxim . . . has been using a headhunter to raid Cypress's touchscreen employees to obtain Cypress's touchscreen technology for Maxim"; that "[u]pon information and belief, Maxim is trying to raid Cypress's touchscreen employees in order to acquire Cypress's confidential information"; and that "in targeting the specific employees with knowledge of Cypress's touchscreen technology, Maxim is improperly attempting to acquire, use or disclose Cypress's substantive confidential information regarding its touchscreen technology. This is threatened misappropriation . . . ."
>
> In other words, according to this theory Maxim was seeking to hire Cypress employees so that it could appropriate whatever trade secrets they might know. We may assume that at least some aspects of "Cypress's touchscreen technology" were genuine trade secrets. It is absolutely clear,

however, that no such misappropriation had occurred when the complaint was filed. Maxim had extended an offer to one Cypress employee, who initially accepted but was ultimately prevailed upon to remain with Cypress. So far as anything in the record suggests, Maxim never extended an offer to any other "touchscreen employee." Therefore it never had the occasion or opportunity to engage in the posited brain-picking. As reflected in the last sentence quoted above, the claim was purely one of threatened misappropriation.

Nothing in the complaint, and nothing submitted by Cypress since filing the complaint, lends any color to the naked assertion that Maxim was pursuing Cypress employees with the object of extracting trade secrets from them. In the trial court Maxim suggested that Cypress's claims in this regard implicitly rested on the doctrine of inevitable disclosure, under which some jurisdictions will permit a plaintiff to substantiate a trade secret claim against a departing employee "'by demonstrating that [the] defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets.'" (*Whyte v. Schlage Lock Co.* (2002) 101 Cal. App. 4th 1443, 1458, 125 Cal. Rptr. 2d 277 (*Whyte*), quoting *PepsiCo, Inc. v. Redmond* (7th Cir. 1995) 54 F.3d 1262, 1269.) This doctrine, as Maxim pointed out, has been flatly rejected in this state as incompatible with the strong public policy in favor of employee mobility. (*Whyte, supra*, at p. 1462, citing Bus. & Prof. Code, § 16600, and cases applying it.) The inevitable disclosure doctrine would

> contravene this policy by "permit[ting] an employer to enjoin the former employee without proof of the employee's actual or threatened use of trade secrets based upon an inference (based in turn upon circumstantial evidence) that the employee inevitably will use his or her knowledge of those trade secrets in the new employment. The result is not merely an injunction against the use of trade secrets, but an injunction restricting employment." (*Whyte, supra*, at pp. 1461–1462.)
>
> Cypress expressly disclaimed any reliance on the doctrine of inevitable disclosure, but in the absence of that doctrine we can detect no basis for its allegation of threatened misappropriation. Indeed, the result condemned in *Whyte, supra*, 101 Cal. App. 4th at page 1461—"to enjoin [hiring of its] . . . employee[s] without proof of [any] . . . actual or threatened use of trade secrets"—is precisely what Cypress prayed for here: "a preliminary and permanent injunction against Defendants . . . enjoining/restraining them from soliciting Cypress's touchscreen employees." Given the complete absence of any coherent factual allegations suggesting a threatened misappropriation, Cypress's second theory of relief was an inevitable disclosure claim, or it was no claim at all—and in either case, it did not state grounds for relief under California law.[38]

38. 236 Cal. App. 4th at 264–65.

The tension between *PepsiCo* and *Cypress* is self-evident. With the inevitable disclosure doctrine, thin trigger facts prevailed in *PepsiCo*; without the inevitable disclosure doctrine, thin trigger facts drew sanctions in *Cypress*. Put differently, an employee's departure for a similar job does not alone justify a trade secret action, but just a little more in conjunction may—if inevitable disclosure applies. Thus, for investigation purposes one must always ask just how "inevitable" is disclosure, determine whether the relevant jurisdiction follows this principle, and then ascertain whether there has been any wrongful conduct.[39]

FAILED DEALS

Failed deal cases abound,[40] and almost all present "trigger" inquiries similar to those in *Glenayre*, *Accenture*, *PepsiCo*, and *Cypress*. The most egregious involve the suitor's poaching of the target's key employees immediately before or after the deal has collapsed, as one might guess.[41] A review of a recent Illinois trade secret "trigger" case, *Destiny Health, Inc. v. Connecticut General Life Insurance Co.*,[42] demonstrates the dynamics of failed deal disputes from a trade secret perspective.

---

39. A whitepaper summarizing the inevitable disclosure doctrine and a chart summarizing the position each state has taken on the doctrine can be found at: https://www.faegrebd.com/webfiles/Inevitable%20Disclosure.pdf.

40. *See, e.g.*, Texas Advanced Optoelectronic Solutions, Inc. v. Renesas Electronics America, Inc., 888 F.3d 1322 (Fed. Cir. 2018) (upholding jury finding that putative buyer misappropriated ambient light sensor combination secret following failed deal to buy plaintiff's company); Smith v. Dravo Corp., 203 F.2d 369 (7th Cir. 1953) (putative buyer's theft of shipping container design trade secrets following failed deal to buy plaintiff's company).

41. *See, e.g.*, Pactiv Corp. v. Menasha Corp., 261 F. Supp. 2d 1009 (N.D. Ill. 2003) (refusing to enforce contract clause prohibiting employee raiding in contract between parties to an unsuccessful business sale).

42. 2015 IL App (1st) 142530, 39 N.E.3d 275 (2015).

In *Destiny*, a case decided on summary judgment, insurer Cigna decided to combine its existing wellness program with a points-based program as part of a package to offer to its employer-clients. Cigna discussed this idea with Destiny, a third-party vendor that had pioneered Vitality, a wellness-based healthcare program designed to make persons healthier by awarding them points for healthy activities. Because Cigna sought to review sensitive Destiny data, the parties amended their existing confidentiality agreement to enable the free exchange of information and to protect Destiny. Destiny then provided Cigna, during due diligence in September 2007, with confidential information concerning its Vitality program, including profitability and how it determined to award points. The following month, October 2007, Cigna advised Destiny that Cigna could not move forward with Destiny due to "system challenges," a euphemism (Cigna later explained) for multiple problems with Destiny's program and its profitability, among other things. Six months later Cigna began reviewing other points program vendors, and then in January 2009, Cigna announced a deal with IncentOne to provide a wellness program.

Unhappy with both the outcome and the sequence of events, Destiny sued Cigna for trade secret misappropriation in April 2009. The trial court granted summary judgement in favor of Cigna in July 2014—nearly seven years after Cigna had terminated the Destiny deal. The Illinois Appellate Court affirmed, noting that Cigna's access to Destiny's confidential information, without more, did not show trade secret misappropriation. The appellate court then stressed the significant differences between the Destiny and IncentOne programs, along with the independent development testimony of Cigna and IncentOne, as defeating an inference of misappropriation. Finally, and perhaps most relevant here, the court rejected inevitable disclosure as a ground for denying summary judgement:

¶ 39 Cigna responds by arguing that *PepsiCo* and *Strata* [an Illinois Appellate Court opinion following *PepsiCo*] are distinguishable because they involve employees leaving one company to work for a competitor. Cigna cites *Omnitech International, Inc. v. Clorox Co.*, 11 F.3d 1316 (5th Cir. 1994) (*Omnitech*), and argues that the inevitable disclosure doctrine should not apply in trade secret cases arising out of failed commercial transactions.

¶ 40 In *Omnitech*, the plaintiff and Clorox signed a nondisclosure agreement and a letter of intent in connection with the possible sale of Omnitech's "Dr. X" line of roach spray. Omnitech agreed to share certain proprietary information with Clorox while keeping Clorox's interest in the insecticide market confidential. Clorox was given the right to conduct laboratory and marketing tests of Dr. X and was granted the right of first refusal to purchase Omnitech's assets. Clorox later acquired another line of insecticides from a different manufacturer and decided not to go forward with the Dr. X acquisition. Omnitech filed suit alleging trade secret misappropriation. Omnitech sought to rely not on direct evidence, but rather on an inference of misappropriation from the fact that Clorox had access to its proprietary information. On appeal, the United States Court of Appeals for the Fifth Circuit held that such evidence was insufficient as a matter of law to support an inference that Clorox improperly disclosed or used any of Omnitech's confidential information. The court explained:

> Certainly 'misappropriation' of a trade secret means more than simply using knowledge gained through a variety of experiences, including analyses of possible target companies, to evaluate a potential purchase. To hold otherwise would lead to one of two unacceptable results: (i) every time a company entered into preliminary negotiations for a possible purchase of another company's assets in which the acquiring company was given limited access to the target's trade secrets, the acquiring party would effectively be precluded from evaluating other potential targets; or (ii) the acquiring company would, as a practical matter, be forced to make a purchase decision without the benefit of examination of the target company's most important assets—its trade secrets. *Omnitech*, 11 F.3d at 1325.

¶ 41 We find that the facts of this case are more akin to the facts in *Omnitech* than to the facts in *PepsiCo* or *Strata*. Unlike *PepsiCo* and *Strata*, this case does not involve an employee who possessed trade secrets leaving his employer to work for a competitor. Rather, this case involves two companies that had entered into negotiations and shared confidential information. The fact that the information provided by Destiny might have made Cigna more informed in evaluating whether to partner with Destiny or another vendor in the development of an incentive-points program does

> not support an inference that Cigna misappropriated Destiny's trade secrets absent some showing that Cigna would not have been able to develop its incentive-points program without the use of Destiny's trade secrets.[43]

Destiny, of course, bears more than a passing resemblance to *Accenture*, and *Destiny* arguably should have been dismissed at the pleadings stage, as in *Accenture*, for failure to allege concrete trigger facts showing misappropriation. But that did not happen, and the parties thus ended up battling over the complete absence of misappropriation proof until the appellate court affirmed summary judgement—almost eight years after the parties had gone their separate ways. In *Destiny*, as in all of these cases except *PepsiCo*, the absence of a controlling appellate opinion defining what does and does not constitute proper pleading of trade secret trigger facts resulted in years of needless litigation.

DEFEND TRADE SECRETS ACT

Do these pre-DTSA cases still matter in the wake of the DTSA? The answer is yes, no, and maybe.

The DTSA amended the Economic Espionage Act in 2016 to provide a trade secret civil cause of action for private plaintiffs.[44] The DTSA is modelled after the Uniform Trade Secrets Act

43. 2015 IL App (1st) 142530, at ¶¶ 39–41, 39 N.E.3d at 284–85 (2015).

44. 18 U.S.C. § 1836(b)(1) (2016) ("An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.").

(UTSA), some form of which virtually all states have adopted.[45] The DTSA departs from the UTSA in certain respects, however, such as its explicit statutory authorization of property seizures to secure trade secret misappropriation evidence[46] and its apparent narrowing (if not exclusion) of the inevitable disclosure doctrine.[47] But its most important feature is that it allows private plaintiffs to prosecute their federal law trade secret actions in federal court.[48]

Federal Jurisdiction Under the DTSA

The first thing to consider under the DTSA is federal subject matter jurisdiction, found in the statutory requirement that the secret be "related to a product or service used in, or intended for use in, interstate or foreign commerce."[49] The constitutional limits of federal jurisdiction, such as they are, arise under the "aggregation principle" tracing back to *Wickard v. Filburn*.[50] In *Wickard*, the United States Supreme Court discarded prior distinctions between "manufacture" and "production" and focused instead on whether an activity has "substantial economic

45. A useful chart comparing the DTSA with the UTSA can be found at https://faircompetitionlaw.files.wordpress.com/2017/02/ts-50-state-chart-20170204-utsa-comparison-beck-reed-riden-20161.pdf.

46. 18 U.S.C. § 1836(b)(2) (setting forth procedures for *ex parte* court orders allowing civil "seizure of property necessary to prevent the propagation or dissemination of the trade secret," and authorizing damages for wrongful seizure).

47. 18 U.S.C. § 1836(b)(3)(A)(i)(I-II).

48. 18 U.S.C. § 1836(c) ("The district courts of the United States shall have original jurisdiction of civil actions brought under this section.").

49. *Id*.

50. 317 U.S. 120 (1942). *See generally* James B. Barnes, *The Font of Federal Power:* Wickard v. Filburn *and the Aggregation Principle*, J. SUP. CT. HIST., Vol. 42, No. 1, 2017, at 49.

effects" on interstate commerce, either individually or in the aggregate. A famous and familiar example of the principle in action is *Heart of Atlanta Motel, Inc. v. United States*,[51] in which the Court reviewed the Civil Rights Act of 1964 and held that individual acts of discrimination, taken together, have a substantial economic effect on commerce. Although rare, the Court has from time to time struck down federal statutes as exceeding the Commerce Clause power, as in *United States v. Lopez*.[52] Given the inherently economic and interstate character of trade secrets, there seems little chance of a successful Commerce Clause challenge to the DTSA.

The question instead is whether the facts of a case satisfy the interstate commerce requirement set forth in the DTSA. Although a pre-DTSA case, an instructive decision on this question is the Second Circuit's well-known trade secret opinion in *United States v. Aleynikov*.[53] The facts of that high-profile controversy are by now familiar to almost anyone following the trade secret field: (1) Aleynikov worked as a computer programmer on high frequency trading for Goldman Sachs in New York; (2) Aleynikov decided to take a job with Teza Technologies, a rival high frequency trading firm in Chicago; (3) Aleynikov downloaded more than 500,000 lines of Goldman Sachs computer code and uploaded them to a server in Germany on his last day before leaving; and (4) Aleynikov subsequently was arrested and indicted for stealing trade secrets—Goldman Sach's com-

51. 379 U.S. 241 (1964).

52. 514 U.S. 549 (1995) (reviewing Gun-Free School Zones Act and finding activity of possessing a firearm was not economic for interstate commerce purposes). *See also* United States v. Morrison, 529 U.S. 598 (2000) (reviewing Violence Against Women Act and finding that gender-motivated crimes were not economic for interstate commerce purposes).

53. 676 F.3d 71 (2d Cir. 2012).

puter code—in violation of the criminal provisions of the Economic Espionage Act (EEA). Aleynikov was convicted and sentenced to 97 months in prison. He then appealed to the Second Circuit.

In a rare reversal, the Second Circuit held that the EEA indictment was insufficient as a matter of law on the facts of the case. As it was then written, Section 1832, the section of the EEA under which Aleynikov was indicted, required that the trade secret be "related to or included in a product that is produced for or placed in interstate or foreign commerce."[54] The Second Circuit held that Aleynikov's acts did not fit the statute under which he was indicted:

> The district court interpreted the phrase "produced for" interstate or foreign commerce more broadly. It held that the HFT system was "produced for" interstate commerce because "the sole purpose for which Goldman purchased, developed, and modified the computer programs that comprise the Trading System was to engage in interstate and foreign commerce" and because "Goldman uses the Trading System to rapidly execute high volumes of trades in various financial markets" and "[t]he Trading System generates many millions of dollars in annual profits."

54. 18 U.S.C. § 1832(a) ("Whoever, with intent to convert a trade secret, *that is related to or included in a product that is produced for or placed in interstate or foreign commerce*, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . without authorization . . . downloads, uploads, . . . transmits, . . . or conveys such information" is guilty of a federal offense, and may be imprisoned for up to 10 years.) (emphasis added).

Aleynikov, 737 F. Supp. 2d at 179. Under that interpretation, a product is "produced for" interstate or foreign commerce if its purpose is to facilitate or engage in such commerce.

The district court erred by construing the phrase––"produced for . . . interstate or foreign commerce"—"in a vacuum." *See Davis v. Mich. Dep't of Treasury*, 489 U.S. 803, 809, 109 S. Ct. 1500, 103 L. Ed. 2d 891 (1989). "It is a fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *Id*. That way, a statutory phrase "gathers meaning from the words around it." *Jones v. United States*, 527 U.S. 373, 389, 119 S. Ct. 2090, 144 L. Ed. 2d 370 (1999) (internal quotation marks omitted). The district court's broad interpretation of the phrase "produced for" commerce becomes untenable in light of the paired phrase "placed in" commerce. Since every product actually sold or licensed is by definition produced for the purpose of engaging in commerce, every product that is "placed in" commerce would necessarily also be "produced for" commerce—and the phrase "placed in" commerce would be surplusage. This interpretation is inconsistent with "one of the most basic interpretive canons, that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant." *Corley v. United States*, 556 U.S. 303, 314, 129 S. Ct. 1558, 173 L. Ed. 2d 443 (2009) (internal quotation marks and alteration omitted); *see also Duncan v. Walker*, 533 U.S. 167, 174, 121 S. Ct.

2120, 150 L. Ed. 2d 251 (2001) ("It is our duty to give effect, if possible, to every clause and word of a statute." (internal quotation marks omitted)). "Judges should hesitate to treat statutory terms in any setting as surplusage, and resistance should be heightened when the words describe an element of a criminal offense." *Jones v. United States*, 529 U.S. 848, 857, 120 S. Ct. 1904, 146 L. Ed. 2d 902 (2000) (internal quotation marks and alterations omitted; emphasis added).

Even construed in isolation, the phrase "produced for . . . interstate or foreign commerce" cannot command the breadth that the district court and the Government ascribe to it. *See generally Fed. Commc'ns Comm'n v. AT & T Inc.*, ___ U.S. ___, 131 S. Ct. 1177, 1184, 179 L. Ed. 2d 132 (2011) ("[C]onstruing statutory language is not merely an exercise in ascertaining 'the outer limits of [a word's] definitional possibilities' . . . ." (quoting *Dolan v. U.S. Postal Serv.*, 546 U.S. 481, 486, 126 S. Ct. 1252, 163 L. Ed. 2d 1079 (2006))). At oral argument, the Government was unable to identify a single product that affects interstate commerce but that would nonetheless be excluded by virtue of the statute's limiting language. And even if one could identify one such example, or two, it would not be a category that would demand the attention of Congress, or be expressed in categorical terms.

If § 1832(a) was intended to have such a sweep, we would expect to see wording traditionally understood to invoke the full extent of Congress's regu-

latory power under the Commerce Clause. Notably, the EEA was enacted the year after the Supreme Court issued its landmark decision in *United States v. Lopez*, which held that Congress's Commerce Clause authority is limited to those activities that "substantially affect interstate commerce." 514 U.S. 549, 558–59, 115 S. Ct. 1624, 131 L. Ed. 2d 626 (1995). The Supreme Court observes a distinction between "legislation invoking Congress' full power over activity substantially 'affecting . . . commerce'" and legislation which uses more limiting language, such as activities "'in commerce,'" and thereby does not purport to exercise the full scope of congressional authority. *Jones*, 529 U.S. at 856, 120 S. Ct. 1904 (quoting *Russell v. United States*, 471 U.S. 858, 859–60 & n.4, 105 S. Ct. 2455, 85 L. Ed. 2d 829 (1985)). The temporal proximity between the enactment of the EEA and the decision in *Lopez* makes significant the omission from the EEA of the language blessed in that case as invoking the outer limit of Congress's regulatory authority.

***

Goldman's HFT system was neither "produced for" nor "placed in" interstate or foreign commerce. Goldman had no intention of selling its HFT system or licensing it to anyone. *Aleynikov*, 737 F. Supp. 2d at 175. It went to great lengths to maintain the secrecy of its system. The enormous profits the system yielded for Goldman depended on no one else having it. Because the HFT system was not designed to enter or pass in commerce, or

> to make something that does, Aleynikov's theft of source code relating to that system was not an offense under the EEA.[55]

In response to that case, the Theft of Trade Secrets Act of 2012 altered the language to expand the scope of the information protected by the EEA. The current language drops the "produced for" and "placed in" conditions, replacing them with the broader phrase noted above, "related to a product or service used in, or intended for use in, interstate or foreign commerce." Precisely how federal courts will construe and apply this new language are open questions, but the answer seems to be "narrowly" if *Aleynikov* is any indication.[56]

Federal Court Pleading of Misappropriation "Triggers" Under the DTSA

Twombly and its progeny set forth the governing pleading standards for federal court civil actions, and these apply to trade secret actions, as *Accenture* reflects. At first blush there would appear to be nothing special about DTSA actions removing them from the reach of *Twombly*. First impressions can be deceiving, however.

Putting aside the peculiar need to allege facts satisfying the DTSA's interstate commerce clause, as in *Aleynikov*, and putting aside inevitable disclosure for the moment, at least one class of cases demands heightened pleading specificity: *ex parte* seizure

---

55. 676 F.3d at 80–82 (footnotes omitted).

56. *But see* People v. Aleynikov, 2018 NY Slip Op. 03174, ___ N.Y.3d ___, ___ N.E.3d ___, ___ N.Y.S.3d ___ (N.Y. Ct. App. May 3, 2018) (upholding Aleynikov's New York state court conviction; statute that criminalizes the making of a tangible reproduction or representation of secret scientific material by electronically copying or recording applies to the acts of a defendant who uploads proprietary source code to a computer server).

proceedings. The DTSA is explicit on this issue in Section 1836(b)(2): it requires an affidavit or verified complaint[57] and then places the burden on plaintiff at the seizure hearing "to prove the facts supporting the findings of fact and conclusions of law necessary to support the [seizure] order."[58] Further, it prohibits an order "unless the court finds that it *clearly* appears from specific facts" that the plaintiff has satisfied this burden.[59] One would think a federal court would be fairly insistent on factual detail, especially regarding vital trigger facts, before issuing such draconian relief.

More subtle is whether the DTSA might prompt federal courts to adopt more stringent "trigger" pleading standards for run-of-the-mill cases not involving seizures. The Racketeer Influenced and Corrupt Organizations Act (RICO) jurisprudence suggests one direction federal courts might take. Faced with a potential flood of garden variety state law fraud cases masquerading as federal court RICO actions, federal courts disregarded RICO's plain language and invented one barrier after another to pleading RICO civil claims. The United States Supreme Court frowned on such judicial limitations in *Sedima, SPRL v. Imrex Co., Inc.*,[60] but the lower court message has remained: RICO will be resisted. Today, that resistance often takes place in the name of the Supreme Court's decision in *H.J. Inc. v. Northwestern Bell Telephone Co.*,[61] in which the Court established the "continuity-

57. 18 U.S.C. § 1836(b)(2)(A)(i).

58. 18 U.S.C. § 1836(b)(2)(F)(ii).

59. 18 U.S.C. § 1836(b)(2)(A)(ii) (emphasis added).

60. 473 U.S. 479 (1985) (holding that RICO does not require a prior criminal conviction of either a predicate act or a RICO violation, nor does RICO require a special "racketeering injury").

61. 492 U.S. 229 (1989).

plus-relationship" test governing pleading and proof of a racketeering "pattern." Rare indeed is a civil case that meets this standard.[62]

If federal courts take this tack in trade secret cases, perhaps it will appear in the form of strict application of *Twombly*, rather than as an explicit, specialized legal pleading standard unique to trade secret cases. It is not hard to imagine a federal appeals court holding that alleged trigger facts fail to set forth a "plausible" claim under the Supreme Court's post-*Twombly* pleading opinion in *Ashcroft v. Iqbal*.[63] There the Court noted that "whether a complaint states a plausible claim for relief will, as the Court of Appeals observed, be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense."[64] As the Court stressed in the very next sentence in *Iqbal*, "where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'show[n]'—that the pleader is entitled to relief."[65] The conclusory trigger facts alleged in *Glenayre*, *Accenture*, *Cypress*, and *Destiny* did not appear to rise above a "mere possibility of misconduct," and even *PepsiCo* barely did so. In truth, properly understood, in all but *PepsiCo*, the allegations were in equipoise and thus well short of the "plausibility" mark.[66]

---

62. *See, e.g.*, Raybestos Products Co. v. Younger, 54 F.3d 1234 (7th Cir. 1995) (upholding RICO verdict of almost $4 million based upon extortionate settlement demand letter).

63. 556 U.S. 662 (2009).

64. 556 U.S. at 679.

65. *Id*. (quoting FED. R. CIV. P. 8(a)(2)).

66. *See, e.g.*, United States v. Pulgar, 789 F.3d 807, 812 (7th Cir. 2015) ("But drug-distribution conspiracies hold a unique position in our legal sufficiency jurisprudence. In these special cases, we will also overturn a conviction when

What is really at issue here is a problem akin to the "parallel behavior" mess in antitrust law that gave rise to *Twombly* itself. In parallel conduct cases, one company takes some action, say, raising prices, and then competitors quickly follow suit. This might indicate an illegal price fixing agreement, but it might also indicate perfectly legal, "follow the leader" market behavior, sometimes called "conscious parallelism." Thus, parallel conduct, by itself, should not be enough to subject the defendant to the extraordinary time and expense of antitrust proceedings only to end where the case began—with no evidence backing an allegation of wrongdoing. Yet, despite *Twombly*, courts are reluctant to dismiss suspicious parallel conduct cases at the pleading stage. For example, in *In re Text Messaging Antitrust Litigation*,[67] an antitrust class action, the Court of Appeals, speaking through Judge Posner, noted that "[p]leading standards in federal litigation are in ferment after *Twombly* and *Iqbal*,"[68] but found the allegations under review survived dismissal because they amounted to a kind of "parallel plus."[69] Even so, the case eventually ended in summary judgment in favor of the defendants, which the Seventh Circuit affirmed in Judge Posner's later opinion in *In re: Text Messaging Antitrust Litigation II*.[70]

---

the plausibility of a mere buyer-seller arrangement is the same as the plausibility of a drug-distribution conspiracy. *See* United States v. Johnson, 592 F.3d 749, 755 (7th Cir. 2010) ("In this situation, the evidence is in equipoise . . . so the jury necessarily would have to entertain a reasonable doubt on the conspiracy charge.")).

67. 630 F.3d 622, 626–27 (7th Cir. 2010).

68. *Id*. at 627.

69. *Id*. at 628 (noting allegations (i) that 90% of the text messaging market was controlled by four firms, (ii) that those firms had steeply falling costs yet raised their prices, and (iii) that the four firms suddenly changed their heterogeneous and complex pricing structures to a uniform pricing structure "and then simultaneously jacked up their prices by a third").

70. 782 F.3d 867 (7th Cir. 2015).

Inevitable Disclosure Under the DTSA

Section 1836(b)(3)(A)(i) has two provisions bearing upon inevitable disclosure.[71] In subsection (I), the statute states that "in a civil action brought under this subsection," a district court can grant an injunction to prevent actual or threatened disclosure so long as the order does not "prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows."[72] Subsection (II), in turn, provides that "in a civil action brought under this subsection," an injunction cannot "otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."[73] What do these provisions mean?

Subsection (I) seems to be an explicit limitation on inevitable disclosure claims—or more precisely, on inevitable disclosure claims "in a civil action brought under this subsection." When applicable, this subsection prevents a total ban on employment and demands evidence of trigger facts beyond mere retained knowledge to justify even a narrower injunction. By its terms, it does not apply to failed deal scenarios like *Destiny* or to any other settings missing employee thieves. Subsection (II) would appear to have even narrower applicability, as few states other than California have broad bans on restraints of a "lawful pro-

71. *See generally* Kenneth J. Vanko, *Revisiting the Seventh Circuit's Decision in PepsiCo: Inevitable Disclosure Injunctions in the Wake of the Federal Defend Trade Secrets Act of 2016*, SEVENTH CIR. RIDER (April 2017), at 50–53.

72. 18 U.S.C. § 1836(b)(3)(A)(i)(I).

73. 18 U.S.C. § 1836(b)(3)(A)(i)(II).

fession, trade, or business." Still, some have prohibitions on restraints for certain professions, like doctors and lawyers.[74] And others, like Illinois, bar noncompetition agreements for television personalities and low-paid workers.[75]

One wrinkle on subsections (I) and (II) is whether they will have any effect on pendent *state law* claims for trade secret theft. Both subsections are qualified by the language preceding them in subsection (b)(3)(A)(i), namely "in a civil action brought under this subsection." The answer will no doubt turn on the meaning of "brought under." This phrase might mean only DTSA claims themselves are restricted when it comes to injunctions. Or it might mean any action involving a DTSA claim, which would necessarily include pendent state law trade secret actions. For example, in determining the scope of the Federal Circuit Court of Appeals' jurisdiction, the Supreme Court in *Christianson v. Colt Industries Operating Corp*.[76] construed the "arising under any Act of Congress relating to patents" language of 28 U.S.C. § 1338(a). The Court held that "a claim supported by alternative theories in the complaint may not form the basis for § 1338(a) jurisdiction unless patent law is essential to each of those theories."[77] Obviously, under this standard the DTSA is not "essential" to a state law trade secret theory, unless

74. *See, e.g.*, Dowd & Dowd Ltd, Gleason, 181 Ill.2d 358, 693 N.E.2d 358 (1998) (holding that lawyer noncompetition agreements are void, except those governing retired partners).

75. *See* Broadcast Industry Free Market Act, 820 ILCS 17/10(a) ("No broadcasting industry employer may require in an employment contract that an employee or prospective employee refrain from obtaining employment in a specific geographic area for a specific period of time after termination of employment with that broadcasting industry employer."); Illinois Freedom to Work Act, 820 ILCS 90/1 *et seq*. (2017) ("A covenant not to compete entered into between an employer and a low-wage employee is illegal and void.").

76. 486 U.S. 800 (1988).

77. 486 U.S. at 810.

a court takes the broad view that "essential" turns on whether there would be no federal court subject matter jurisdiction over the state law claim without the DTSA. At least in diversity cases, federal court jurisdiction would exist independent of the DTSA, meaning the DTSA would be irrelevant rather than essential to such state law trade secret claims.

A narrow reading of "brought under" is also supported by the anti-preemption language found in 18 U.S.C. § 1838.[78] Section 1838 states that the DTSA does not displace any state law remedies. This explicit language can be reconciled with the DTSA's injunction limitations in Section 1836 if one assumes the specific (Section 1838) controls over the general (Section 1836). In addition, all statutory provisions are to be read together in such a way as to avoid rendering one superfluous.[79] From this vantage point, the simplest answer would be that the DTSA injunction limitations only apply to DTSA injunctions; state law injunctions are in no way restricted or displaced in light of Section 1838.

CONCLUSION

As should be apparent, the scope of a trade secret investigation necessarily depends on an understanding of relevant federal and state law. Factual triggers under some state laws may be insufficient under others, as the *PepsiCo*/*Cypress* comparison above shows. And these state law triggers do not automatically

78. 18 U.S.C. § 1838 ("Except as provided in section 1833(b), this chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act.").

79. Hibbs v. Winn, 542 U.S. 88, 101 (2004).

reflect the DTSA standards. Moreover, if one is proceeding under the property seizure section of the DTSA, heightened factual "trigger" pleadings are required. Unfortunately, few state or federal appellate decisions comprehensively limn these triggers for pleading purposes. The best practice, then, is to err on the side of caution and to search for as many true trigger facts as possible on misappropriation.

DISPUTED ISSUES IN AWARDING UNJUST ENRICHMENT DAMAGES IN TRADE SECRET CASES

*David S. Almeling, Walter Bratic, Monte Cooper, Alan Cox & P. Anthony Sammi**

I. INTRODUCTION

There are three primary forms of compensatory damages in trade secret cases: unjust enrichment, actual loss, and a reasonable royalty. This article addresses unjust enrichment damages.

In civil cases involving trade secret misappropriation, a successful plaintiff can recover a defendant's unjust enrichment that was caused by the misappropriation. Both state law and federal law use similar language in permitting unjust enrichment damages:

- Federal Defend Trade Secrets Act ("DTSA"): "damages for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss"[1]

* David Almeling is a partner with O'Melveny & Myers LLP in San Francisco; he was the primary author of Sections I and III. Walter Bratic is a Managing Director of OverMont Consulting, a division of Whitley Penn LLC, in Houston; he was the primary author of Section VI. Monte Cooper is Of Counsel with Orrick, Herrington & Sutcliffe in Menlo Park; he was the primary author of Section IV. Alan Cox is Chair of the Global Intellectual Property Practice of NERA Economic Consulting in San Francisco; he was the primary author of Section V. P. Anthony Sammi is a partner with Skadden, Arps, Slate, Meagher & Flom LLP in New York; he was the primary author of Section II. The opinions expressed in this article are those of the authors and do not necessarily reflect the views of the firms or clients.

1. 18 U.S.C. § 1836(b)(3)(B)(i)(II).

- State-based Uniform Trade Secrets Act ("UTSA"): "unjust enrichment caused by misappropriation that is not taken into account in computing actual loss"[2]

We focus on unjust enrichment damages because it is often the largest measure of damages in trade secret cases and because it contains several disputed issues. This article addresses five such issues:

1. whether unjust enrichment can include the entire fair market value of the trade secret defendant;
2. the appropriate duration of unjust enrichment damages;
3. the appropriate role of burden shifting in determining defendant's profits in the context of unjust enrichment damages;
4. how to avoid double-counting of damages between unjust enrichment and actual loss; and
5. under what circumstances convoyed sales should be included within unjust enrichment damages.

II. UNJUST ENRICHMENT AS THE ENTIRE FAIR MARKET VALUE OF THE DEFENDANT

In December 2016, The Sedona Conference Working Group on Patent Damages and Remedies (Working Group 9) published *The Sedona Conference Commentary on Patent Reasonable Royalty Determinations* (the "Patent Commentary").[3] The Patent Commentary includes certain principles and best practices concerning the Entire Market Value Rule ("EMVR"), which, in the

2. Uniform Trade Secrets Act (UTSA) § 3(a) (amended 1985).

3. *Available at* https://thesedonaconference.org/publication/WG9%20Patent%20Damages%20and%20Remedies.

context of patent law, "allows for the recovery of damages based on the value of an entire apparatus containing several features only when the feature patented constitutes the basis for customer demand."[4] Those principles and best practices are reproduced below for context:

> **Principle No. 3**: In cases involving an accused product with many components, the royalty should not be applied to the entire market value of the accused product unless it is shown that the patented feature or method provides the basis for customer demand for the product or substantially creates the value of the component parts.
>
> **Best Practice 1**: When determining whether the entire market value rule (EMVR) applies, the basic, underlying functionality of an accused product or process must not be disregarded.
>
> **Best Practice 2**: When determining whether the EMVR applies, it is important to consider whether the particular claimed invention was in fact the basis for consumer demand, and not merely one alternative among noninfringing alternatives to achieve a desired solution.
>
> **Principle No. 4(a)**: Where a patent claim is drawn to an individual component of a multi-component product that is found to infringe, and the entire market value rule does not apply, it is necessary to apportion the royalty base between its patented and unpatented features.

4. *Id*. at sec. III.B.

> **Principle No. 4(b)**: It may be appropriate to consider the smallest salable unit containing the feature or embodying the patented method for use as the apportioned royalty base; however, consideration of further apportionment may be required in assessing the royalty rate to ensure that the royalty reflects only the value of the patented features.

This section addresses whether and in what circumstances the unjust enrichment measure of damages can include the entire fair market value of the trade secret defendant. A preliminary question is whether the EMVR is applicable in trade secret cases at all.

A. Is the Entire Market Value Rule Applicable in Trade Secret Cases?

The EMVR originated in patent law, but that does not necessarily preclude its applicability to trade secret law. Courts regularly consider patent law precedents when determining damages for trade secret misappropriation.

Indeed, courts take a "flexible and imaginative approach to the problem of damages" in cases of trade secret misappropriation.[5] Even where damages are uncertain, that uncertainty does not preclude recovery because "the plaintiff should be afforded every opportunity to prove damages once misappropriation is shown."[6] That mandate of flexibility ensures that plaintiffs can recover when defendants misappropriate trade secrets instead of acquiring them legally as "the law is far more concerned with

5. Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518 (5th Cir. 1974).

6. *Id.* at 539.

the rights and interests of the aggrieved plaintiff than in the interests of the defendants which they would have tried to protect had they dealt openly with the plaintiff from the beginning."[7]

Accordingly, a number of courts have considered the EMVR in cases involving trade secrets. For example, in *Versata Software, Inc. v. Internet Brands, Inc.*,[8] a court in the Eastern District of Texas (Bryson, J., Fed. Cir., sitting by designation) addressed five post-trial motions, including a motion for remittitur.[9] The dispute concerned competitors who developed software for car manufacturers for use by shoppers to configure and compare different models.[10] The jury awarded $2,000,000 on counterclaims concerning trade secret misappropriations after determining that Versata misappropriated counterclaimant Autodata's trade secrets in applications that Versata provided to Toyota.[11] The damages award represented the full amount of Versata's profits from its projects related to Toyota.[12]

Versata argued that the jury's award was invalid because Autodata's "damages expert did not properly apportion the amount of Versata's profits that were directly attributable to the misappropriation." Versata asserted that Autodata was relying on the EMVR, questioned whether the EMVR was applicable to trade secret cases, and argued that even if the EMVR was applicable, Autodata's evidence was "not up to the task."[13] The court sidestepped the question of applicability, stating:

---

7. *Id.* at 544.
8. 902 F. Supp. 2d 841 (E.D. Tex. 2012).
9. *Id.* at 845.
10. *Id.*
11. *Id.* at 845, 851.
12. *Id.* at 855.
13. *Id.* at 855 n.3.

> In any event, all that is at issue here is whether the evidence supports the jury's finding that Autodata's trade secrets were of sufficient importance to Versata's work on the Toyota project that requiring Versata to disgorge all of its profits on the Toyota contracts is an appropriate remedy on the facts of this case.[14]

The court concluded that the evidence supported the verdict. Specifically, the court noted evidence that "one of Autodata's trade secrets . . . was incorporated into the vast majority of the software components sold by Versata"; "the basis for the demand for Versata's product was the . . . functionality enabled by the misappropriated [trade secret]"; and "the jury was entitled to conclude that the trade secrets were the basis for the core features of the products offered to Toyota and that Versata's profits on the Toyota contracts were therefore entirely attributable to the trade secrets."[15]

Although the district court's analysis is resonant with the EMVR, on appeal both parties asserted that the EMVR was inapplicable.[16] The Federal Circuit summarily affirmed, without comment, pursuant to Federal Circuit Rule 36.[17] Although the parties disclaimed the applicability of the EMVR to the facts of that case, Judge Bryson's query may be a useful formulation of the EMVR as applied to trade secret cases: Is the basis for the market demand for the infringing product the functionality enabled by the misappropriated trade secret?

---

14. *Id.*

15. *Id.* at 856–57.

16. (Fed. Cir. Nos. 13-1074, ECF No. 69 at 15, ECF No. 76 at 5 n.1).

17. 550 F. App'x 897 (Fed. Cir. 2014).

In a subsequent case, *Bianco v. Globus Medical, Inc.*,[18] Judge Bryson again addressed the EMVR while sitting by designation in the Eastern District of Texas. The plaintiff was a surgeon who alleged that Globus had misappropriated trade secrets concerning the design of continuously adjustable and reversible spacers for use in spinal surgeries.[19] The jury awarded $4.3 million in damages, "which was five percent of the profits that Globus earned on the products up to the original trial date."[20] The court also awarded an ongoing royalty of five percent of future sales for 15 years.[21] In evaluating the defendant's motion for a new trial on damages, Judge Bryson assumed, without deciding, that the EMVR was applicable to trade secret law, and he proceeded to reject the argument that the EMVR would preclude the jury's award, distinguishing *Bianco* from the "prototypical fact pattern in which the infringing feature in the accused product is a minor subcomponent of, or makes a minor contribution to, the overall product."[22] He explained:

> In this case, however, Dr. Bianco's trade secret was the idea for the adjustable interbody spacer itself. *Dr. Bianco's trade secrets did not relate to only a single subcomponent or feature* of the Caliber and Rise products; *instead, they related to the overall idea* for a continuously adjustable and reversible interbody spacer for use in fusion surgeries and included many of the key features disclosed in Dr. Bianco's drawings. Therefore, even assuming that the Federal Circuit's strict requirements for applying the

18. No. 2:12-cv-00147, 2014 WL 5462388 (E.D. Tex. Oct. 27, 2014).

19. *Id.* at *1–2.

20. *Id.* at *2.

21. *Id.*

22. *Id.* at *18.

> entire market value rule apply in this case under Texas trade secret law, Dr. Bianco met his burden of proof when he presented the jury with sufficient evidence to support his theory of trade secret misappropriation. In other words, the Caliber and Rise products are the "smallest salable units" that reflect the use of Dr. Bianco's trade secrets. . . . [T]he jury was entitled to find that the scope of the appropriation extended to the entire Caliber and Rise line of products, since what was alleged to have been appropriated was the idea for an adjustable interbody spacer and the combination of the basic features of such a spacer, which were incorporated in the Caliber and Rise devices. *In that setting, the entire market value rule does not require that the royalty base be apportioned among features of the device in question.*[23]

The court continued by recognizing an alternative rationale for the jury's conclusion: there was evidence that "[u]nlike in the Federal Circuit cases dealing with the entire market value rule, . . . Globus's regular practice was to grant royalties based on the net sales of its product."[24] Thus, the specific defendant's actual business practice of basing royalties on the net sales of the entire product may have outweighed the EMVR's general application. This alternative rationale may be generally applicable.

In another case, *MSC Software Corp. v. Altair Engineering, Inc.*,[25] after a jury determined that the defendants misappropriated three of the plaintiff's trade secrets for use in their software program, a special master, in advance of a new trial on damages,

---

23. *Id.* at *18–19 (emphasis added).

24. *Id.* at *19.

25. No. 07-12807, 2015 WL 13273227 (E.D. Mich. Nov. 9, 2015).

issued a report and recommendation concerning the defendant's *Daubert* motion regarding the testimony of the plaintiff's damages expert.[26] That expert based his analysis on "his estimate of the entire profit of [the software at issue] or the entire value of [that software]."[27] He did not "apportion the damages to the contribution made by [the] three trade secrets."[28]

The plaintiff sought to preserve the expert's testimony by arguing, among other things, that the EMVR "is not directly applicable to trade secret cases."[29] The special master, citing *University Computing*, noted that "[t]he requirement of apportionment, and the related Entire Market Value Rule (EMVR), are both established parts of the patent damages case law," such that it was appropriate to consider the EMVR in the trade secret context.[30] The special master analyzed the applicability of the EMVR to trade secrets cases as follows:

> [The plaintiff] contends that the EMVR requirement that the infringing component "drive the demand" for the entire product cannot ever literally apply to a trade secret case because, by its very nature, the trade secret is hidden from the customer. The hidden and unknown trade secret may not literally be what the customer demands, but in a credible EMVR case, the product's known functionality or physical property that is *enabled* by the

26. *Id.* at *1–2.

27. *Id.* at *6.

28. *Id.* at *2.

29. *Id.* at *12.

30. *Id.* at *14.

> hidden trade secret could very well be the basis of the customer's demand for the product.[31]

The special master also rejected the plaintiff's contention that the *Versata Software* court declined to apply the EMVR in that trade secrets case.[32] The special master concluded that the plaintiff had failed to show that its trade secrets enabled any identifiable feature that was the basis for customer demand.[33] Accordingly, he recommended that the court exclude the proffered damages opinion.[34]

B. Can Damages for Trade Secret Misappropriation Be Based on the Entire Value of the Misappropriating Company?

Where the entire value of a company stems from misappropriated trade secrets, it may be appropriate to consider the value a reasonably prudent investor would pay for the company when evaluating damages. Several courts have taken that approach.

For example, in *Wellogix, Inc. v. Accenture, L.L.P.*,[35] the plaintiff (Wellogix) had developed software to help oil companies

---

31. *Id.* at *15 (citation omitted).

32. *Id.* (quoting the *Versata Software* court's statement that "the basis for the demand for Versata's product was the . . . functionality enabled by the misappropriated [trade secret]").

33. *Id.* at *16.

34. *Id.* at *20. The court in *MSC Software* did not rule on the *Daubert* motion until 2017, after the parties engaged in extensive additional briefing, mainly under seal. The special master issued a Second Supplemental Report and Recommendation under seal in March 2017. ECF No. 1188. The court later granted the motion to exclude the damages expert's testimony in a sealed order. *See* ECF No. 1218 (referring to having granted the motion to exclude in ECF No. 1213, which is sealed). Because the order is under seal, it is not clear whether the court adopted the special master's analysis of the EMVR.

35. 716 F.3d 867 (5th Cir. 2013).

plan, procure, and pay for certain well-construction costs known as complex services.[36] Wellogix shared its source code subject to confidentiality agreements with two other companies (SAP and Accenture). When a Wellogix client sought to "implement global software that was not just for complex services, but was for its entire system," SAP and Accenture developed that software together, without notifying Wellogix, and used Wellogix's technology without permission.[37] Wellogix asserted claims for misappropriation of its trade secrets, and the jury awarded substantial damages.[38] The jury's award was based on an actual investment made in Wellogix and reflected the entire value of Wellogix, which the Fifth Circuit concluded was reasonable because the company's value derived entirely from the misappropriated technology.[39] The court specifically noted that the jury's award was based on testimony that "established the market value of the business immediately before and after the alleged misappropriation."[40]

Similarly, in *CardioVention, Inc. v. Medtronic, Inc.*,[41] the defendant argued that "there is no precedent for allowing a plaintiff in a trade secret misappropriation case to recover unjust enrichment damages constituting the entire business value of a company."[42] Yet the court allowed the expert to testify, noting that "[c]ourts have recognized that a plaintiff's actual damages can be measured by the value of the loss of the secret to the

36. *Id.* at 872.

37. *Id.* (internal quotation marks, omissions, and alterations omitted).

38. *Id.*

39. *Id.* at 879–80 & n.6.

40. *Id.* at 880.

41. 483 F. Supp. 2d 830 (D. Minn. 2007).

42. *Id.* at 845.

plaintiff under the circumstances" and determining that the entire value of the company was an accurate measure in that case.[43]

Indeed, in *DSC Communications Corp. v. Next Level Communications*,[44] Judge Paul Brown of the Eastern District of Texas observed that where a company has no marketable product and the assets of the company "consist almost exclusively" of misappropriated intellectual property, the price at which the misappropriating company was purchased "may be the least speculative measure" of damages:

> DSC has contended both before and during trial that the entire acquisition of Next Level by GI is relevant to show the amount of damages suffered by DSC. In fact, since neither party has yet to produce a product that is ready for sale to customers, *the purchase price of Next Level, whose assets consist almost exclusively of the ideas that DSC claims were stolen, may be the least speculative method of deriving the value of the alleged trade secrets.*[45]

The Fifth Circuit ultimately affirmed the jury's damages award for misappropriation based on "[t]he damages model DSC presented," that is, a damages model based on the entire market value of the misappropriating company.[46]

On the other hand, in some circumstances the entire market value of a misappropriating company may be an inappropriate measure of damages. For example, in *Alcatel USA, Inc. v. Cisco*

43. *Id.* at 845–46.

44. 929 F. Supp. 239 (E.D. Tex. 1996).

45. *Id.* at 246 (emphasis added).

46. DSC Commc'ns Corp. v. Next Level Commc'ns, 107 F.3d 322, 327–28 (5th Cir. 1997).

Systems, Inc.,[47] a plaintiff (Alcatel) sued Cisco, a company that had acquired another company (Monterey) that allegedly had stolen Alcatel's trade secrets prior to its acquisition by Cisco. Alcatel sought to measure its damages under theories of reasonable royalty and unjust enrichment by the price that Cisco had paid to acquire Monterey. Monterey's sole product was a network router that it had developed *prior to* any alleged misappropriation. Alcatel contended that Cisco would not have acquired Monterey but for Monterey's subsequent incorporation of Alcatel trade secrets into its router, on the theory that Monterey would not have been invited to compete on a critical bid without the benefit of those misappropriated trade secrets. The discovery record established, however, that numerous companies making competing routers had been invited to participate in that bid, and Alcatel's own expert could not say whether Monterey would have been invited to bid in the absence of misappropriation.[48] Given those facts, Judge Brown held that Alcatel could not establish its damages without providing any basis for segregating the value of its alleged trade secrets "from the rest of Monterey's cross-connect product or Wavelength Router technology," and he granted summary judgment against Alcatel "for lack of remedy."[49]

Based on these cases, it appears that the entire fair market value of a misappropriating company can be an acceptable measure of damages in appropriate circumstances, such as when the entire value of the company is based on a misappropriated trade secret.

47. 239 F. Supp. 2d 660 (E.D. Tex. 2002).

48. *Id.* at 669.

49. *Id.* at 671, 673.

III. DURATION OF "HEAD START" UNJUST ENRICHMENT DAMAGES

The duration of unjust enrichment damages in trade secret cases is relatively straightforward, at least until a court gets to the issue of deciding the issue of a "head start" period.

The general rule is that the accounting of unjust enrichment damages commences at the moment that use of the misappropriated trade secret confers a benefit on the defendant.[50] Damages then accrue until such time, if ever, that the defendant would have acquired knowledge of the trade secret through legitimate means, such as public disclosure, reverse engineering, or independent development.[51]

In certain cases, a misappropriator tries to limit the duration of unjust enrichment based on the head start doctrine. Under this doctrine, unjust enrichment damages are limited to a head start period when a misappropriator can show that it would have acquired knowledge of the trade secret through legitimate means.[52] This period is defined as the time between the date a misappropriator began benefiting from misuse of a trade secret

50. LOUIS ALTMAN & MALLA POLLACK, CALLMANN ON UNFAIR COMP., TR. & MONO. § 14:42 (4th Ed.); NuCar Consulting, Inc. v. Doyle, 2005 WL 820706, at *13 (Del. Ch. Apr. 5, 2005), *aff'd*, 913 A.2d 569 (Del. 2006).

51. *See, e.g.*, RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 (1995); 92 A.L.R.3d 138 (collecting cases); Med. Store, Inc. v. AIG Claim Servs., Inc., No. 02-80513-CIV, 2003 WL 25669175, at *5 (S.D. Fla. Oct. 17, 2003) (citing RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 (1995); Specialized Tech. Res., Inc. v. JPS Elastomerics Corp., 80 Mass. App. Ct. 841, 849 (2011) (affirming disgorgement of all of defendant's net profits when defendant "would not have been able to develop [the trade secret method] independently").

52. LOUIS ALTMAN & MALLA POLLACK, CALLMANN ON UNFAIR COMP., TR. & MONO. § 14:42 (4th Ed.); Russo v. Ballard Med. Prods., 550 F.3d 1004, 1020 (10th Cir. 2008).

and the date the misappropriator would have gained knowledge of the trade secret through legitimate means.

The complication of the head start doctrine is in its application. Courts take different approaches in calculating the head start period, and it is usually the subject of competing expert testimony about what would theoretically happen in a world in which the misappropriator did not misappropriate but instead acquired the trade secret through legitimate means. Below are examples of how various courts have addressed this doctrine:

- In *Agilent Technologies, Inc. v. Kirkland*, the defendant misappropriated trade secrets for developing liquid chromatography columns.[53] In determining that defendant's misappropriation gave it a three-year head start, the court considered expert testimony by both parties. The court also considered that it took plaintiff, and a third-party competitor, three years to develop their analogous products.[54]
- In *NuCar Consulting, Inc.*, the defendant misappropriated the plaintiff's automotive dealers client list and created a new company to compete with the plaintiff.[55] In a bench trial, the court concluded that had the defendant not misappropriated this trade secret, he would have developed a comparable client list within

53. C.A. No. 3512-VCS, 2010 WL 610725, at *1 (Del. Ch. Feb. 18, 2010).

54. *Id.* at *26; *see also* Robin Singh Educ. Servs., Inc. v. Blueprint Test Preparation, LLC, No. B204775, 2013 WL 240273, at *33 (Cal. Ct. App. Jan. 23, 2013), *as modified on denial of reh'g* (Feb. 20, 2013) (using competing expert testimony to determine "head start" period, in which the defendant's expert developed his opinion by comparing its development time to plaintiff's own development time).

55. *See* NuCar Consulting, Inc. v. Doyle, No. Civ.A. 19756-NC, 2005 WL 820706, at *13 (Del. Ch. Apr. 5, 2005).

two years. In reaching this conclusion, the court considered the facts that the defendant purchased contact information from various automotive dealers, sent out promotional mailers, and "could have engaged in other activities" to grow the client list. The court did not consider expert testimony nor mention how long it took for the plaintiff to develop its client list.

- In *Johns Manville Corp.*, the defendant argued on summary judgment that damages for misappropriation of a trade secret used in a spinner alloy should be limited to a head start period of 39 months.[56] The defendant arrived at this number because plaintiff's 30(b)(6) witness "opined" in deposition that creating an analogous spinner alloy from scratch would take 40–52 months. Then defendant argued that 12 of these months are merely inventory build-up and that another month was allotted to selecting a spinner alloy recipe that instead could be taken from the public domain. The court found there were "many unknowns in this computation" and denied the motion.

Courts occasionally decide not to apply a head start limitation, even if it is otherwise applicable. In *RRK Holding Co.*, the court upheld a jury award beyond the head start period simply because it found that Illinois case law, though requiring a head start limitation for injunctive relief, did not require such a limitation for damages.[57] Further, after the *Agilent* court determined the appropriate head start period, discussed above, it concluded that "Agilent is entitled to damages beyond the three year head

56. *See* Johns Manville Corp. v. Knauf Insulation, LLC, 2017 WL 4333621, at *8–10 (D. Colo. Sept. 22, 2017).

57. RRK Holding Co. v. Sears, Roebuck & Co., 563 F. Supp. 2d 832, 836 (N.D. Ill. 2008).

start period."[58] The court found that defendant would continue to enjoy an increased market share from its misappropriation and thus it was "equitable" to award more damages.

Courts view calculations of the head start as a fact question for the jury to resolve. In *Premier Lab Supply*, for example, the judge gave a jury instruction titled "Accounting Period," which "instructed the jury that, with respect to calculating the amount of unjust enrichment, the jury should award damages only for the period of time the trade secret remained a trade secret."[59] The jury considered evidence that certain technology incorporating the trade secret was "widely available" but nonetheless awarded damages that were not limited by the defendant's proffered head start period. The defendant appealed, arguing the judge erred in refusing to give the jury further guidance on how to determine the duration of head start damages. The appellate court affirmed the jury award, finding that it was the "domain of the finder of fact" to determine the appropriate time period.

Ultimately, the application of unjust enrichment damages is a fact-intensive inquiry. The fact-finder must determine if the misappropriator would have ever discovered the trade secret through legitimate means. If so, the fact-finder must determine the period of time the misappropriator enjoyed a head start through its misappropriation, including through expert testimony and comparison to plaintiff's own production time.

Another factor to consider in analyzing a head start damages period is the methodology used to calculate the defendant's profits during the assumed head start period. There are at least two approaches that can be used to quantify the defendant's

58. *Agilent Techs., Inc.*, 2010 WL 610725, at *27.

59. Premier Lab Supply, Inc. v. Chemplex Indus., Inc., 94 So. 3d 640, 643 (Fla. Dist. Ct. App. 2012).

profits during a head start period: (1) profits acceleration approach, and (2) incremental profits approach.

The profits acceleration approach is premised on the assumption that, as a result of the defendant's use of the trade secrets, it was able to accelerate its generation of sales and profits that it otherwise would have generated in a later time period if it had not used the trade secrets. The analysis consists of a comparison between the present value of the defendant's profits attributable to the trade secret and the present value of the defendant's profits, if any, that were expected if the defendant had not used the trade secrets. From an economic perspective, the present value calculations can be performed as of the date of the alleged misappropriation. The difference between these two amounts is the defendant's head start advantage in the form of profits acceleration. It is essentially a time value of money benefit obtained through unauthorized use of the trade secrets.

The profits acceleration approach may be considered in situations where customers would have delayed their purchases of the defendant's products if the trade secrets had not been misappropriated. For example, consider a scenario where installation of new manufacturing equipment embodying a trade secret results in a significant cost reduction associated with a manufacturing process. A manufacturer may decide to replace its existing equipment with new equipment containing the trade secret if it expects to obtain cost reductions from doing so. However, if the manufacturer does not have the opportunity to purchase equipment with the trade secret, it would make do with its existing equipment. Thus, the trade secrets would result in the defendant's ability to generate sales and profits that would not have been made during the head start period, but for the defendant's misappropriation of the trade secrets. But if the defendant had lawfully developed the trade secret, or equiva-

lent information, on its own during the avoided head start period, the defendant still could have, arguably, made the same sales to the same customers, but at a later date. Therefore, the profits acceleration approach focuses primarily on the timing of sales made by the defendant, thereby suggesting present valuation calculations of the defendant's profits with and without the benefit of its misappropriation.

The incremental profits approach focuses more closely on the sales and profits made by the defendant during the head start period. The notion behind the incremental profits approach is that if the defendant had not misappropriated the trade secrets, it may have missed a unique opportunity to sell products or services incorporating the trade secrets during the head start period.

The incremental profits approach may be considered in situations where there is an existing market for products or services incorporating the trade secrets and there are competitors in the market. It may also be considered if the defendant's customers would not have delayed their purchases absent the incorporation of the trade secrets into the defendant's products. For example, consider a scenario where there are multiple suppliers of a chemical feedstock used in a continuous manufacturing process. One of the suppliers is the defendant, which differentiates itself by selling feedstock incorporating the trade secrets. Manufacturers would not delay their purchases of feedstock to obtain the benefits of the trade secrets at a later date because that would disrupt their continuous manufacturing process. Instead, they would buy feedstock from one of the defendant's competitors, thereby precluding the defendant from making those specific sales during the head start period. In this scenario, one may consider a calculation of the defendant's incremental profits attributable to the trade secrets during the head start period, as opposed to the profits acceleration approach.

The selection of a methodology to use when calculating the defendant's profits based on the head start advantage is a fact-specific exercise that depends not only on the market dynamics in play during the head start period, but also the availability of relevant financial information before, during, and after the head start period.

IV. BURDEN SHIFTING IN DETERMINING DEFENDANTS' PROFITS IN UNJUST ENRICHMENT DAMAGES

The burden of proving unjust enrichment in trade secrets litigation can be daunting due to the inherent difficulties in valuing trade secrets themselves and in evaluating the market channels in which the allegedly misappropriated trade secret has been employed. An expert is essentially mandatory.[60] And, as already noted in Sections II and III, significant issues remain regarding whether a plaintiff can rely upon the EMVR when seeking unjust enrichment damages, and whether it is necessary or appropriate to apportion such damages or employ the head start rule.

Nonetheless, history has shown that a plaintiff, upon proving both misappropriation of trade secrets and unjust enrichment, may be entitled to a very significant recovery as exemplified by the previously discussed cases in Section II.B.[61] That is

60. *See, e.g.*, Trident Prods. & Servs., LLC v. Canadian Soiless Wholesale, Ltd., 859 F. Supp. 2d 771 (E.D. Va. 2012) (granting summary judgment to defendant on claims for misappropriation of trade secrets and unjust enrichment where the plaintiff failed to proffer expert testimony, noting that "[t]he defendant . . . bears no burden on proving the role of the trade secret in a new product").

61. For instance, in *E. I. du Pont de Nemours and Company v. Kolon Industries Inc. et al.*, Case No. 3:09-cv-00058 (E.D. Va.), a jury in the Eastern District of Virginia found that Kolon Industries, a South Korean entity, stole trade secrets related to the production and marketing of Kevlar bulletproof vests from DuPont, and awarded damages in the amount of $919.9 million. After

because unjust enrichment can include more than the defendant's increased profits derived from its use of a misappropriated trade secret. In many courts, unjust enrichment can also include any "avoided costs," such as a defendant's increased savings related to its avoiding development of its own technology.[62] These savings may reflect research and development (R&D) that the defendant avoided, as well as the shortened time to production that the defendant experienced as a result of misappropriating the trade secret. Unjust enrichment may also include any increased business value to defendant that is attributable to the misappropriation, such as the company's potentially lucrative (though difficult to quantify) "first mover advantage" achieved by acceleration of its product or business to market before that of any other competitor (including the plaintiff).[63] As the Fifth

---

the Fourth Circuit reversed the damages finding due to the improper exclusion of evidence, the parties settled for $275 million in restitution as a part of a larger agreement in which Kolon also paid $85 million to the U.S. Government in fines. Similarly, in *Lexar Media, Inc. v. Toshiba Corp.*, CV-812458 (Cal. Super. Ct., Santa Clara County, March 2005), a California jury awarded the plaintiff $465.4 million in damages upon a finding of trade secret misappropriation. After the trial court ordered a new trial on damages, the parties settled for $288 million.

62. Not all courts permit recovery of avoided costs in trade secrets cases. *See* E.J. Brooks Co. v. Cambridge Security Seals, 2018 N.Y. LEXIS 1080 (N.Y. Ct. App. May 3, 2018) (responding to certified question from the U.S. Court of Appeals for the Second Circuit, and holding that, in New York, a plaintiff in a trade secrets case cannot recover damages that are measured by the costs the defendant avoided due to its unlawful activity).

63. *See*, *e.g.*, Bourns, Inc. v. Raychem Corp., 331 F.3d 704 (9th Cir. 2003); Ajaxo, Inc. v. E*Trade Fin. Corp., 187 Cal. App. 4th 1295 (2010); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 cmt. f (1995) ("[i]f the benefit derived by the defendant consists primarily of cost savings, such as when the trade secret is a more efficient method of production, the 'standard of comparison' measure that determines relief based on the savings achieved through the use of the trade secret may be the most appropriate measure of relief").

Circuit observed in *University Computing Co. v. Lykes-Youngstown Corp.*,[64] when it characterized "the appropriate measure of damages" for unjust enrichment in trade secret cases to be analogous to remedies available in patent infringement actions, the relevant measure of harm is "not what [the] plaintiff lost, but rather the benefits, profits, or advantages gained by the defendant in the use of the trade secret." Not surprisingly, therefore, unjust enrichment is rapidly becoming a popular recovery tool in situations in which the plaintiff claims that the defendant's use of the trade secret inherently is responsible for the underlying value assigned to a company's net worth, such as when a start-up company obtains significant capital investment shortly after introducing a technology alleged to be predicated upon misappropriated trade secrets.[65]

Unjust enrichment is a case and fact-specific remedy available in jurisdictions that employ variations of the UTSA,[66] in states like New York and Massachusetts[67] in which trade secrets litigation is premised on the common law, and under the newly enacted DTSA.[68] Typically, unjust enrichment, as opposed to a calculation of lost profits, is used as a remedy for trade secret misappropriation in all of these legal systems only when there

64. 504 F.2d 518 (5th Cir. 1974).

65. That is not to say that such a theory will be successful, however. *Cf.* Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA (N.D. Cal. Nov. 2, 2017) (Order under seal) (excluding plaintiff's expert who alleged he calculated trade secret misappropriation damages in the amount of $1.86 billion from the acquisition by defendant Uber of a company that employed plaintiff's former engineer by simply looking at Uber's own estimate of how valuable the technology was to Uber at the time of acquisition).

66. Uniform Trade Secrets Act § 3(a) (amended 1985), 14 U.L.A. 384 (2005).

67. *See, e.g.*, Softel, Inc. v. Dragon Med. & Sci. Commc'ns, 891 F. Supp. 935 (S.D.N.Y. 1995); Incase Inc. v. Timex Corp., 488 F.3d 46 (1st Cir. 2007).

68. 18 U.S.C. § 836(b)(3)(B)(i).

are no provable profits earned by the defendant, such as when the plaintiff itself is a start-up and has not ramped up production.[69] Unjust enrichment can also be employed when additional losses beyond lost profits are proven, as well as in situations involving convoyed sales of products tainted by the misappropriation (*see infra*, Section VI).[70] However, a plaintiff can never recover both lost profits and unjust enrichment if to do so will result in double recovery for the same harm (*see infra*, Section V).[71]

A plaintiff seeking unjust enrichment damages will have the burden of proving the defendant's net profits gained from actions like those attributable to accelerated time to market and avoided costs that are proximately caused by the misappropriation of the plaintiff's trade secrets.[72] A common mechanism

---

69. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 cmt. f (1995) ("[i]f the benefit derived by the defendant consists primarily of cost savings, such as when the trade secret is a more efficient method of production, the 'standard of comparison' measure that determines relief based on the savings achieved through the use of the trade secret may be the most appropriate measure of relief").

70. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 cmt. f (1995) ("profits on the sale of consumable supplies used in a machine embodying the trade secret or profits on spare parts and service may be included in the accounting to the extent that such profits were made possible by the defendant's sale of the original product").

71. *See* comments to Uniform Trade Secrets Act § 3 (amended 1985), 14 U.L.A. 384 (2005).

72. *See, e.g.*, MicroStrategy, Inc. v. Li, 268 Va. 249 (2004) (the proponent "must bear the burden of proving a trade-secret claim," and "[t]his burden does not shift, even when a plaintiff has presented a prima facie case"); Microstrategy, Inc. v. Bus. Objects, S.A., 429 F.3d 1344 (Fed. Cir. 2005) (affirming the district court's grant of partial summary judgment on damages in favor of defendant on the grounds that plaintiff did not show the amount of damages "sustained with reasonable certainty" or "a causal connection between the damages it suffered and the actions of" defendant); Do It Best Corp. v.

used to calculate unjust enrichment is an accounting of the defendant's actual profits earned by using the misappropriated trade secrets.[73] As with largely identical calculations directed to determining lost profits, a defendant's profits achieved through unjust enrichment are typically measured by determining the number of additional sales that the plaintiff would have made if the defendant had not acted improperly, coupled with the plaintiff's incremental profits on these sales.[74] These incremental profits may consist of the revenue that the plaintiff would have made on the additional sales, subtracting any incremental costs that the court or jury concludes the plaintiff would necessarily have incurred while making those same sales.[75]

The defendant bears its own burdens in the unjust enrichment calculation too. In determining the defendant's net prof-

---

Passport Software, Inc., No. 01-C-7674, 2005 WL 743083, at *16 (N.D. Ill. Mar. 31, 2005) ("[Plaintiff] offers numerous facts that purportedly establish a violation of ITSA, but there is nothing to tie that alleged violation to [Defendant's] provision of maintenance services to its members.").

73. *See*, *e.g.*, Reingold v. Swiftships, Inc., 210 F.3d 320 (5th Cir. 2000); Softel Inc. v. Dragon Med. & Sci. Commc'ns, Inc., 118 F.3d 955 (2d Cir. 1997).

74. *See*, *e.g.*, ADA Motors, Inc. v. Butler, No. 70047–2–I, 183 Wash. App. 1002 (Wash. Ct. App. Aug. 18, 2014) (unpub.) (holding that the jury instructions incorrectly stated the law because Ada Motors' initial burden was only to prove there were sales attributable to the use of a trade secret, but the instructions further required "damages from sales" to prove unjust enrichment, which was incorrect since the plaintiff did not need to prove anything beyond "sales" to meet its initial burden); RRK Holding Co. v. Sears, Roebuck & Co., 563 F. Supp. 2d 832 (N.D. Ill. 2008) (noting that the "unjust enrichment portion of damages is calculated by subtracting the Plaintiff's loss amount from Defendant's total gain").

75. *See generally* John E. Elmore, *A Quantitative Analysis of Damages in Trade Secrets Litigation*, INSIGHTS, Spring 2016, at 79-94, *available at* http://www.willamette.com/insights_journal/16/spring_2016_11.pdf.

its, the court also may consider various setoffs that the defendant establishes which then lower the expected recovery.[76] For instance, the court may exclude from recovery any research and development expenses the defendant proves it incurred independently from its use of the trade secret, any gross receipts that the defendant establishes reflect its actual costs of production, the salaries and labor expenses the defendant can show would have been paid by the company notwithstanding the misappropriation, any advertising and marketing expenses the defendant demonstrates were inevitable notwithstanding the misappropriation, and similar expenses that the defendant establishes are unrelated to or incurred by the company notwithstanding the misappropriation.[77]

With these basic principles in mind, a highly over-simplified hypothetical may be helpful to understand how the unjust enrichment calculation is rendered in a scenario where some lost profits can also be determined, and where defendant can prove it is entitled to setoffs. Assume that a defendant corporation with hundreds of millions of dollars in capital acquires a recently incorporated start-up whose employees have misappropriated key trade secrets related to Widget A from their former employer. As a result of the acquisition, further assume that the defendant is able to enter the product market for Widgets by a full year earlier than it otherwise would have been able to do so.

---

76. *See* Annotation, *Proper Measure and Elements of Damages for Misappropriation of Trade Secrets*, 11 A.L.R.4th 12 (1982); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 cmt. f (1995) ("[t]he plaintiff has the burden of establishing the defendant's sales; the defendant has the burden of establishing any portion of the sales not attributable to the trade secret and any expenses to be deducted in determining net profits").

77. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 cmt. f (1995) ("[t]he rules governing the deductibility of expenses and the allocation of overhead are analogous to those stated in § 37, Comments g and h, on accountings in actions for trademark infringement").

This entry to market not only causes the plaintiff to lose revenues of $50 million as a result of a reduction in sales of its own Widgets, but it also causes the plaintiff to expend $10 million more in marketing. However, the loss of market share also saves the plaintiff $5 million in incremental costs. The combination of $50 million in lost sales and $10 million in additional advertising results in compensable damages to plaintiff of $60 million. That amount must then have the incremental savings the company achieved of $5 million in costs subtracted from it, for a total of $55 million. However, assume further that the defendant's first mover advantage allows it to achieve $100 million in sales in year one after the acquisition of the start-up that employed the individuals who misappropriated plaintiff's trade secrets, and further that during this time it saved $50 million in R&D costs. Nonetheless, of those $50 million in R&D savings, $10 million were attributable to independent development of concepts ultimately implemented in the Widget sold by defendant.

Here, to avoid any double recovery on the amount of lost profits that plaintiff suffered that is reflected equally in the amount that defendant gained, the total amount of lost profits that plaintiff would be entitled to recover is $90 million (its own losses of $45 million, plus an additional $45 million of the defendant's own $100 million in profits from year one). Defendant thus does not have to pay plaintiff $55 million of the $100 million in sales it produced in year one. However, plaintiff would also be entitled to recover as additional unjust enrichment damages the $10 million in marketing expenses it incurred, and the $50 million in savings to defendant in R&D and other costs. So, plaintiff would be entitled in this admittedly simplistic scenario to a total award of $150 million. Defendant would then be able to set off $10 million from that amount due to its independent contributions to R&D, so that plaintiff presumably could recover "only" $140 million.

However, this hypothetical does not tell the whole story about how unjust enrichment calculations would actually have to be proven, or what other issues are buried in the calculations as a result of the burdens that the parties carry at trial. For instance, all courts require that unjust enrichment damages must not be speculative, and hence the plaintiff must establish these damages with reasonable certainty.[78] In situations in which the plaintiff seeks recovery for the increased value that a company has achieved as a result of investment after an alleged misappropriation, it may be highly speculative for the plaintiff to claim that increased value was a product of defendant's use of its trade secrets, as opposed to independent venture capital enthusiasm generated from other aspects of the defendant's marketing and introduction of a particular technology. In the hypothetical above, a similar issue may prevent the plaintiff from establishing without speculation what amount of additional unjust enrichment profits the defendant achieves as a result of its first mover advantage *after* year one, or for how long that advantage will last and be subject to recovery. Indeed, that problem arguably is what often incentivizes plaintiffs to claim as unjust enrichment damages virtually all of the value of a start-up which is alleged to have misappropriated plaintiff's trade secrets prior to its receiving significant capitalization. Yet, such a claim is fraught with danger since investor capitalization can be attributable to any number of independent factors, such as the potential of the start-up to independently develop its own intellectual property.

78. *See* Microstrategy, Inc. v. Bus. Objects, S.A., 429 F.3d 1344 (Fed. Cir. 2005) (affirming the district court's grant of partial summary judgment on damages in favor of defendant on the grounds that plaintiff did not show the amount of damages "sustained with reasonable certainty" or "a causal connection between the damages it suffered and the actions of" defendant).

Further complicating the unjust enrichment calculation is the fact that the plaintiff carries the burdens of proving the existence of a legally protectable trade secret and a nexus between the misappropriation of that trade secret and the profits associated with the defendant's unlawful gain.[79] Needless to say, the requirement of establishing the relevant nexus between the perceived value of what is often an intangible asset and the profits a defendant achieved in introducing its own products or services allegedly incorporating that asset can be challenging for a plaintiff. For instance, in *Vermont Microsystems, Inc. v. Autodesk, Inc.*,[80] in a case in which the plaintiff alleged misappropriation of trade secrets related to its software product, the court of appeals affirmed a magistrate judge's finding that the evidence

79. ClearOne Commc'ns v. Chang, No. 09-4128, 2011 WL 3468215 (10th Cir. Aug. 9, 2011) (slip op.) (upholding the denial of prejudgment interest to a plaintiff awarded unjust enrichment damages, finding that there was no definite and ascertainable sum of money to define the unjust enrichment; the court reasoned that the unjust enrichment only approximated the value of the benefits the defendants gained from misappropriating plaintiff's trade secrets, and the plaintiff's expert calculated unjust enrichment by calculating the defendants' profits, but the relevant benefits could have been determined in numerous ways, and not all of the defendants' profits may have been attributable to the misappropriation of trade secrets); Jet Spray Cooler v. Compton, 377 Mass. 159 (1979) (Court holds that it "cannot determine whether the plaintiffs' lost profits in this action were "due to" the defendants' sales of products utilizing the trade secrets, or whether the plaintiffs' lost profits were "due to" the plaintiffs' own business decision to refrain from marketing products containing the information in the report," and therefore the plaintiffs failed to prove "their lost profits 'due to' the defendants' sales to the plaintiffs' customers with sufficient certainty to allow the plaintiffs to recover damages based on lost profits."); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 45 cmt. B; RESTATEMENT (SECOND) OF TORTS § 912; MicroStrategy, Inc. v. Li, 268 Va. 249 (2004); Katskee Nev. Bob's Golf of Neb., Inc., 472 N.W.2d 372 (Neb. 1991); Midland Hotel Corp. v. Rueben H. Donnelley Corp., 515 N.E.2d 61 (Ill. 1987).

80. 138 F.3d 449 (2d Cir. 1998).

that had been presented before him was "too imprecise and speculative as well as based on opinion and survey results which rely on assumptions and hypotheticals" to permit the trier-of-fact to determine the amount of unjust enrichment that plaintiff argued the defendant should disgorge. In that situation, the court of appeals agreed with the magistrate judge that the doctrine of "reasonable royalty" should instead be applied, greatly reducing the plaintiff's proposed recovery. Similarly, in *02 Micro Int'l, Ltd. v. Monolithic Power Systems*,[81] the jury found that the plaintiff, which was seeking recovery based on unjust enrichment, was entitled to recover for just one of eleven allegedly misappropriated secrets. Since the court found, based on the record, that there was no reasonable basis upon which the jury could have determined the portion of the defendant's alleged unjust enrichment that was attributable to only one secret, it concluded that unjust enrichment was not provable as a matter of law. Because neither unjust enrichment nor damages had been proven, the trial court granted the plaintiff's request in the alternative for a reasonable royalty.

As these cases reflect, the burdens associated with proving unjust enrichment are inherently tied to the plaintiff's critical decision to identify what information it contends are its trade secrets and, equally importantly, how that information is alleged to have benefited the defendant. As any attorney who has litigated a trade secret knows, these are not easy tasks, since the burden will always remain with plaintiff to prove the confidentiality and value of its trade secrets, while normally being prevented outside discovery from knowing how the defendant potentially is using that valuable intellectual property. Further, virtually all the information about how a defendant has profited will be in the control of the defendant, and an error in judgment

81. 399 F. Supp. 2d 1064 (N.D. Cal. 2005).

by the plaintiff about how the trade secret has been employed in defendant's marketing channels can have a significant impact upon its damages calculations. These issues are further complicated by the fact that some courts may further require the plaintiff to apportion the damages it attributes to trade secret misappropriation (*see supra* Section II).[82]

Defendants to trade secret actions also face complicated tactical decisions due to the burdens of proof. For instance, as discussed in Section III, *supra*, in the discussion of "head start," depending upon the court in which the plaintiff is seeking recovery, the defendant may carry the burden of proving when any accounting period for the defendant's lost profits terminated as a result of the trade secret becoming public information. That, of course, requires the defendant to deconstruct its own R&D process, which can easily expose how the defendant has profited in the period that the plaintiff alleges misappropriation has occurred, providing plaintiff with the very proof it needs to establish entitlement to recovery of unjust enrichment. Further, in some jurisdictions, the calculation of unjust enrichment damages may necessitate a bench trial, as opposed to the use of a jury.[83] As long as there remains significant room for further development of these concepts, or divisions of opinion about their applicability, they will continue to warrant careful consideration by plaintiffs and defendants alike.

---

82. *E.g.*, Goldberg v. Medtronic, Inc., 686 F.2d 1219 (7th Cir. 1982) (awarding plaintiff, as damages for trade secret misappropriation, 10% of the profits of electrical leads, where the court concluded plaintiff's confidential disclosures contributed 10% to the development of those leads).

83. *See* Texas Advanced Optoelectronic Solutions, Inc. v. Renesas Electronics America, Inc., Nos. 2016-2021, -2208, 2235 (Fed. Cir. May 1, 2018) (holding that any disgorgement award in a trade secrets case under Texas law lies in equity, and requires a Bench trial rather than a calculation by a jury).

V. RIGOROUS ESTIMATION OF UNJUST ENRICHMENT AND LOST PROFITS

We start with a relatively simple trade secrets damages scenario. We assume that the benefits of trade secret misappropriation contain two elements: (1) savings on the costs of R&D and (2) early entry into the market which results in sales that would not otherwise have been made by the misappropriator.[84]

The expected profit from selling a new product or service when there is no trade secret misappropriation is:

$$\pi_0 = PV((P_t - MC) \times Q_t^0) - PV(RD_0) - I_0$$

Where $PV(\ )$ indicates a present value calculation, P_t is the expected price in year t, Q_t^0 is the expected quantity sold in year t when there is no misappropriation, RD_0 is the research and development costs incurred to develop the infringer's product without misappropriation, and I_0 is the investment in manufacturing facilities to make that product. MC is the costs of goods sold incurred in making the product.

The expected profit when there is misappropriation is:

$$\pi_M = PV((P_t - MC) \times Q_t^M) - PV(RD_M) - I_M$$

Q_t^M is the expected quantity sold in year t when there is misappropriation, RD_M is the research and development costs incurred to develop the product that embodies the misappropriated trade secrets, and I_M is the investment in manufacturing facilities to make the product that embodies the trade secrets.

84. It can be just as general to assume that trade secrets misappropriation results in increased incremental profit or total profit through lowering production cost. Lowering production costs either increases incremental profit or keeps incremental profit the same with lower prices, resulting in larger market share and increased total sales.

Annual profits with misappropriation and profits without misappropriation are depicted in Figure 1.

For simplicity, we can assume that there is no difference between the misappropriation case and the no-misappropriation case in investment spending, in prices, and in marginal costs. We assume that research and development costs are lower in the misappropriation situation than the no-misappropriation situation, that is $RD_M < RD_0$.

The gains from misappropriation are simply:

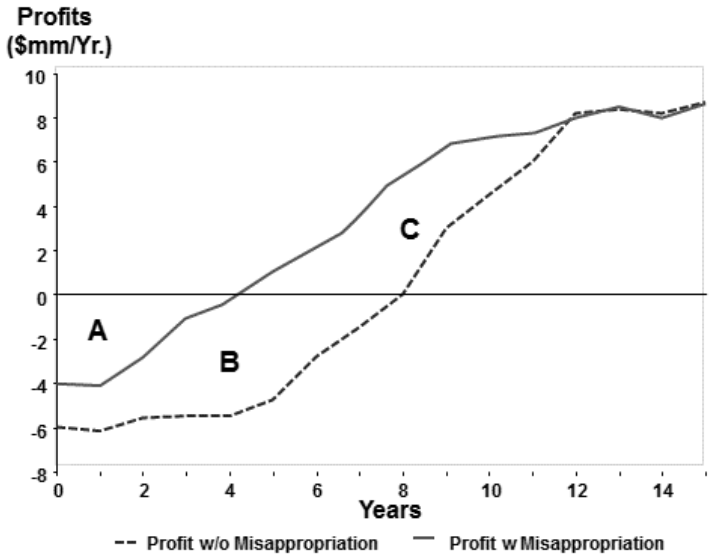
$$\Delta = \pi_M - \pi_0$$

$$\Delta = PV((P_t - MC) \times (Q_t^M - Q_t^0)) + PV(RD_0 - RD_M)$$

This is the amount of unjust enrichment that results from misappropriation. The term on the left side of the plus sign represents the benefit of the head start, including both the plaintiff's lost profits and unjust enrichment from sales taken from other market participants. The term on the right side represents the benefits of reduced research and development costs due to misappropriation.

Figure 1 provides a general depiction of the scenario, displaying these two terms. The area labeled B represents the savings in R&D costs, and the area labeled C represents profits from the additional sales made due to the head start. This depiction does not adjust lost profits for price erosion or differences in manufacturing costs between plaintiff and defendant, a matter we discuss below.

Figure 1. Gross Profits and Investment Costs



RD_0, defendant's research and development expenditure had it not misappropriated, cannot be observed. Plaintiffs' costs of developing the trade secrets at issue might provide a reasonable estimate of RD_0, though they often must be calculated.

So far, we have not accounted for the different sources of lost profits. Some part of the amount $(Q_t^M - Q_t^0)$ in the first term in the formula for Δ are the defendant's profits resulting from sales being diverted from the owner of the trade secrets, (lost profits). The rest are profits that arise from sales that would have been made by other market participants. If the defendant's production costs are different from those of the plaintiff, it is generally necessary to separate these two sets of sales. Sales that result in lost profits may be determined in a variety of ways, including the market share approach.[85] Defendant's sales that would have

85. Agilent Techs. v. Kirkland, C.A. No. 3512-VCS, 2010 WL 610725, at *28 (Del. Ch. Feb. 18, 2010). (The "method of determining lost profits based on a

been made by the defendant are then subtracted from the additional sales made due to the head start. Other issues that may need to be accounted for include the possibility that entrance of the misappropriator may cause price erosion.[86] Finally, entrance of the misappropriator may increase plaintiff's costs.

One immediate conclusion that can be drawn from even this simple model is that calculating damages merely on the basis of getting to market earlier understates the full extent of the unjust enrichment. The misappropriator also benefits from reduced expenditure on R&D. In *Agilent*, however, the court made no damage award related to defendant's saved R&D costs, notwithstanding that it had found clear evidence of such savings.[87]

This simple formula for unjust enrichment also makes it very clear that damages could be greater than the entire value of the defendant company. This would be the case, for example, if a company sells only product made with the misappropriated technology and if both unjust enrichment and saved R&D costs are awarded. If the plaintiff can show that, absent the misappropriation, the defendant could not have entered the plaintiff's market and would not have made any sales, then the first term in the formula above becomes merely $PV((P_t - MC) \times Q_t^M)$. This is the present value of all future gross profits earned using misappropriated trade secrets which should approximate the defendant company's market value.[88] The damages award could

market share is an acceptable approach [for] demonstrating the causal relationship between misappropriation and lost profits.").

86. Roton Barrier, Inc. v. Stanley Works, 79 F.3d 1112, 1119–20 (Fed. Cir. 1996) (holding that losses included price reductions necessary to compete with misappropriator until the plaintiff could restore prior pricing).

87. *Agilent*, 2010 WL 610725, at *28.

88. A more realistic accounting would take into account the present value of future capital and other expenditures that the misappropriator would need to make in order to remain in business.

be greater than the market value if saved R&D costs are also awarded.

USA Power Corp., LLC v. PacifiCorp[89] provides an example of an award of all the profits from an investment that incorporated misappropriated trade secrets. The defendant was accused of misappropriating financial data and other trade secrets on an electric generation project. Both defendant and plaintiff later submitted bids for the right to build a project to supply electricity. The misappropriated trade secrets allowed the defendant to submit the winning bid to build a technically very similar project at a different location. The Supreme Court of Utah sustained an award that disgorged all profits over the plant's thirty-year life because the jury could have reasonably concluded "that all of [defendant's] profits were the result of misappropriation." Had the court also awarded saved R&D costs, the award would have been greater than the value of the project.

The formula can be used to examine the reasonableness of using plaintiff's entire expenditure on R&D on the relevant product as an estimate of unjust enrichment. This was, for instance, what was done in the *Kevlar* case, where the original damages award of nearly $1 billion was based on DuPont's cost of developing Kevlar.[90] It appears that this is not a generally accurate derivation of unjust enrichment under the assumptions used in deriving the formula. It can only be an accurate measure of unjust enrichment if three conditions are met. First, the defendant must have incurred no R&D costs, (that is, $RD_M = 0$). Second, the defendant's R&D costs had it not misappropriated (RD_0) would have been the same as plaintiff's. Finally, there was

89. USA Power, LLC v. PacifiCorp, 372 P.3d 629 (Utah 2016).

90. Redacted Final Brief of Appellee E.I. Du Pont de Nemours and Company, E.I. du Pont de Nemours and Company v. Kolon Industries, Inc., No. 12-1260 (4th Cir. Feb. 22, 2013), *available at* http://s3.amazonaws.com/cdn.orrick.com/files/Trade-Secret-Blog-Jun5-Attachment-H-DuPont-brief.pdf.

no head start due to the misappropriated trade secrets, (that is, the average value of $(Q_t^M - Q_t^0)$ is zero).[91]

An additional issue relates to apportioning damages among the trade secrets alleged to have been misappropriated. In *O2 Micro v. Monolithic*,[92] O2 asserted eleven trade secrets and claimed consequential damages of $16 million for infringement of all eleven trade secrets. O2's damages expert did not apportion the damages among the trade secrets. The jury found that five trade secrets were infringed and awarded $12 million. The court vacated all consequential trade secret damages since the jury had not been provided any basis upon which to award partial damages.

Since the *O2 Micro* decision, experts have often avoided the burden of apportionment among trade secrets by claiming that the impact on unjust enrichment would be exactly the same if any subset of the asserted trade secrets were found to be valid and misappropriated. In other words, these experts assert that no matter how many or which of the asserted trade secrets were infringed, the amount of unjust enrichment is the same. For example, in *CardiAQ Valve Technologies, Inc. v. Neovasc Inc. et al.*, CardiAQ's damages expert claimed "that the total damages figure was $90 million, that the jury could award that figure by finding misappropriation of Trade Secrets 1 and 2 together, or 3, 4, or 6 separately, but that if the jury found misappropriation of multiple trade secrets, it should not add damages for each theory of liability."[93] While such assertions may be reasonable in some cases, they are probably not generally correct, given the

91. Of course, the result of such a calculation may occasionally give an accurate value of unjust enrichment but that would merely be coincidental.

92. O2 Micro Int'l Ltd. v. Monolithic Power Sys., 399 F. Supp. 2d 1064 (N.D. Cal. 2005).

93. CadiAQ Valve Techs., Inc. v. Neovasc Inc., 708 Fed. Appx. 654, 666 n.7 (Fed. Cir. Sept. 1, 2017).

sequential nature of research and scientific discovery and the incremental costs of making the discoveries that are the subject of each trade secret.

There is also the issue of apportionment between the alleged trade secrets and other inputs into the production, marketing, and sale of products that embody the alleged trade secrets. The ruling in *Mentor Graphics* may be pertinent.[94] There the Federal Circuit held that a *Panduit* analysis provides adequate apportionment of patent infringement lost profits. The court appeared to understand that in the but-for world, a patent infringer, if unable to use patented technology, would still attempt to compete by offering a noninfringing alternative or offering lower prices or both. A properly done *Panduit* analysis arguably takes these competitive responses into account. The conventional unjust enrichment damages analysis undertaken in trade secrets matters also attempts to model what would have happened if there had been no misappropriation. If that is correct, then no further apportionment may be required.

VI. CONVOYED SALES AND UNJUST ENRICHMENT

The federal patent statute provides for recovery of the plaintiff's damages, which are no less than a reasonable royalty for the defendant's use of the patent.[95] The patent statute does not provide for recovery of defendant's profits with respect to utility patents.

In the context of patent infringement, the Federal Circuit has defined convoyed sales as "the relationship between the sale of a patented product and a functionally associated non-patented

94. Mentor Graphics Corp. v. EVE-USA, Inc., No. 2015-1470, 2017 WL 1024502 (Fed. Cir. Mar. 16, 2017).

95. 35 U.S.C. § 284.

product."[96] Specifically, "[a] patentee may recover lost profits on unpatented components sold with a patented item . . . if both the patented and unpatented products 'together were considered to be components of a single assembly or parts of a complete machine, or they together constituted a functional unit.'"[97]

In addition to lost profits, the issue of convoyed sales is a factor considered in determining a reasonable royalty in a patent infringement matter. The oft-cited *Georgia-Pacific* factors indicate that one may consider "[t]he effect of selling the patented specialty in promoting sales of other products of the licensee; the existing value of the invention to the licensor as a generator of sales of his non-patented items; and the extent of such derivative or convoyed sales."[98]

Trade secrets law is not well developed with respect to recovery of a defendant's convoyed sales. As discussed above, both state and federal trade secrets law provide for recovery of the defendant's unjust enrichment caused by misappropriation.[99] One could contemplate circumstances wherein a defendant's profits from products that do not incorporate trade secrets are nonetheless attributable to its misappropriation. For example, consider the following set of circumstances:

1. The defendant sells a product incorporating the plaintiff's trade secrets.
2. The trade secrets are the sole basis of demand for the defendant's products.

---

96. Am. Seating Co. v. USSC Grp., Inc., 514 F.3d 1262, 1268 (Fed. Cir. 2008).

97. *Id*.

98. Georgia-Pacific Corp. v. United States Plywood Corp., 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970).

99. Defend Trade Secrets Act of 2016, § 2(b)(3)(B)(i)(II); Uniform Trade Secrets Act § 3(a) (amended 1985).

3. The defendant sells additional products that do not incorporate the trade secrets to customers who purchased the products containing the trade secrets (i.e., convoyed sales).

4. The only reason the defendant generated convoyed sales was due to the defendant's sale of products containing the alleged trade secrets.

In the above circumstances, it appears that the owner of the trade secrets can establish that defendant's convoyed sales are attributable to its misappropriation. As a result, one may consider calculating the defendant's profits from convoyed sales as an additional measure of the defendant's unjust enrichment. However, as discussed above, there appears to be no legal consensus on the issue of apportionment of a defendant's profits under a claim for unjust enrichment. Thus, if assumptions 2 or 4 in the above scenario are eliminated, a claim for defendant's profits from convoyed sales may become more tenuous and, therefore, more difficult to establish.

For example, consider a scenario where only 50% of the defendant's profits from a product are directly attributable to incorporation of a trade secret into the product's design, and only 50% of the defendant's convoyed sales are attributable to the sale of products incorporating the trade secrets. Without additional confirmatory evidence, several possible dynamics could result in this sales relationship, as follows:

- 25% of the defendant's convoyed sales are attributable to its misappropriation, based on serial application of apportionment factors (50% x 50% = 25%);
- 50% of the defendant's convoyed sales are attributable to its misappropriation, based on 100% alignment between the portion of convoyed sales attributable to

sales of products containing the trade secrets and consumer demand for the trade secrets (i.e., for all customers who purchased a convoyed item, the trade secrets were the sole basis of demand for the product containing the trade secrets: 50% x 100% = 50%); and

- 0% of the defendant's convoyed sales are attributable to its misappropriation, based on no overlap in demand for the trade secrets and convoyed sales (i.e., the only customers who purchased a convoyed item did so because of their demand for features other than the trade secrets: 0% x 50% = 0%).

The above dynamics indicate the potential challenge associated with calculating defendant's profits from convoyed sales attributable to misappropriation. However, an analysis of unjust enrichment is a fact-specific exercise that depends on the market dynamics present in each case.

RECENT CHANGES TO FEDERAL RULES OF EVIDENCE: WILL THEY MAKE IT EASIER TO AUTHENTICATE ESI?

Honorable Paul W. Grimm
U.S. District Judge
District of Maryland

Kevin F. Brady
Of Counsel
Redgrave, LLP

While there was great fanfare for the changes to the Federal Rules of Civil Procedure in 2006 and 2015 and the changes to Rule 502 of the Federal Rules of Evidence ("Fed. R. Evid." or "Rule(s)") in 2011, there has been little attention paid to the December 1, 2017, changes to Fed. R. Evid. 803(16) as well as Rule 902(13) and (14), which are intended to positively influence how parties manage electronically stored information (ESI). The changes to Rule 803(16) address authentication of digital information that has been stored for more than 20 years, eliminating the concern that factual assertions made in massive volumes of ESI will be admissible for the truth contained in the documents simply because of their age. The concurrent addition of new subsections (13) and (14) to Rule 902 provide for streamlined authentication of ESI, and potentially eliminate the need to call a witness at trial to authenticate the evidence. In addition, more changes to the Fed. R. Evid. are coming. The Advisory Committee on the Rules of Evidence is considering proposed changes to Rule 807.

I. THE ESI EVIDENCE ADMISSIBILITY CHART

Notwithstanding these helpful additions to the litigator's toolkit, many challenges remain for attorneys handling evidence from the rapidly-evolving landscape of data sources such as bitcoin, blockchain, smart contracts, social media, Internet of Things (IoT), mobile devices, and cloud computing services.

Moreover, the ever-expanding use of social media like Facebook, LinkedIn, and Instagram, as well as social messaging applications like WhatsApp, Viber, and Messenger present significant challenges for lawyers trying to authenticate digital evidence using the traditional rules of evidence. The ESI Evidence Admissibility Chart ("Chart") offers discovery lawyers and trial attorneys a quick reference guide for handling diverse sources of ESI evidence. From Rule 104 to Rule 803(6) to Rule 901 and Rule 902, the Chart provides a step-by-step approach for authenticating digital information and successfully getting that information admitted into evidence. The 2018 edition of the Chart, which has been updated to reflect the changes to Rules 803 and 902, is provided in Appendix A (*Admissibility of Electronic Evidence*).

II. FED. R. EVID. 803(16)—MODIFICATION OF THE ANCIENT DOCUMENTS EXCEPTION TO THE HEARSAY RULE

When it was enacted, Rule 803 was intended to address exceptions to the hearsay rule that were premised on the theory that "under appropriate circumstances a hearsay statement may possess circumstantial guarantees of trustworthiness sufficient to justify nonproduction of the declarant in person at the trial even though he may be available."[1] Under former Rule 803(16), commonly referred to as the "ancient document" exception to the hearsay rule, a document that would normally be excluded as hearsay is nonetheless admissible and may be introduced at trial or summary judgment for the truth of its content if the document was created more than 20 years earlier and the proponent of the document can prove the document is authentic under Rule 902. Historically, an "ancient document" theoretically

1. FED. R. EVID. 803(16), Notes of Advisory Committee on Proposed Rules (1972).

could be deemed more trustworthy because "age affords assurance that the writing antedates the present controversy."[2] Under that rationale, something mystical happens to a document when it turns 20 years old; it acquires a hearsay-defeating level of trustworthiness that it did not have one day earlier. The reality is that, based on anecdotal evidence, this exception was rarely used; and, when it was used, it was for hardcopy documents.[3] The recent concern leading to the amendment was that Rule 803(16) could someday apply to the ever-expanding volume of digital information that currently exceeds four zettabytes (four trillion gigabytes) of data.[4] Given the increasing reliance on computers and the creation of significant amounts of digital information in the mid- to late-1990s (launch dates for big data generators: Yahoo (1994), Amazon (1995), eBay (1995), Google and PayPal (1998)) and early 2000s,[5] some jurists and commentators were concerned about a tsunami of ESI turning 20 years old in the near future [6] and the real risk that substantial

---

2. *Id*.

3. Professor Daniel J. Capra found that Rule 803(16) was used to admit documents in fewer than 100 reported cases since the Federal Rules of Evidence were enacted. *See* Daniel J. Capra, *Electronically Stored Information and the Ancient Documents Exception to the Hearsay Rule: Fix It Before People Find Out About It*, 17 YALE J. L. & TECH. 1, 12 (2015). The Advisory Committee also noted that "[a] party will often offer hardcopy that is derived from ESI." May 7, 2016 Report of the Advisory Committee on Evidence Rules to the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, Standing Committee Agenda Book at 73 (June 6–7, 2016), http://www.uscourts.gov/sites/default/files/2016-06-standing-agenda-book.pdf (Hereinafter May 2016 Advisory Committee Report).

4. Daniel J. Capra, *supra* note 3, at 13 & n.46.

5. Gil Press, *A Very Short History of Big Data*, FORBES (May 9, 2013), https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/#2608231b65a1.

6. Daniel J. Capra, *supra* note 3, at 3–4.

amounts of unreliable ESI would be subject to near-automatic admissibility under the existing exception.

Indeed, the looming problem with Rule 803(16) remained under the radar until 2015 when Professor Daniel Capra of Fordham Law School, who serves as the reporter to the Judicial Conference Advisory Committee on Evidence Rules ("Advisory Committee"), highlighted the problem in his article, *Electronically Stored Information and the Ancient Documents Exception to the Hearsay Rule: Fix It Before People Find Out About It*.[7] As Professor Capra pointed out:

> The question, then, is whether the explosion of electronic information has separated ESI from the original justifications for the hearsay exception for ancient documents. As stated above, the primary justification for the ancient documents exception is necessity, which comes down to the premise that it is likely that all reliable evidence (such as business records) has been destroyed within the twenty-year time period, and thus we have to make do with more dubious evidence. This necessity assumption is substantially undermined by the growth of ESI. Because ESI is prevalent and easily preserved, whatever reliable evidence existed at the time of a twenty-year-old event *probably* still exists. Indeed, the probability that most or all ESI records (emails, text messages, receipts, scanned documents, etc.) will be available is certainly higher than the probability that hardcopy documents or eyewitnesses will still be available

7. Daniel J. Capra, *Electronically Stored Information and the Ancient Documents Exception to the Hearsay Rule: Fix It Before People Find Out About It*, 17 YALE J. L. & TECH. 1.

> and useful several decades after a contested event. There is no reason to admit *unreliable* ESI on necessity grounds if it is quite likely that there will be *reliable* ESI that is admissible under other hearsay exceptions.[8]

The Advisory Committee considered four proposals for addressing the problem: (1) abrogation of Rule 803(16); (2) limiting the exception to hardcopy; (3) adding the necessity requirement from the residual exception (Rule 807); and (4) adding the Rule 803(6) requirement that the document would be excluded if the opponent could show that the document was untrustworthy under the circumstances. In concluding that Rule 803(16) had to be abrogated, the Advisory Committee noted that the problems presented by the ancient documents exception could not be fixed by tinkering with it—the appropriate remedy is to abrogate the exception and leave the field to other hearsay exceptions such as the residual exception (Rule 807) and the business records exception (Rule 803(6)). In particular:

> [t]here was no support for the proposal that would limit the exception to hardcopy, as the distinction between ESI and hardcopy would be fraught with questions and difficult to draw. For example, is a scanned copy of an old document, or a digitized version of an old book, ESI or hardcopy? As to the proposals to import either necessity or reliability requirements into the rule, Committee members generally agreed that they would be problematic because they would draw the ancient documents exception closer to the residual

8. *Id.* at 15 (citations omitted).

> exception, thus raising questions about how to distinguish those exceptions.[9]

As the Advisory Committee also concluded, hearsay that is in fact reliable will very likely be admissible under other reliability-based exceptions.[10]

However, the public reaction to that approach was largely negative. Many of the comments complained that without Rule 803(16), "important documents in certain specific types of litigation would no longer be admissible—or would be admissible only through expending resources that are currently not necessary under Rule 803(16). Examples of litigation cited by the public comment include cases involving latent diseases; disputes over the existence of insurance; cases involving environmental cleanups; and title disputes."[11]

In light of the public sentiment, the Advisory Committee went back to the drawing board and ultimately decided to limit the "ancient documents" exception to documents prepared before 1998 because that would not affect any of the specific cases raised in the public comments because those cases involved records prepared well before 1998. The Advisory Committee also recognized "that any cutoff date will have a degree of arbitrariness, but . . . the ancient documents exception itself set an arbitrary time period for its applicability."[12]

---

9. April 17, 2015 Meeting Minutes of the Advisory Committee on Evidence Rules, Standing Committee Agenda Book at 492 (May 28–29, 2015), http://www.uscourts.gov/sites/default/files/2015-05-standing-agenda-book_1.pdf.

10. May 2016 Advisory Committee Report, *supra* note 3, at 46.

11. *Id.*

12. *Id.* at 47.

As a result, under new Rule 803(16), *documents (hard copy and ESI) that were prepared prior to January 1, 1998, and whose authenticity has been established will qualify as a hearsay exception, regardless of whether the preparer or declarant is available as a witness*.

III. FED. R. EVID. 902(13) AND (14)—NEW OPTIONS FOR AUTHENTICATING ESI

When the proponents of evidence want to offer a document into evidence either at the summary judgment stage or at trial in a civil case or criminal case, there are some evidentiary steps they have to climb before the judge or jury can consider the information. First, it has to be relevant: Does the evidence logically relate to what is at issue in the case? Second, it has to be authentic: Is the evidence what it purports to be? For example, if someone took a forensic image of a hard drive from a laptop computer as part of discovery in a case and, a year later, they wanted to introduce that forensic image into evidence, the proponent must be able to show that the forensic image that the proponent wants to show the jury is what it purports to be—namely, a document in the identical condition as it was when the image of the hard drive was made a year earlier that has not been altered, doctored or manipulated.

Rule 902 identifies evidence that is "self-authenticating," i.e., information that can be admitted at trial without being authenticated by a witness. Self-authenticating evidence is admissible without extrinsic evidence of authenticity "sometimes for reasons of policy but perhaps more often because practical considerations reduce the possibility of unauthenticity to a very small dimension."[13] Most of the items listed in Rule 902 are self-authenticating on their face, thus requiring no extrinsic evidence

13. FED. R. EVID. 902, Notes of Advisory Committee on Proposed Rules (1972). *See also In re* Miller, No. 10–25453, 2012 WL 6041639, at *7 (Bankr. D.

of authenticity for the document to be admitted. Other items, such as those listed in Rule 902(11) and Rule 902(12) (for records of regularly conducted activity, domestic and foreign, respectively), are self-authenticating *only* to the extent the party seeking to introduce them into evidence certifies their authenticity and provides notice to the opposing party to give them a fair opportunity to challenge the certification. In conjunction with the amendment of Rule 803(6) in 2000, the enactment of Rule 902(11) that same year streamlined the process by which business records could be admitted into evidence under the business records exception to the hearsay rule.[14]

The Advisory Committee in 2017 supplemented Rule 902 by adding two subsections permitting similar certifications to authenticate electronic evidence. The amendments should eliminate the need for a live witness to testify as to the authenticity

---

Colo. Dec. 4, 2012) ("Rule 902 strikes a balance in favor of self-authentication for certain enumerated evidence because the likelihood of fabricating such evidence is slight versus the time and expense which would be required for authentication through extrinsic evidence. When a self-authenticating document is offered under Rule 902, the proponent is relieved of the requirement to lay foundation or present testimony through a witness. In other words, if a document is self-authenticating, the general authentication requirement of Rule 901 is deemed satisfied." (citation omitted)); Leo v. Long Island R. Co., 307 F.R.D. 314, 325 (S.D.N.Y. 2015) (in rejecting the applicability of Rule 902 to videotapes, the court explained that "the drafters of the Federal Rules of Evidence anticipated that, in specified circumstances, certain types of exhibits may be so evidently that which the proponent claims them to be that they may be deemed authentic without extrinsic evidence."); United Asset Coverage, Inc. v. Avaya Inc., 409 F. Supp. 2d 1008, 1052 (N.D. Ill. 2006) (describing new Rule 902(11) as "[o]ne of the most useful (though perhaps least noticed) accomplishments" of the Committee during that court's tenure, and lamenting that "[t]oo few lawyers have caught up with that valuable amendment").

14. *See generally* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 552 (D. Md. 2007).

of ESI, thereby streamlining the process at trial. New subsection 13 addresses certifying information generated by an electronic process or system, and new subsection 14, which is narrower than Rule 902(13), addresses certifying data copied from an electronic device, storage medium, or file.[15] The new subsections to Rule 902 are:

> **(13) Certified Records Generated by an Electronic Process or System.** A record generated by an electronic process or system that produces an accurate result, as shown by a certification by a qualified person that complies with the certification requirements of Rule 902(11) or Rule 902(12). The proponent must also meet the notice requirements of Rule 902(11).
>
> **(14) Certified Data Copied from an Electronic Device, Storage Medium, or File.** Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification by a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

As with the provisions on business records in Rules 902(11) and 902(12), the Advisory Committee noted that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary because the adversary either stipulates to authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. Under the amendments to Rule 902, the parties are now able to determine in advance of trial whether a real challenge to authenticity will be made.

---

15. May 2016 Advisory Committee Report, *supra* note 3, at 54–57 (discussing proposed new subsections (13) and (14)).

It is important to note that Rule 902(11) relates "only to the procedural requirements" of authentication.[16] Likewise, new Rules 902(13) and 902(14) are designed to do "nothing more than authenticate" ESI.[17] Therefore, the proponent of the evidence sought to be admitted still must prove the requirements of Rule 803(6) after clearing the authenticity hurdle. Put more simply, the new rules are intended merely to simplify the process of proving that ESI sought to be admitted constitute true and accurate copies of electronic information maintained in the ordinary course of business by the proponent or a third party. What is important to note from Rule 902(13) and (14) is that the references to Rule 902(11) and (12) are simply to the form of the declaration—the affidavit you want to introduce must have the same formality and style as the certifications referred to in Rule 902(11) and (12). Rule 902(13) and (14) are not saying that the certification for subsections (13) and (14) has to include the substantive certification of Rule 902(11), which is tied to Rule 803(6)(A)(B)(C) elements for the business record exception.

New subsections 13 and 14, like Rule 902(11) and (12), permit a foundation witness or "qualified person" to establish the authenticity of information by way of certification.[18] Subsection

16. May 2016 Advisory Committee Report, *supra* note 3, at 55.

17. April 29, 2016 Meeting Minutes of the Advisory Committee on Evidence Rules, Advisory Committee Agenda Book at 25 (Oct. 21, 2016), http://www.uscourts.gov/sites/default/files/2016-10-evidence-agenda-book.pdf.

18. Pursuant to Rule 901(11) and (12), a "qualified person" is a custodian or other individual who has the ability to establish the authenticity of the ESI as if that person would have testified at trial such as under Fed. R. Evid. 901(b)(1) [Testimony of a Witness with Knowledge] or 901(b)(4) [Distinctive Characteristics and the Like]. The threshold question for a court to determine the authenticity of a document is not whether the evidence is necessarily what the proponent says it is, but rather whether the evidence is sufficient

13 provides for self-authentication of machine-generated information—such as system metadata—upon the submission of a certification prepared by a qualified person. Subsection 14 provides for authentication of data copied from an electronic device, medium, or file—such as an email or Excel spreadsheet that was stored on a computer—through digital identification. The Advisory Committee noted, in most instances, digital identification involves authentication of data copied from electronic devices by comparing the "hash value" of the proffered copy to that of the original document. A hash value is a unique alphanumeric sequence of characters that an algorithm determines based upon the digital contents of the device.[19] The hash value serves as the digital fingerprint that a qualified person uses to compare the numeric value of the proffered item with the numeric value of the original item. If the hash values for the original and copy are identical, the information can be proffered, and the court can rely on them as authentic copies. The Advisory Committee also noted that "the rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology."[20]

The new Rules 902(13) and 902(14) have the same effect as other Rule 902 provisions of shifting to the opponent the burden of going forward, but not the burden of proof, on authenticity disputes regarding the electronic evidence at issue. Shifting the burden of questioning the authenticity of such records to the opponent who has a fair opportunity to challenge both the certification and the records streamlines the process by which these

---

that a jury ultimately might be able to so determine. *See* U.S. v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006).

19. May 7, 2016, Advisory Committee Report, *supra* note 3, at 56.

20. *Id.*

items can be authenticated, reducing the time, cost, and inconvenience of presenting this evidence at trial or summary judgment. The proponent of the evidence bears the burden of establishing a prima facie case that the ESI is what it purports to be and establishing authenticity if challenged, but need not go through the expense and inconvenience of using a witness to establish authenticity in the first instance. The opponent, of course, is able to object to the admissibility of the evidence on any other applicable ground.

Rule 902(13) is designed to permit the proponent to show that the evidence in question is authentic by attaching an affidavit under oath by the person or people with the technical or specialized knowledge of how the system or process works certifying that the evidence is reliable and accurate. Rule 902(14) allows for a certification—an affidavit or declaration by someone who has first-hand, personal knowledge (or expertise, if qualified as provided by Rule 702)—that would explain the process by which that person took a forensic copy of the evidence such as a hard drive of a laptop, hashed it, and then compared the hash value of the forensic copy with the hash value of the original hard drive. If the original hash value and the hash value of the forensic copy are the same, then the information in the copy is identical to the information in the original.

For example, if an individual takes a picture with his smart phone, embedded within the electronic metadata of that photograph are Global Position System (GPS) coordinates of the location where that photograph was taken. In a criminal case, where the prosecution must prove that the defendant was in a specific location by virtue of photographs taken from that defendant's cell phone, the metadata from that electronic photograph that shows the GPS coordinates is evidence of where the smartphone and, by extension, where the person was located when the picture was taken. Now, the prosecutor can put that information in

an affidavit and offer the affidavit to the defendant with the request to voice any objection regarding authenticity. If the defendant objects, the prosecutor must actually prove the authenticity and will need to bring one or more witnesses—persons with the scientific, technical, or specialized knowledge—to the trial to testify under oath how the system and processes produce reliable results. If the defendant does not object, the prosecutor has established authenticity and no authenticating witness would be needed at trial. Unless the affiant qualifies as an expert under Rule 702, she must provide information based on direct personal knowledge. The affiant's testimony cannot be based on what someone else told the affiant. Moreover, if the proponent has a system or process that requires explanation by multiple persons in order to be complete, affidavits are needed from each of those persons.

In a situation where the proponent wants to authenticate a process that predates any current employee at the organization, the proponent will need an expert to provide an affidavit. That expert must be able to testify that they have knowledge, training, experience, education, or skill which constitutes scientific, technical, or other specialized knowledge—and, based upon that, they can state how the process operates. Experts may base their opinions on information derived from other sources so long as the sources are reliable.[21]

21. Under Fed. R. Evid. 702, if the jury lacks the subject matter knowledge in an area involving scientific, technical, or other specialized knowledge, the proponent can have a subject matter expert base their opinion on information which is provided to them by others as long as the source of information they rely upon is generally recognized as reliable by other people with that degree of specialty or expertise.

Fed. R. Evid. 902(13) and (14) Certifications

The Rule 902 certification is intended to take the place of the testimony traditionally required to establish the authenticity of the ESI sought to be admitted; therefore, it should follow the same pattern as the testimony it is intended to replace. The certification should start by establishing the background, education, training, and expertise of the affiant in order to establish that she is a "qualified person" as required by Rule 902(11) and (12). Although Rule 902(13) and (14) do not refer to Rule 702, careful lawyers would be wise to ensure that the affiant providing the certificate meets the requirements of an expert witness under Rule 702 if the underlying facts to be authenticated involve scientific, technical, or specialized knowledge, as the underlying facts often do. The added benefit of showing that the affiant meets these Rule 702 requirements is that the affiant may base her certification on information beyond her personal knowledge, provided it is reliable, as described in Rule 703. The certification should then describe the affiant's role in the case, i.e., that she was retained by the party as a computer forensics expert in order to assist the party and its counsel in the identification, preservation, collection, and production of ESI. The certification should describe in detail the evidence in question and establish its authenticity consistent with the formality requirements of Rule 901(11) and (12). The certification need not meet the requirements of Rule 803(6)(A–C), unless the proponent also seeks to qualify the evidence as a business record. Rather, the certification must provide the information required by Rule 902(13) and (14), as discussed below.

If the certificate seeks to authenticate evidence under Rule 902(13), the affiant should describe in detail the "electronic process or system" that was used to generate the information in question. For example, if the information in question is a series

of monthly sales reports, the affiant should describe: (i) the system from which the reports were generated; (ii) the process by which the data that was used to generate the statements was gathered, processed, and stored; and (iii) the process by which the statements or reports sought to be admitted were generated and produced for the litigation. The Rule 902(13) certificate should establish that the information sought to be admitted has not been altered from the form in which it was maintained in the ordinary course of business. While the process of preparing a certification under Rule 902 is seemingly straightforward, the affiant must be careful to describe the "electronic process or system" with enough specificity to satisfy the court and the opponent of the authenticity of the evidence sought to be admitted, and to avoid a hearing during which the opponent of the evidence may cross-examine the affiant.

If the certificate seeks to authenticate evidence under Rule 902(14), the affiant also should describe in detail the electronic information that was copied from its original location and now offered into evidence, as well as the steps taken by the affiant at the time of duplication (including recording the date, time, surrounding circumstances, and hardware and software tools as well as versions utilized). For example, if the information sought to be admitted is a series of Excel and PowerPoint files that were stored on the departmental file share for the client's accounting department, the affiant should list the files in question and include the hash value of each of the files as they existed on the file share as well as the hash value for the copy of each of the files sought to be admitted in order to establish that the files sought to be admitted are authentic copies of the files as they were maintained in the ordinary course of business. The identical hash values will attest that the information sought to be admitted into evidence is a true and correct copy of the information as it existed in its original state.

As final practice pointers, the proponent should keep in mind that the certifications required by Rules 902(13) and Rule 902(14) must be substantive and not boilerplate. As a rule of thumb, they should be as detailed and specific as they would have to be if the witness was testifying in court to authenticate the digital evidence. And, because neither Rule 902(13) or Rule 902(14) provide a deadline by which the party receiving the certification must indicate its objection to the use of the certificate to authenticate the evidence, the cautious lawyer will seek a stipulation as to when the opponent will assert an objection, or ask the court to set a deadline, so that, if an objection is made, the proponent has sufficient time to arrange to bring in a live witness or witnesses.

Sample certifications under Rules 902(13) and 902(14) are provided in Appendices B and C, respectively.

IV. FED. R. EVID. 807—PROPOSED AMENDMENT TO RESIDUAL EXCEPTION TO THE HEARSAY RULE

In 2016 and 2017, the Advisory Committee considered whether to propose an amendment to Rule 807, the residual exception to the hearsay rule, and specifically whether to expand the exception to allow the admission of reliable hearsay even absent "exceptional circumstances." On October 21, 2016, the Advisory Committee met at Pepperdine University School of Law in Los Angeles[22] and held a symposium to review, among other things, possible amendments to Rule 807, including a working draft of an amendment that had been prepared in advance.

22. March 2017 Report of the Committee on Rules of Practice and Procedure to the Judicial Conference of the United States, Standing Committee Agenda Book at 72–73 (June 12–13, 2017), http://www.uscourts.gov/sites/default/files/2017-06-standing-agenda_book_0.pdf.

After the symposium, the Advisory Committee decided against expansion of the residual exception, but concluded that several problems with the current Rule 807 could be addressed by rule amendment.[23] In April 2017, the Advisory Committee proposed and the Standing Committee approved an amendment to Rule 807 for publication in August 2017.[24] The amendment eliminates the "equivalence" standard in the existing rule in favor of a more direct focus on circumstantial guarantees of trustworthiness for proffered statements, taking into account the presence or absence of corroboration. In addition, the proposed amendment eliminates the "materiality" and "interests of justice" requirements as duplicative, while retaining the "more probative" requirement in the existing rule.

The proposed amendment to Rule 807 was published for public comment, with the comment period officially closing on February 15, 2018.[25] At its April 2018 meeting, the Advisory Committee approved a proposed amendment to Rule 807 and submitted it to the Standing Committee for final approval. The current text of Rule 807 is restated in Section A, below, followed by: the main issues that the Advisory Committee identified with

23. September 2017 Report of the Committee on Rules of Practice and Procedure to the Judicial Conference of the United States, Standing Committee Agenda Book at 99–100 (Jan. 4, 2018), http://www.uscourts.gov/sites/default/files/2018-01-standing-agenda-book.pdf. The proposed amendment addresses several issues with the current notice requirements that are not discussed here.

24. Draft Minutes of the June 12–13, 2017 Meeting of the Committee on Rules of Practice and Procedure, Standing Committee Agenda Book at 52–53 (Jan. 4, 2018), http://www.uscourts.gov/sites/default/files/2018-01-standing-agenda-book.pdf.

25. October 26, 2017 Meeting Minutes of the Advisory Committee on Evidence Rules, Advisory Committee Agenda Book at 15 (April 26–27, 2018), http://www.uscourts.gov/sites/default/files/agenda_book_advisory_committee_on_rules_of_evidence_-_final.pdf.

current Rule 807 (Section B); comments regarding proposed changes published by the Advisory Committee following their October 2017 meeting (Section C); and the proposed amended Rule 807 including the proposed Committee Note (Section D).

A. Current Rule 807:

Rule 807. Residual Exception

(a) In General. Under the following circumstances, a hearsay statement is not excluded by the rule against hearsay even if the statement is not specifically covered by a hearsay exception in Rule 803 or 804:

(1) the statement has equivalent circumstantial guarantees of trustworthiness;

(2) it is offered as evidence of a material fact;

(3) it is more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts; and

(4) admitting it will best serve the purposes of these rules and the interests of justice.

(b) Notice. The statement is admissible only if, before the trial or hearing, the proponent gives an adverse party reasonable notice of the intent to offer the statement and its particulars, including the declarant's name and address, so that the party has a fair opportunity to meet it.

B. Issues[26] with Current Rule 807 as Identified by The Advisory Committee:

- The requirement that the court find trustworthiness "equivalent" to the circumstantial guarantees in the Rule 803 and 804 exceptions is difficult to apply because there is no unitary standard of trustworthiness in the Rule 803 and 804 exceptions.
- The requirements in Rule 807 that the residual hearsay must be proof of a "material fact" and that admission of residual hearsay be in "the interests of justice" have not served any purpose.
- Is the requirement that the hearsay statement must be "more probative than any other evidence that the proponent can obtain through reasonable efforts" necessary?

C. Comments Regarding the Proposed Changes to Rule 807 Published by the Advisory Committee Following Their October 2017 Meeting:

> The requirement that the court find trustworthiness "equivalent" to the circumstantial guarantees in the Rule 803 and 804 exceptions should be deleted—without regard to expansion of the residual exception. That standard is exceedingly difficult to apply, because there is no unitary standard of trustworthiness in the Rule 803 and 804 exceptions. It is common ground that statements falling

26. May 7, 2017 Report of the Advisory Committee on Evidence Rules to the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, Standing Committee Agenda Book at 736–737 (June 12–13, 2017), http://www.uscourts.gov/sites/default/files/2017-06-standing-agenda_book_0.pdf.

within the Rule 804 exceptions are not as reliable as those admissible under Rule 803; and it is also clear that the bases of reliability differ from exception to exception. Moreover, one of the exceptions subject to "equivalence" review—Rule 804(b)(6) forfeiture—is not based on reliability at all. Given the difficulty of the "equivalence" standard, a better approach is simply to require the judge to find that the hearsay offered under Rule 807 is trustworthy. This is especially so because a review of the case law indicates that the "equivalence" standard has not fulfilled the intent of the drafters to limit the discretion of the trial court. Given the wide spectrum of reliability found in the hearsay exceptions, it is not difficult to find a statement reliable by comparing it to a weak exception, or to find it unreliable by comparing it to a strong one.

Trustworthiness can best be defined in the Rule as requiring an evaluation of both 1) circumstantial guarantees surrounding the making of the statement, and 2) corroborating evidence. Most courts find corroborating evidence to be relevant to the reliability enquiry, but some do not. An amendment would be useful to provide uniformity in the approach to evaluating trustworthiness under the residual exception—and substantively, that amendment should specifically allow the court to consider corroborating evidence, as corroboration is a typical source for assuring that a statement is reliable. Adding a requirement that the court consider corroboration is an improvement to the rule independent of any decision to expand the residual exception.

> The requirements in Rule 807 that the residual hearsay must be proof of a "material fact" and that admission of residual hearsay be in "the interests of justice" and consistent with the "purpose of the rules" have not served any good purpose. The inclusion of the language "material fact" is in conflict with the studious avoidance of the term "materiality" in Rule 403—and that avoidance was well-reasoned, because the term "material" is so fuzzy. The courts have essentially held that "material" means "relevant"—and so nothing is added to Rule 807 by including it there. Likewise nothing is added to Rule 807 by referring to the interests of justice and the purpose of the rules because that guidance is already provided by Rule 102.
>
> The requirement in the residual exception that the hearsay statement must be "more probative than any other evidence that the proponent can obtain through reasonable efforts" should be retained. This will preserve the principle that proponents cannot use the residual exception unless they need it. And it will send a signal that the changes proposed are modest—there is no attempt to allow the residual exception to swallow the categorical exceptions, or even to permit the use the residual exception if the categorical exceptions are available.[27]

27. April 21, 2017 Meeting Minutes of the Advisory Committee on Evidence Rules; Advisory Committee Agenda Book at 13–14 (Oct. 26–27. 2017), http://www.uscourts.gov/sites/default/files/a3_0.pdf.

D. Proposed Amended Rule 807 and Committee Note:

Rule 807. Residual Exception[28]

(a) In General. Under the following ~~circumstances~~ conditions, a hearsay statement is not excluded by the rule against hearsay even if the statement is not ~~specifically covered by~~ admissible under a hearsay exception in Rule 803 or 804:

> **(1)** the statement ~~has equivalent circumstantial~~ is supported by sufficient guarantees of trustworthiness—after considering the totality of the circumstances under which it was made and evidence, if any, corroborating the statement; and
>
> ~~**(2)** it is offered as evidence of a material fact;~~
>
> **(~~3~~2)** it is more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts~~; and~~
>
> ~~**(4)** admitting it will best serve the purposes of these rules and the interests of justice~~.

(b) Notice. The statement is admissible only if~~, before the trial or hearing,~~ the proponent gives an adverse party reasonable notice of the intent to offer the statement ~~and its particulars, including the declarant's name and address,~~ —including its substance and the declarant's name—so that the party has a fair opportunity to meet it. The notice must be provided in writing before the trial or

28. May 14, 2018 Report of the Advisory Committee on Evidence Rules to the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, Standing Committee Agenda Book at 409–410 (June 12, 2018), http://www.uscourts.gov/sites/default/files/2018-06_standing_agenda_book_final.pdf. New material is underlined; matter to be omitted is lined through.

hearing—or in any form during the trial or hearing if the court, for good cause, excuses a lack of earlier notice.

Committee Note[29]

Rule 807 has been amended to fix a number of problems that the courts have encountered in applying it.

Courts have had difficulty with the requirement that the proffered hearsay carry "equivalent" circumstantial guarantees of trustworthiness. The "equivalence" standard is difficult to apply, given the different types of guarantees of reliability, of varying strength, found among the categorical exceptions (as well as the fact that some hearsay exceptions, e.g., Rule 804(b)(6), are not based on reliability at all). The "equivalence" standard has not served to guide a court's discretion to admit hearsay, because the court is free to choose among a spectrum of exceptions for comparison. Moreover, experience has shown that some statements offered as residual hearsay cannot be compared usefully to any of the categorical exceptions and yet might well be trustworthy. Thus the requirement of an equivalence analysis has been eliminated. Under the amendment, the court should proceed directly to a determination of whether the hearsay is supported by guarantees of trustworthiness. See Rule 104(a). As with any hearsay statement offered under an exception, the court's threshold finding that admissibility re-

29. May 14, 2018 Report of the Advisory Committee on Evidence Rules to the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, Standing Committee Agenda Book at 410–414 (June 12, 2018), http://www.uscourts.gov/sites/default/files/2018-06_standing_agenda_book_final.pdf.

quirements are met merely means that the jury may consider the statement and not that it must assume the statement to be true.

The amendment specifically requires the court to consider corroborating evidence in the trustworthiness enquiry. Most courts have required the consideration of corroborating evidence, though some courts have disagreed. The rule now provides for a uniform approach, and recognizes that the existence or absence of corroboration is relevant to, but not dispositive of, whether a statement should be admissible under this exception. Of course, the court must consider not only the existence of corroborating evidence but also the strength and quality of that evidence.

The amendment does not alter the case law prohibiting parties from proceeding directly to the residual exception, without considering admissibility of the hearsay under Rules 803 and 804. A court is not required to make a finding that no other hearsay exception is applicable. But the opponent cannot seek admission under Rule 807 if it is apparent that the hearsay could be admitted under another exception.

The rule in its current form applies to hearsay "not specifically covered" by a Rule 803 or 804 exception. The amendment makes the rule applicable to hearsay "not admissible under" those exceptions. This clarifies that a court assessing guarantees of trustworthiness may consider whether the statement is a "near-miss" of one of the Rule 803 or 804 exceptions. If the court employs a "near-miss" analysis it should—in addition to evaluating all relevant guarantees of trustworthiness—take into account the reasons that the hearsay misses the admissibility requirements of the standard exception.

In deciding whether the statement is supported by sufficient guarantees of trustworthiness, the court should not consider the credibility of any witness who relates the declarant's hearsay statement in court. The credibility of an in-court witness does not present a hearsay question. To base admission or exclusion of a hearsay statement on the witness's credibility would usurp the jury's role of determining the credibility of testifying witnesses. The rule provides that the focus for trustworthiness is on circumstantial guarantees surrounding the making of the statement itself, as well as any independent evidence corroborating the statement. The credibility of the witness relating the statement is not a part of either enquiry.

Of course, even if the court finds sufficient guarantees of trustworthiness, the independent requirements of the Confrontation Clause must be satisfied if the hearsay statement is offered against a defendant in a criminal case.

The Committee decided to retain the requirement that the proponent must show that the hearsay statement is more probative than any other evidence that the proponent can reasonably obtain. This necessity requirement will continue to serve to prevent the residual exception from being used as a device to erode the categorical exceptions.

The requirements that residual hearsay must be evidence of a material fact and that its admission will best serve the purposes of these rules and the interests of justice have been deleted. These requirements have proved to be superfluous in that they are already found in other rules. See Rules 102, 401.

The notice provision has been amended to make four changes in the operation of the rule:

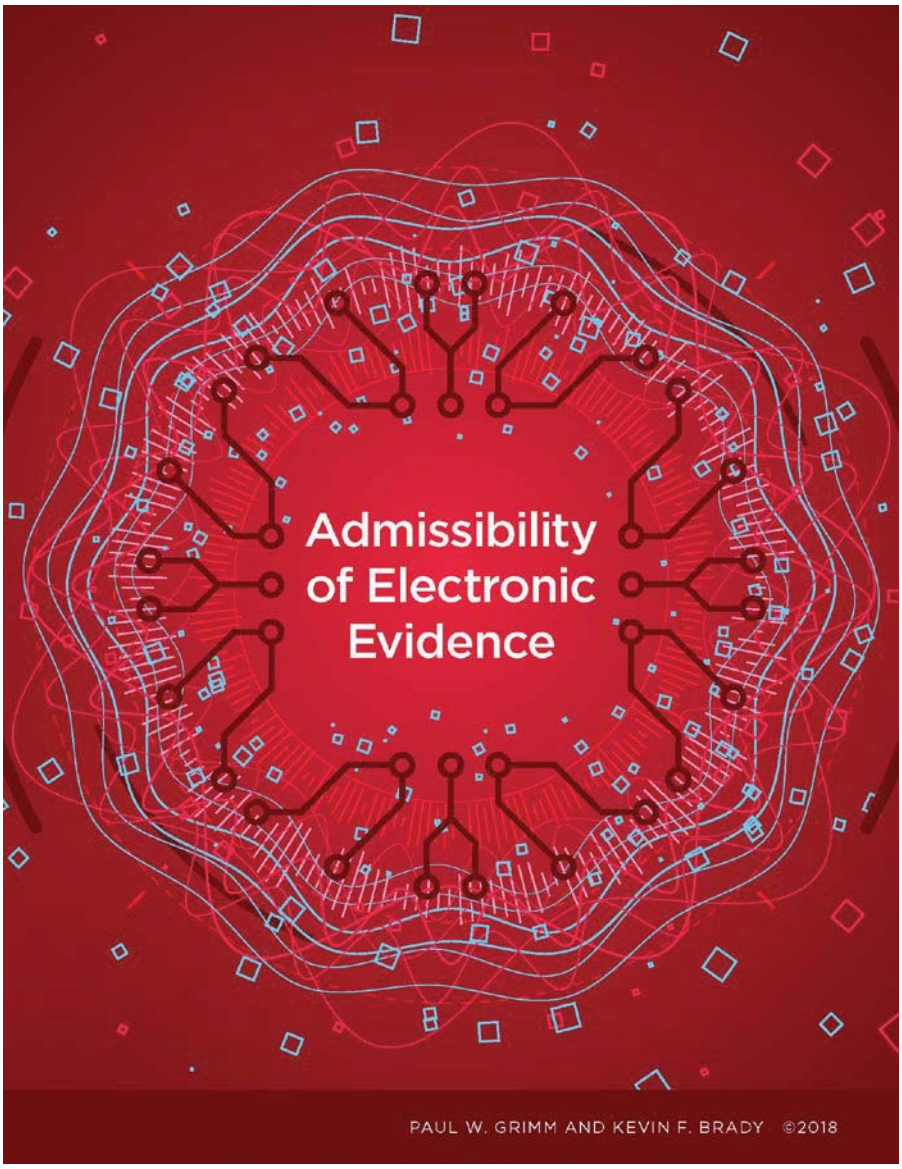
- First, the amendment requires the proponent to disclose the "substance" of the statement. This term is intended to require a description that is sufficiently specific under the circumstances to allow the opponent a fair opportunity to meet the evidence. See Rule 103(a)(2) (requiring the party making an offer of proof to inform the court of the "substance" of the evidence).
- Second, the prior requirement that the declarant's address must be disclosed has been deleted. That requirement was nonsensical when the declarant was unavailable, and unnecessary in the many cases in which the declarant's address was known or easily obtainable. If prior disclosure of the declarant's address is critical and cannot be obtained by the opponent through other means, then the opponent can seek relief from the court.
- Third, the amendment requires that the pretrial notice be in writing—which is satisfied by notice in electronic form. See Rule 101(b)(6). Requiring the notice to be in writing provides certainty and reduces arguments about whether notice was actually provided.
- Finally, the pretrial notice provision has been amended to provide for a good cause exception. Most courts have applied a good cause exception under Rule 807 even though the rule in its current form does not provide for it, while some courts have read the rule as it was written. Experience under the residual exception has shown that a

good cause exception is necessary in certain limited situations. For example, the proponent may not become aware of the existence of the hearsay statement until after the trial begins; or the proponent may plan to call a witness who without warning becomes unavailable during trial, and the proponent might then need to resort to residual hearsay.

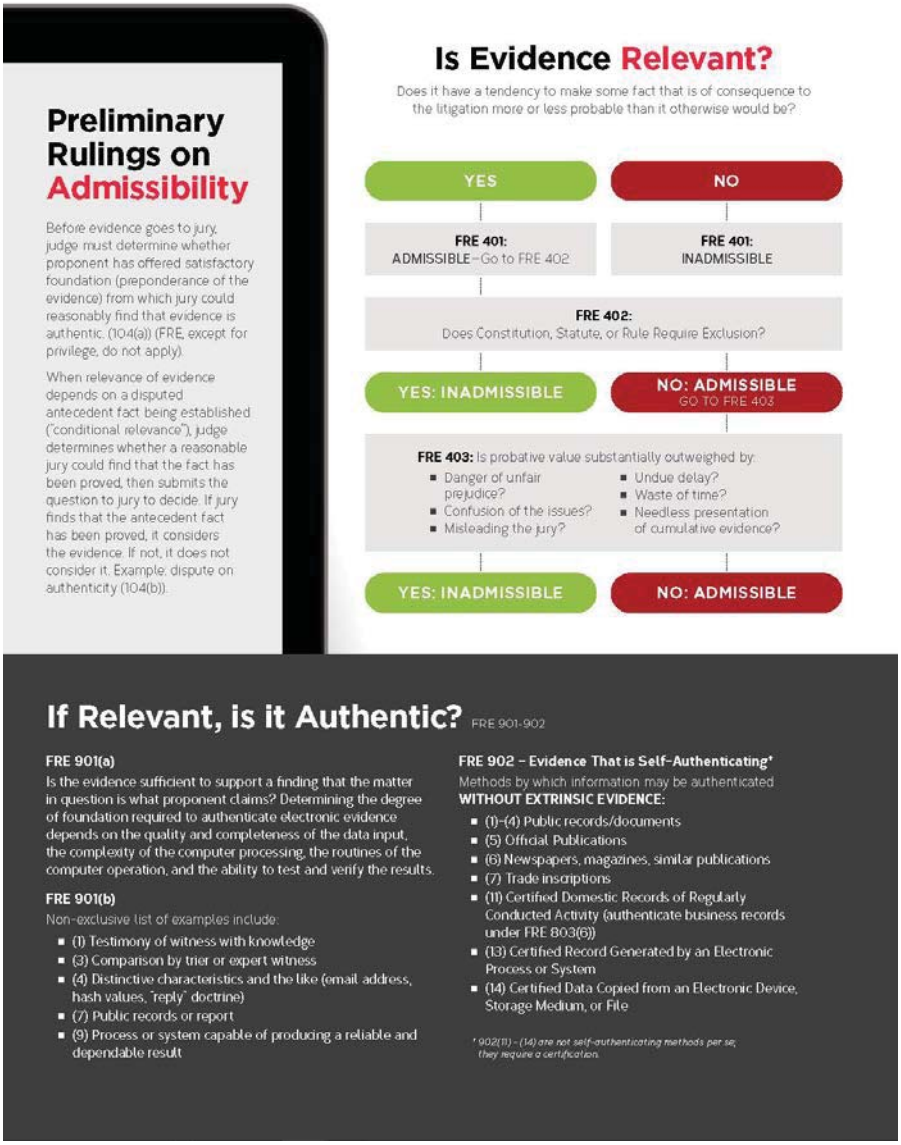
- The rule retains the requirement that the opponent receive notice in a way that provides a fair opportunity to meet the evidence. When notice is provided during trial after a finding of good cause, the court may need to consider protective measures, such as a continuance, to assure that the opponent is not prejudiced.

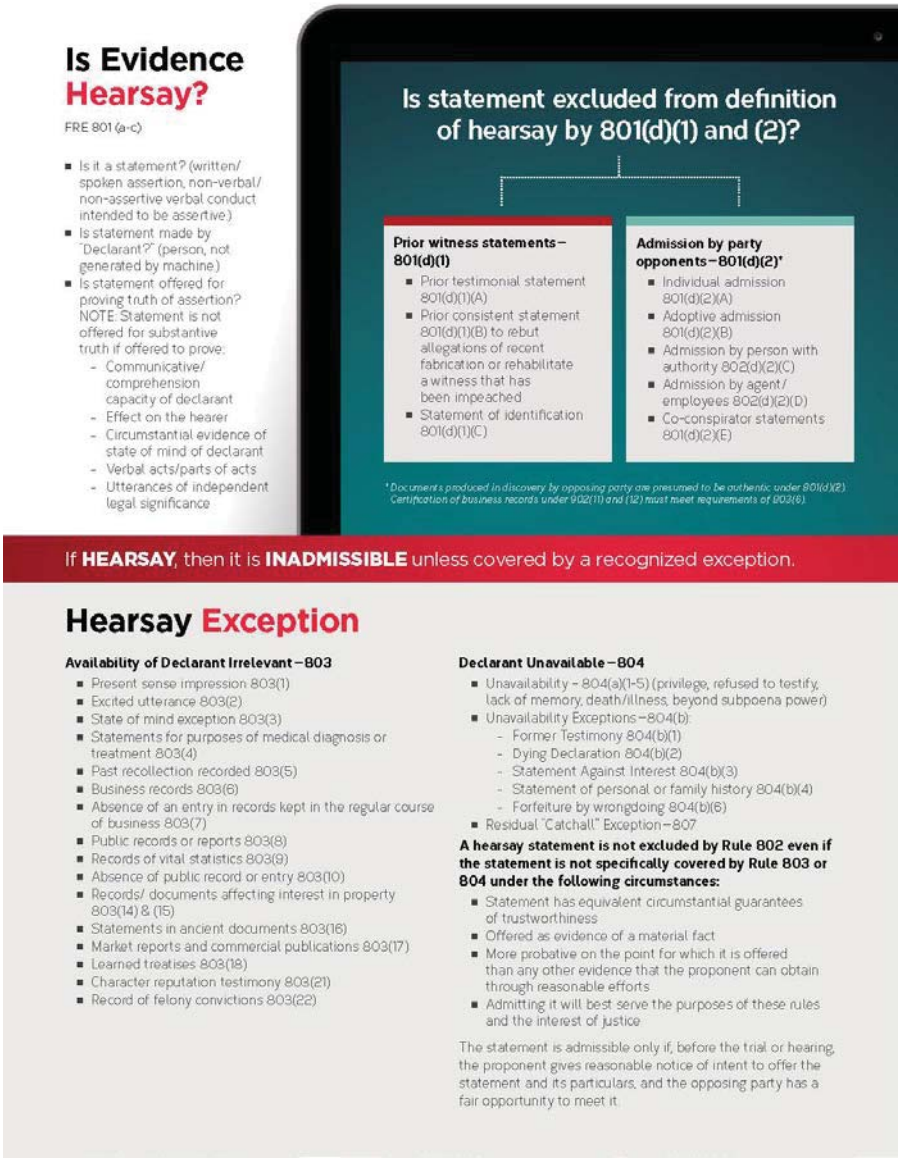
APPENDIX A:
ESI EVIDENCE ADMISSIBILITY CHART

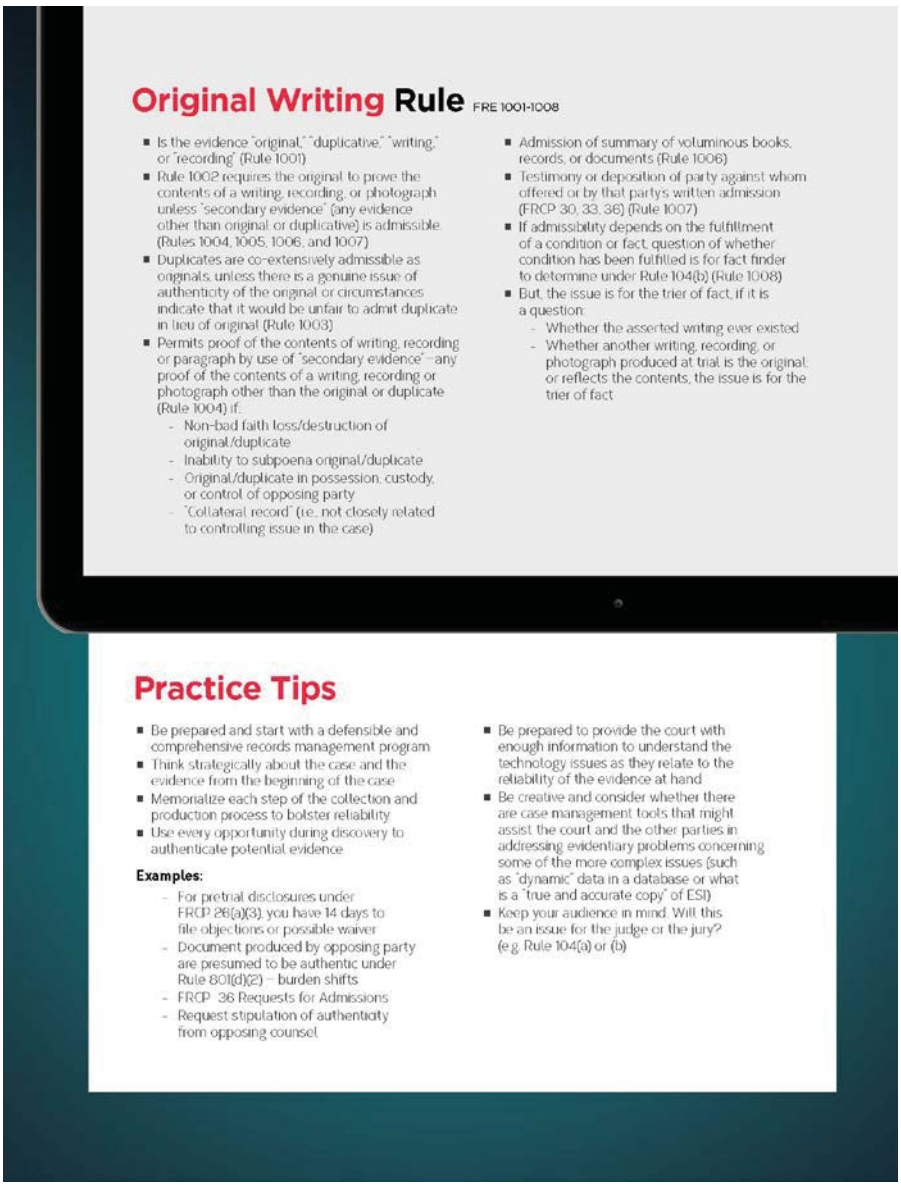
Admissibility of Electronic Evidence has been reprinted with permission from the Honorable Paul W. Grimm and Kevin F. Brady. To download an enlarged version, *see* https://bit.ly/2NFWlp0.




Potential Authentication Methods
Email, Text Messages, and Instant Messages
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
Distinctive characteristics including circumstantial evidence (901(b)(4))
System or process capable of proving a reliable and dependable result (901(b)(9))
Trade inscriptions (902(7))
Certified copies of business record (902(11))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
Chat Room Postings, Blogs, Wikis, and Other Social Media Conversations
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
Distinctive characteristics including circumstantial evidence (901(b)(4))
System or process capable of proving a reliable and dependable result (901(b)(9))
Official publications (902(5))
Newspapers and periodicals (902(6))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
Digitally Stored Data and Internet of Things
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
Distinctive characteristics including circumstantial evidence (901(b)(4))
System or process capable of proving a reliable and dependable result (901(b)(9))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
Computer Processes, Animations, Virtual Reality, and Simulations
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
System or process capable of proving a reliable and dependable result (901(b)(9))
Certified records generated by an electronic process or system (902(13))
Digital Photographs
Witness with personal knowledge (901(b)(1))
System or process capable of providing reliable and dependable result (901(b)(9))
Official publications (902(5))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
Social Media Sites (Facebook, LinkedIn, Twitter, Instagram, and Snapchat)
Witness with personal knowledge (901(b)(1))
Expert testimony or comparison with authenticated examples (901(b)(3))
Distinctive characteristics including circumstantial evidence (901(b)(4))
Public records (901(b)(7))
System or process capable of proving a reliable and dependable result (901(b)(9))
Official publications (902(5))
Certified records generated by an electronic process or system (902(13))
Certified data copied from an electronic device, storage medium, or file (902(14))
Know Which Approach Your Jurisdiction Follows
Maryland Approach to Rules 104 and 901:
A higher standard for authentication for social media evidence. In this approach, the burden is on the admitting party to show that the social media evidence was not falsified or created by another user through either:
Testimony of the creator of the website page or the post
Search of the internet history or hard drive of the purported creator's computer
Information obtained directly from social media site
See, Griffin v. State, 19 A. 3d 415, 423 (Md. 2011).
Texas Approach to Rules 104 and 901:
A lower standard for authentication of social media evidence. In this approach, the burden is on the admitting party to show evidence sufficient to support a finding by a reasonable juror that the social media evidence is what its proponent claims it to be through either:
Direct testimony of a witness with personal knowledge
Expert testimony or comparison with authenticated evidence
Circumstantial evidence
See, Tienda v. State, 358 S.W. 3d 633 (Tex. Crim. App. 2012)


Preliminary Rulings on Admissibility
Before evidence goes to jury, judge must determine whether proponent has offered satisfactory foundation (preponderance of the evidence) from which jury could reasonably find that evidence is authentic. (104(a)) (FRE, except for privilege, do not apply).
When relevance of evidence depends on a disputed antecedent fact being established ("conditional relevance"), judge determines whether a reasonable jury could find that the fact has been proved, then submits the question to jury to decide. If jury finds that the antecedent fact has been proved, it considers the evidence. If not, it does not consider it. Example: dispute on authenticity (104(b)).
Is Evidence Relevant?
Does it have a tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be?
YES
NO
FRE 401: ADMISSIBLE – Go to FRE 402
FRE 401: INADMISSIBLE
FRE 402: Does Constitution, Statute, or Rule Require Exclusion?
YES: INADMISSIBLE
NO: ADMISSIBLE GO TO FRE 403
FRE 403: Is probative value substantially outweighed by:
Danger of unfair prejudice?
Confusion of the issues?
Misleading the jury?
Undue delay?
Waste of time?
Needless presentation of cumulative evidence?
YES: INADMISSIBLE
NO: ADMISSIBLE
If Relevant, is it Authentic? FRE 901-902
FRE 901(a)
Is the evidence sufficient to support a finding that the matter in question is what proponent claims? Determining the degree of foundation required to authenticate electronic evidence depends on the quality and completeness of the data input, the complexity of the computer processing, the routines of the computer operation, and the ability to test and verify the results.
FRE 901(b)
Non-exclusive list of examples include:
(1) Testimony of witness with knowledge
(3) Comparison by trier or expert witness
(4) Distinctive characteristics and the like (email address, hash values, "reply" doctrine)
(7) Public records or report
(9) Process or system capable of producing a reliable and dependable result
FRE 902 – Evidence That is Self-Authenticating*
Methods by which information may be authenticated WITHOUT EXTRINSIC EVIDENCE:
(1)-(4) Public records/documents
(5) Official Publications
(6) Newspapers, magazines, similar publications
(7) Trade inscriptions
(11) Certified Domestic Records of Regularly Conducted Activity (authenticate business records under FRE 803(6))
(13) Certified Record Generated by an Electronic Process or System
(14) Certified Data Copied from an Electronic Device, Storage Medium, or File
* 902(11) - (14) are not self-authenticating methods per se; they require a certification.


Is Evidence Hearsay?
FRE 801 (a-c)
Is it a statement? (written/ spoken assertion, non-verbal/ non-assertive verbal conduct intended to be assertive)
Is statement made by "Declarant?" (person, not generated by machine)
Is statement offered for proving truth of assertion? NOTE: Statement is not offered for substantive truth if offered to prove:
Communicative/ comprehension capacity of declarant
Effect on the hearer
Circumstantial evidence of state of mind of declarant
Verbal acts/parts of acts
Utterances of independent legal significance
Is statement excluded from definition of hearsay by 801(d)(1) and (2)?
Prior witness statements – 801(d)(1)
Prior testimonial statement 801(d)(1)(A)
Prior consistent statement 801(d)(1)(B) to rebut allegations of recent fabrication or rehabilitate a witness that has been impeached
Statement of identification 801(d)(1)(C)
Admission by party opponents – 801(d)(2)*
Individual admission 801(d)(2)(A)
Adoptive admission 801(d)(2)(B)
Admission by person with authority 802(d)(2)(C)
Admission by agent/ employees 802(d)(2)(D)
Co-conspirator statements 801(d)(2)(E)
* Documents produced in discovery by opposing party are presumed to be authentic under 801(d)(2). Certification of business records under 902(11) and (12) must meet requirements of 803(6).
If HEARSAY, then it is INADMISSIBLE unless covered by a recognized exception.
Hearsay Exception
Availability of Declarant Irrelevant – 803
Present sense impression 803(1)
Excited utterance 803(2)
State of mind exception 803(3)
Statements for purposes of medical diagnosis or treatment 803(4)
Past recollection recorded 803(5)
Business records 803(6)
Absence of an entry in records kept in the regular course of business 803(7)
Public records or reports 803(8)
Records of vital statistics 803(9)
Absence of public record or entry 803(10)
Records/ documents affecting interest in property 803(14) & (15)
Statements in ancient documents 803(16)
Market reports and commercial publications 803(17)
Learned treatises 803(18)
Character reputation testimony 803(21)
Record of felony convictions 803(22)
Declarant Unavailable – 804
Unavailability – 804(a)(1-5) (privilege, refused to testify, lack of memory, death/illness, beyond subpoena power)
Unavailability Exceptions – 804(b):
Former Testimony 804(b)(1)
Dying Declaration 804(b)(2)
Statement Against Interest 804(b)(3)
Statement of personal or family history 804(b)(4)
Forfeiture by wrongdoing 804(b)(6)
Residual "Catchall" Exception – 807
A hearsay statement is not excluded by Rule 802 even if the statement is not specifically covered by Rule 803 or 804 under the following circumstances:
Statement has equivalent circumstantial guarantees of trustworthiness
Offered as evidence of a material fact
More probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts
Admitting it will best serve the purposes of these rules and the interest of justice
The statement is admissible only if, before the trial or hearing, the proponent gives reasonable notice of intent to offer the statement and its particulars, and the opposing party has a fair opportunity to meet it.


Original Writing Rule FRE 1001-1008
Is the evidence "original," "duplicative," "writing," or "recording" (Rule 1001)
Rule 1002 requires the original to prove the contents of a writing, recording, or photograph unless "secondary evidence" (any evidence other than original or duplicative) is admissible. (Rules 1004, 1005, 1006, and 1007)
Duplicates are co-extensively admissible as originals, unless there is a genuine issue of authenticity of the original or circumstances indicate that it would be unfair to admit duplicate in lieu of original (Rule 1003)
Permits proof of the contents of writing, recording or paragraph by use of "secondary evidence" – any proof of the contents of a writing, recording or photograph other than the original or duplicate (Rule 1004) if:
Non-bad faith loss/destruction of original/duplicate
Inability to subpoena original/duplicate
Original/duplicate in possession, custody, or control of opposing party
"Collateral record" (i.e., not closely related to controlling issue in the case)
Admission of summary of voluminous books, records, or documents (Rule 1006)
Testimony or deposition of party against whom offered or by that party's written admission (FRCP 30, 33, 36) (Rule 1007)
If admissibility depends on the fulfillment of a condition or fact, question of whether condition has been fulfilled is for fact finder to determine under Rule 104(b) (Rule 1008)
But, the issue is for the trier of fact, if it is a question:
Whether the asserted writing ever existed
Whether another writing, recording, or photograph produced at trial is the original; or reflects the contents, the issue is for the trier of fact
Practice Tips
Be prepared and start with a defensible and comprehensive records management program
Think strategically about the case and the evidence from the beginning of the case
Memorialize each step of the collection and production process to bolster reliability
Use every opportunity during discovery to authenticate potential evidence
Examples:
For pretrial disclosures under FRCP 26(a)(3), you have 14 days to file objections or possible waiver
Document produced by opposing party are presumed to be authentic under Rule 801(d)(2) – burden shifts
FRCP 36 Requests for Admissions
Request stipulation of authenticity from opposing counsel
Be prepared to provide the court with enough information to understand the technology issues as they relate to the reliability of the evidence at hand
Be creative and consider whether there are case management tools that might assist the court and the other parties in addressing evidentiary problems concerning some of the more complex issues (such as "dynamic" data in a database or what is a "true and accurate copy" of ESI)
Keep your audience in mind. Will this be an issue for the judge or the jury? (e.g. Rule 104(a) or (b))


Electronic copies of the chart are available at no charge. To obtain a copy or for more information,
contact Kevin Brady, Redgrave LLP, at kbrady@redgravellp.com.

APPENDIX B:
CERTIFICATION OF AUTHENTICITY UNDER FEDERAL RULE OF EVIDENCE 902(13)

I, _____, being duly sworn, hereby certify that:

1. I have been requested by [organization] to provide an [affidavit/certification] under Federal Rule of Evidence 902(13) that the [information/records/data] described below were generated by an electronic process/system that produces an accurate result consistent with the requirements of Federal Rules of Evidence 902(11) [or 902(12)] and 803(6)(A-C) [only if also seeking to qualify the records as business records in addition to authenticating them].
2. I am an adult, over the age of 21 years, and I am competent to testify. [Note: If the affiant would qualify to give opinion testimony on a topic of scientific, technical, or specialized knowledge under Federal Rule of Evidence 702, insert a description of his/her qualifications, as noted in No. 3, below. If not, establish that the information used to certify the evidence is based on the affiant's personal knowledge.]
3. Describe: educational background and relevant work experience including current job description, professional training, and membership in professional organizations.
4. Describe prior certification experience.
5. Identify and describe prior testimony.
6. I am currently a [title], [organization].
7. Describe knowledge and experience in information systems in general and in particular the "electronic process or system" that was used to generate the information in question or system at issue. [Note: Person signing affidavit or certification must have personal knowledge of the facts and systems [hardware and software] that are at issue and they

must describe the "electronic process or system" with enough specificity to satisfy the court and the opponent that the evidence sought to be admitted is authentic.]

I declare under penalty of perjury that the foregoing is true and correct.

Dated: _____

_____

Name of Affiant/Declarant

[For Affidavits - Insert Notary Public Notarization Here]

APPENDIX C:
CERTIFICATION OF AUTHENTICITY UNDER FEDERAL RULE OF EVIDENCE 902(14)

I, _____, being duly sworn, hereby certify that:

1. I have been requested by [organization] to provide an [affidavit/certification] under Federal Rule of Evidence 902(14) that the [records/data] described below were generated by an electronic process/system that produces an accurate result consistent with the requirements of Federal Rules of Evidence 902(11) [or 902(12)] and 803(6) (A-C) [only if also seeking to qualify the records as business records in addition to authenticating them].
2. I am an adult, over the age of 21 years, and I am competent to testify. [Note: If the affiant would qualify to give opinion testimony on a topic of scientific, technical, or specialized knowledge under Federal Rule of Evidence 702, insert a description of his/her qualifications, as noted in No. 3, below. If not, establish that the information used to certify the evidence is based on the affiant's personal knowledge.]
3. Describe: educational background, relevant work experience, professional training, and membership in professional organizations.
4. Describe prior certification experience.
5. I am currently a [title], [organization].
6. Describe knowledge and experience in information systems in general and the particular system at issue.
7. I performed the following [X]. Attached as Exhibit "A" is a list of items that I examined. Describe in detail the electronic information that was copied from its original location and the steps the affiant took (including date, time, circumstances, hardware and software tools as well as

versions utilized) regarding the information to be offered into evidence. [Note: To prove that the information to be admitted into evidence is a true and correct copy of the original information, it is important to list the files or data in question and show the hash value of each on the original source and then the hash value of the file or data sought to be admitted into evidence. If the hash values are identical, that is proof that the information sought to be admitted into evidence is a true and correct copy of the information as it originally existed.]

I declare under penalty of perjury that the foregoing is true and correct.

Dated: _____

_____

Name of Affiant/Declarant

[For Affidavits - Insert Notary Public Notarization Here]

META-DISCOVERY: ALLEGATIONS OF AN INCOMPLETE DOCUMENT PRODUCTION

Honorable Xavier Rodriguez
U.S. District Judge
Western District of Texas

Honorable David L. Horan
U.S. Magistrate Judge
Northern District of Texas

Introduction

The federal courts have not yet provided a clear standard to apply to cases where a requesting party alleges that the producing party has made an incomplete production. The Texas Supreme Court has recently ventured into this arena. United States Magistrate Judge (Ret.) Craig Shaffer also recently discussed this topic and thoroughly discussed the applicable federal rules of civil procedure in a recent *Sedona Conference Journal* article.[1] Judge Shaffer's article, however, addressed two distinct issues. His thoughtful discussion addressed whether initial discovery about discovery that may help a litigant "properly frame" discovery requests is relevant and proportional.[2] Judge Shaffer's article then also interwove an analysis of cases that tackled allegations of an incomplete document production. Judge Shaffer concludes that "process-directed" discovery as opposed to "merits-based" discovery "may, in fact, fall within the scope of relevance under Rule 26(b)(1) when a party's production has been incomplete."[3] After acknowledging the various differing

1. Hon. Craig B. Shaffer, *Deconstructing "Discovery about Discovery,"* 19 SEDONA CONF. J. 215 (2018).

2. Judge Shaffer opines that "[p]ursuing discovery in order to draft discovery seems, at the very least, unnecessarily expensive." *Id*. at 235.

3. *Id*. at 239.

approaches courts have used to review allegations of an incomplete production, Judge Shaffer advocates that "[p]rocess-directed discovery be predicated on a thoughtful analysis of strategic considerations, the goals of the Federal Rules, and a factual record that is consistent with the well-recognized burdens of proof." Yet he proposes no standard that courts should apply to address an allegation of incomplete production nor reconciles the numerous cases applying differing theories with his statement that there are "well-recognized burdens of proof."

This article analyzes the recent Texas opinion, compares it with federal court cases, proposes a standard that courts should apply, and opines that when a requesting party has made an initial showing (beyond subjective belief) of a material deficiency in the producing party's discovery production, a court should grant a motion to compel allowing further discovery into the producing party's discovery processes applying the discovery proportionality factors, and in appropriate cases allow for limited forensic examination of relevant computer devices to ensure that discovery production has been adequately completed.

In re Shipman[4]

Jamie Shelton argued that Marion Shipman, her former business partner, kept detailed business records on his computers––both the one that "crashed" in 2012 and his current computer. After exchanges of discovery, a motion to compel was filed. The trial court ordered Shipman to produce more financial documents. In a deposition following the court order, Shipman testified that he had produced all such documents in his possession. He added, however, that some relevant data was on a computer that "crashed" in 2012, more than two years before Shelton sued him. Shipman testified he was unable to retrieve records from

4. *In re* Shipman, 540 S.W.3d 562 (Tex. 2018).

that computer. A few days after his deposition, Shipman reported that his son had helped him discover files from his old computer in a "backup" folder on his replacement computer, and his attorney subsequently produced these newly found documents.

Shipman further testified in his deposition that several years before suit was filed, his certified public accountant had advised him that he could destroy documents more than seven years old, so he burned those files in 2011. Both Shipman and his attorney submitted affidavits stating they had diligently searched Shipman's files, both physical and electronic, and produced all responsive documents, more than 6,000 pages.

Because of the new deposition testimony and belated production of new documents, Shelton filed a second motion to compel, essentially arguing that Shipman could not be trusted to fulfill his discovery obligations. Shelton asked the trial court to compel Shipman to turn over his computers for forensic inspection. The forensic examiner testified he could determine if more backup files existed, whether files had been deleted, and whether files could be recovered from the "crashed" computer.

The trial court ordered Shipman to produce not only his computer but also all "media" for forensic examination, including "all internal hard drives and external media (including, without limitation, thumb drives, hard drives, CDs, DVDs, zip drives and any other storage medium) in Shipman's possession, custody or control and used by Shipman or his agents at any time during the period January 1, 2000 through the present."[5] The order provided a forensic-examination protocol to protect

5. It appears that, at the Supreme Court, all parties agreed that this Order was broader in scope than requested, and the Supreme Court found the breadth and time span violated the Court's recent opinion in *In re* State Farm Lloyds, 520 S.W.3d 595 (Tex. 2017).

Shipman's privacy and legal privileges. The forensic examiner would generate a list of all file names on the media and provide the list only to Shipman's counsel, who could then make objections before turning anything over to Shelton's counsel.

In response to the court order, Shipman filed a mandamus action in the court of appeals arguing the trial court had abused its discretion in ordering the forensic examination. The appellate court denied the petition. Shipman then filed his action in the Texas Supreme Court.

In granting the mandamus petition, the Texas Supreme Court acknowledged that Shipman had given conflicting answers in his deposition testimony. At one point he stated he searched his files and he didn't have any responsive documents. At other times when asked about certain financial documents he stated: "I'll have to look and see," "I don't know if our records go back that far," and "I don't know if I've still got it."[6] In his deposition testimony he also admitted deleting files from a computer, but he later clarified that he meant deletion from the "old" computer.

The Texas Supreme Court concluded that Shipman's belated production of the backup files, although inconsistent with his earlier testimony, indicated an effort to comply with his discovery obligations. "And the discovery process is best served by rules that encourage parties to produce documents belatedly discovered in good faith. They should not face the perverse incentive to conceal such information lest they be forced to hand over the underlying electronic devices for forensic examination."[7]

6. *In re Shipman*, 540 S.W.3d at 568.

7. *Id*.

Regarding the adequacy of the initial searches, the Court concluded that Shipman was "competent at some level to operate a computer and create and negotiate computer files"[8] and that Shelton offered no evidence that Shipman was incapable of searching for computer files, "or that an exhaustive search for backup files has not now been conducted, either by Shipman or his son."[9] "Shipman's affidavit testimony that he has produced all responsive documents is his ultimate answer on what documents are in his possession. His inability to remember off the cuff what documents he possesses, even when combined with any skepticism surrounding late production of the 'backup' folder, creates only more skepticism, not evidence of default under *Weekley*."[10]

So what evidence is necessary to show that a party has not complied with his discovery obligations?

The *Shipman* Court stated that it was not suggesting "that a requesting party can never establish a discovery-obligation default under *Weekley*[11] by offering evidence of a producing party's technical ineptitude."[12] Nor did the Court "discount trial-court discretion in determining when that line is crossed."[13] But the Court concluded that the "burden imposed by *Weekley* is high."[14] The Court complained that the record was silent as to what exactly Shipman's and his son's technical capabilities were.

---

8. *Id*. at 569.
9. *Id*.
10. *Id*.
11. *In re* Weekley Homes, L.P., 295 S.W.3d 309 (Tex. 2009).
12. *In re Shipman*, 540 S.W.3d at 569.
13. *Id*.
14. *Id*.

In *Weekley*, which in turn relied on Texas Rule of Civil Procedure 196.4,[15] the Texas Supreme Court addressed a case where the defendant had produced only a handful of emails and no emails from the email accounts of two individuals "very involved" in a subdivision project at issue in the case. The Supreme Court recognized "the trial court could have concluded that HFG made a showing that Weekley did not search for relevant deleted emails that HFG requested."[16] Nevertheless, the Court stated that this foundation did not necessarily establish that a search of the employees' hard drives would likely reveal deleted emails or that they would be reasonably capable of recovery.[17] "[Plaintiff's] conclusory statements that the deleted emails it seeks 'must exist' and that deleted emails are in some cases recoverable is not enough to justify the highly intrusive method of discovery the trial court ordered, which afforded the forensic experts 'complete access to all data stored on [the Employees'] computers.' The missing step is a demonstration that the particularities of Weekley's electronic information storage

15. "196.4 Electronic or Magnetic Data. To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot—through reasonable efforts—retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information."

16. *In re Weekley Homes, L.P.*, 295 S.W.3d at 319.

17. *Id*. at 320.

methodology will allow retrieval of emails that have been deleted or overwritten, and what that retrieval will entail."[18]

So according to the *Shipman* Court, evidence that some discovery production was late, and some deposition answers were equivocal, only amounts to mere suspicion that more unrecovered data exists. A party must be "pressed" at his deposition concerning the producing party's computer skills, the specific steps taken to search his computer, and the adequacy of the search. All this because "forensic examination of electronic devices is 'particularly intrusive and should be generally discouraged.'"[19]

The Texas Supreme Court is rightly concerned with ensuring that discovery requests propounded by a party are proportional to the case at hand. But courts should be mindful that relevant discovery generally no longer resides in "hard copy" and is prevalent in computer systems and mobile devices.[20] Although there are legitimate privacy interests that need to be weighed and costs to be taken in account, courts should approach discovery of electronically stored information (ESI) with these realities of modern recordkeeping practices in mind.

Does Texas's practice mirror federal court rules and opinions?

Generally, federal courts have analyzed discovery disputes in four ways: (1) objections asserting a lack of relevance, (2) ob-

18. *Id*.

19. *In re Shipman*, 540 S.W.3d at 569.

20. FEDERAL JUDICIAL CENTER POCKET GUIDE SERIES, *Managing Discovery of Electronic Information* (3d Ed. 2017) ("Discovery involving word-processing documents, spreadsheets, email, and other ESI is commonplace. Once seen primarily in large actions involving sophisticated entities, it is now routine in civil actions and is increasingly seen in criminal actions.").

jections lodged because of privilege, work product, or trade secrets assertions, (3) proportionality or undue burden/cost assertions, or (4) failure to produce relevant documents. This article confines its analysis to this last segment of cases.

Federal courts assume that parties have fulfilled their obligations under Federal Rule of Civil Procedure 26(g). "The discovery process is designed to be extrajudicial, and it relies on responding parties to search their own records and produce documents or other data."[21] Under Rule 26(g), counsel must certify that to the best of her knowledge, information, and belief formed after a reasonable inquiry, a discovery production is complete and correct as of the time it was made, and counsel may rely on assertions made by a client, as long as that reliance is appropriate and reviewed on the totality of the circumstances.[22]

Thereafter, federal courts require that the parties confer in good faith prior to the filing of any motion to compel and/or for sanctions.[23] In appropriate cases, some courts have utilized the services of a special master or an eDiscovery mediator to resolve any dispute.[24]

---

21. Hespe v. City of Chicago, No. 13 C 7998, 2016 WL 7240754, at *4 (N.D. Ill. December 15, 2016).

22. *See* Venator v. Interstate Resources, Inc., No. CV415-086, 2016 WL 1574090 (S.D. Ga. April 15, 2016).

23. FED. R. CIV. P. 37(a)(1) ("The motion must include a certification that the movant has in good faith conferred or attempted to confer with the person or party failing to make disclosure or discovery in an effort to obtain it without court action."); *cf.* TEX. R. CIV. P. 191.2.

24. *See* EPAC Tech., Inc. v. HarperCollins Christian Publ', Inc., No. 3:12-cv-00463, 2018 WL 1542040, at *4 (M.D. Tenn. Mar. 29, 2018) (Court appointed a special master despite the defendant's objection that "it should have an opportunity to continue to supplement its production in light of the revealed deficiencies and that any discovery issues could be more expediently handled by the Court.").

Regarding the failure to produce relevant documents thought likely to exist, the party seeking discovery has the burden of proving that a discovery response is inadequate. But that burden has not been interpreted as strictly as was suggested by the Texas Supreme Court in *In re Shipman*.[25]

When a motion to compel has been filed for incomplete disclosure under Federal Rule of Civil Procedure 37(a), many courts have reached the same conclusion as *In re Shipman* that "mere suspicion" or speculation that a party is withholding discoverable information is insufficient.[26] Some courts have also

25. *See* Tsanacas v. Amazon.com, Inc., No. 4:17-CV-00306, 2018 WL 324447, at *4 (E.D. Tex. Jan. 8, 2018) ("When some documents have been produced in response to a request, Courts have interpreted 'evasive or incomplete' to place a modest burden on the requesting party to support, with existing documents, a reasonable deduction that other documents may exist or did exist but have been destroyed."); *see also* Toyo Tire & Rubber Co. v. CIA Wheel Grp., No. SACV1500246DOCDFMX, 2016 WL 6246384, at *1 (C.D. Cal. Feb. 23, 2016) (Court found CIA's response inadequate because it told the court "next to nothing about what was searched and what search terms were performed." Furthermore, the court did not "share CIA's belief that Toyo must take a deposition to identify shortcomings in CIA's methods. At a minimum, parties must share some information about the protocol used to ensure that responsive documents are collected and produced." Notwithstanding the above, the request for a forensic examination of CIA's computer systems was denied "at this time.").

26. John B. v. Goetz, 531 F.3d 448, 460 (6th Cir. 2009) ("[M]ere skepticism that an opposing party has not produced all relevant information is not sufficient to warrant drastic electronic discovery measures."); *In re* Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (vacating order allowing discovery to defendant's databases because there was no finding of some non-compliance by Ford of its discovery obligations); Gordon v. Greenville Indep. Sch. Dist., No. 3:13-cv-178-P, 2014 WL 6603420, at *2 (N.D. Tex. Nov. 20, 2014) ("Although Plaintiff is not satisfied with this response, he fails to point to anything that suggests such reports actually exist. The Court cannot compel GISD to produce documents that do not exist."); Seahorn Investments, L.L.C. v. Fed. Ins. Co., No. 1:13CV320-HSO-RHW, 2014 WL 11444117, at *4 (S.D.

referenced the intrusiveness of an examination of a party's electronic devices or information systems.[27] "However, when the requesting party is able to demonstrate that 'the responding party has failed in its obligations to search its records and produce the requested information,' . . . an inspection of the responding party's electronic devices may be appropriate."[28] Further, courts have been less apprehensive of requests to inspect electronic devices where there is a "substantiated connection between the device the requesting party seeks to inspect and the claims in the case."[29]

By way of example, in *Wallace v. Tesoro Corp.*, the court granted a motion to compel after Tesoro failed to produce a single document responsive to the central issue in the case. The

Miss. Oct. 16, 2014) ("In response to the motion to compel, Plaintiff affirms that all responsive documents have been produced. The Court will therefore require no further response . . . ."); NOLA Spice Designs, L.L.C. v. Haydel Enterprises, Inc., No. 12-2515, 2013 WL 3974535 (E.D. La. Aug. 2, 2013) (defendant failed to receive documents it suspected should exist, but plaintiff stated under oath it did not possess any such documents); McElwee v. Wallantas, No. Civ. A. L-03-CV-172, 2005 WL 2346945, at *3 (S.D. Tex. Sept. 26, 2005) ("[T]he Court cannot order the Defendants to produce documentation that does not exist. Therefore, unless the Plaintiff can provide proof that the documents exist, rather than mere speculation, the Court will not entertain motions to compel the Defendants to produce documentation whose existence is nothing more than theoretical."); Henderson v. Compdent of Tenn., Inc., No. Civ. A. 97-617, 1997 WL 756600, at *1 (E.D. La. Dec. 4, 1997) ("The Court cannot compel production of what does not exist. Of course, if defendants have or acquire evidence that the response is incomplete or that the affidavit is false, other remedies may be sought by motion.").

27. *See* A.M. Castle & Co. v. Byrne, 123 F. Supp. 3d 895, 909 (S.D. Tex. 2015).

28. Hespe v. City of Chicago, No. 13 C 7998, 2016 WL 7240754, at *4 (N.D. Ill. December 15, 2016).

29. *Id*.

plaintiff learned that the defendants refused to employ a Boolean search in their document review process and instead employed a restrictive qualifier that was "virtually guaranteed to avoid finding relevant ESI."[30]

In *Venator v. Interstate Resources, Inc.*, the court granted in part a motion to compel and for sanctions when counsel never confirmed that all hard drives had been searched and a party merely designated a human resource manager responsible for the searches of its computer systems to gather responsive documents. The client had an IT department, but failed to adequately consult that department, and the HR manager admitted he did not fully understand the IT systems. The court required the defendants to pay the plaintiff's reasonable expenses and fees associated with the filing of her motion because of the "woefully insufficient electronic records search" but declined to order a site inspection of the defendant's computer systems.[31]

One court granted a motion to conduct a forensic examination where a party failed to timely implement a litigation hold, allowed executives to self-collect ESI, and collected email using a single search term. In that case, many of the witnesses testified that counsel never issued instructions on how to search for ESI or documents, never saw the requests for production, and were unable to state whether there was an automated deletion process or backup tapes.[32]

---

30. Wallace v. Tesoro Corp., No. SA-11-CA-00099, 2016 WL 7971286 (W.D. Tex. Sept. 26, 2016).

31. Venator v. Interstate Resources, Inc., CV415-086, 2016 WL 1574090 (S.D. Ga. April 15, 2016).

32. Procaps S.A. v. Pantheon Inc., No. 1:12-cv-24356, 2014 WL 11498060 (S.D. Fl. Dec. 1, 2014).

In some cases, courts have ordered the taking of a corporate representative's deposition under Federal Rule of Civil Procedure 30(b)(6) "to consider whether adequate efforts have been made to respond to requests for production."[33] Thereafter, some courts have ordered the production of relevant computer hard drives "based upon discrepancies or inconsistencies in a response to a discovery request or the responding party's unwillingness or failure to produce relevant information."[34]

By comparison, in denying a motion to compel, the Court in *A.M. Castle & Co. v. Byrne*[35] concluded that Castle had not shown that the defendants were in wrongful possession of any company documents, nor had it provided any evidence that the defendants were or had been deleting files. To the contrary, the defendants hired an independent firm to perform a forensic examination of their computers that included a search for hundreds of terms requested by Castle. "That Castle is skeptical, without anything else to support its request for an intrusive fishing expedition in Defendants' electronic devices is insufficient to support such a drastic discovery request."[36]

Likewise, in *Memry Corp. v. Kentucky Oil Technology, N.V.*,[37] the court denied a motion to compel a forensic examination where the defendant represented it had made a reasonable search for responsive documents and the plaintiff could only point to two missing emails out of thousands of documents produced. In addition, the court appeared concerned that there was

33. Robinson v. City of Arkansas City, Kan., No. 10-1431-JAR-GLR, 2012 WL 603576, at *15 (D. Kan. Feb. 24, 2012).

34. *Id*. at *17.

35. 123 F. Supp. 3d 895, 908 (S.D. Tex. 2015).

36. *Id.* at 908–09.

37. No. C04-03843, 2007 WL 832937 (N.D. Cal. Mar. 19, 2007).

no showing that the computer devices to be inspected had a "special connection to the lawsuit."[38]

In *Areizaga v. ADW Corp*., the court noted that "'courts have permitted restrained and orderly computer forensic examinations where the moving party has demonstrated that its opponent has defaulted in its discovery obligations by unwillingness or failure to produce relevant information by more conventional means.'"[39] In this wage and hour case, the plaintiff discarded his personal laptop and smart phone. The court determined that the employer's "request to obtain a forensic image of Plaintiff's personal electronic devices was too attenuated and not proportional to the needs of the case at this time, when weighing [the employer's] explanation and showing as to what information it believed might be obtainable and might be relevant against the significant privacy and confidentiality concerns implicated by [the employer's] request—even with [the employer's] offer to pay all expenses and to use a third-party vendor who would restrict [the employer's] access to the substantive information of any user-created files and particularly data that appears to be of a personal nature that may be included in the proposed forensic image."[40]

Other courts have denied motions to compel while admonishing the party that the Federal Rules of Civil Procedure require a party to conduct a reasonable search of its files to determine whether it has responsive documents, stating that the parties should have a meaningful meet-and-confer session, and

38. *Id*. at *3–4.

39. No. 3:14-cv-2899-B, 2016 WL 9526396, at *3 (N.D. Tex. Aug. 1, 2016) (quoting NOLA Spice Designs, LLC v. Haydel Enters., Inc., No. Civ. A. 12-2515, 2013 WL 3974535, at *2–*3 (E.D. La. Aug. 2, 2013)).

40. *Id*.

telling a party that it "cannot meet its discovery obligations by 'sticking its head in the sand' and claiming ignorance."[41]

Tips for requesting parties

The case law cited above fails to provide any clear guidance––but some general principles can be mined from federal court decisions to date.

If a requesting party suspects that the producing party has failed to make a complete production, consider the following before filing a motion to compel:

- Did you make a specific request for the ESI or documents?
- If so, did the request seek relevant, nonprivileged documents or ESI?
- Was the request overly broad, unduly burdensome, or not proportional under the factors stated by Texas Rule of Civil Procedure 192.4 or Federal Rule of Civil Procedure 26(b)(1)?
- Have you conferred with the producing party and suggested search terms that it may wish to employ?
- What questions should you pose to deposition witnesses to support your position that all responsive documents have not been produced?
- Among the documents produced, do any of these documents or ESI support your position that other relevant documents exist but have not been produced?

41. E. Bridge Lofts Prop. Owners Ass'n, Inc. v. Crum & Forster Specialty Ins. Co., No. 2:14-CV-2567-RMG, 2015 WL 12831731, at *3 (D.S.C. June 18, 2015).

- Should you take the deposition of a corporate representative under Texas Rule of Civil Procedure 199.2 or Federal Rule of Civil Procedure 30(b)(6)?[42]
- Have you conferred and exhausted all good-faith efforts to resolve the dispute with opposing counsel pursuant to Federal Rule of Civil Procedure 37(a)?

Laying a factual predicate to support a motion to compel will be critical to achieving relief; conclusory statements that there must exist additional documents or ESI or speculation that such data exists will likely not suffice.

Tips for producing parties

- Ensure that you have complied with Federal Rule of Civil Procedure 26(g) or Texas Rule of Civil Procedure 191.2.

42. *See* Burnett v. Ford Motor Co., No. 3:13-CV-14207, 2015 WL 4137847, at *9 (S.D.W. Va. July 8, 2015) ("Contrary to Ford's contentions, discovery of document retention and disposition policies is not contingent upon a claim of spoliation or proof of discovery abuses, and may be accomplished through a Rule 30(b)(6) witness." Ford "has failed to supply any detailed information to support its position. Indeed, Ford has resisted sharing any specific facts regarding its collection of relevant and responsive materials. At the same time that Ford acknowledges the existence of variations in the search terms and processes used by its custodians, along with limitations in some of the searches, it refuses to expressly state the nature of the variations and limitations, instead asserting work product protection. Ford has cloaked the circumstances surrounding its document search and retrieval in secrecy, leading to skepticism about the thoroughness and accuracy of that process.").

- Consider carefully whether you may have unreasonably relied on your client to conduct the search for responsive documents.[43]
- Discuss with the requesting party why they believe other documents exist.
- Consider conferring with the requesting party about how the search for responsive documents was conducted.[44]
- Review the steps you have taken to validate the accuracy of your search and production (i.e., quality control).[45]

---

43. *See, e.g.*, Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents. Proper communication between a party and her lawyer will ensure (1) that all relevant information (or at least all sources of relevant information) is discovered, (2) that relevant information is retained on a continuing basis; and (3) that relevant non-privileged material is produced to the opposing party.").

44. Ruiz-Bueno v. Scott, No. 2:12-cv-0809, 2013 WL 6055402 (S.D. Ohio Nov. 15, 2013) (concluding that the plaintiff's concern about the lack of ESI appeared to be reasonably grounded and defendants were less than forthcoming with information about the discovery process, and ordering defendants to fully answer interrogatories and discuss in good faith what additional search methods should be undertaken).

45. The Sedona Conference, *Commentary on Defense of Process: Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process*, Principle 6, THE SEDONA CONFERENCE (Sept. 2016), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Defense%20of%20Process ("[V]alidating the results of an e-discovery process entails gaining a reasonable level of confidence that the process has resulted in a reasonably accurate, correct, and complete production, consistent with the responding party's legal obligations. As with other aspects of the e-discovery process, the effort undertaken to validate the results of a process should be proportionate to the expected benefits of that validation.").

- Keep in mind that a late production is better than being caught in a misrepresentation to the court.

Tips for Judges

When faced with arguments that a document production is incomplete, consider requiring the respondent to file a sworn statement confirming that it has no unproduced, responsive documents or ESI in its possession, custody, or control.[46] Although the Rule 26(g)(1) certification on a response generally should suffice, sometimes requiring a statement under penalty of perjury from a client representative with knowledge could be warranted and will avoid the expense and burden of further discovery on discovery or "meta-discovery."

And consider including in that sworn statement an explanation of the search and retrieval process that allowed the affiant to reach the conclusion that all responsive documents have been produced—but do so with caution where an argument can be made that this kind of disclosure could invade the work-product privilege.[47]

---

46. *See, e.g.*, Harper v. City of Dallas, Texas, No. 3:14-cv-2647, 2017 WL 3674830, at *16 (N.D. Tex. 2017); ORIX USA Corp. v. Armentrout, No. 3:16-mc-63, 2016 WL 4095603, at *6 (N.D. Tex. 2016); Desire, LLC v. Rainbow USA, Inc., No. CV154725DSFPLAX, 2016 WL 6106740, at *5 (C.D. Cal. June 29, 2016) ("Rainbow shall provide a declaration signed under penalty of perjury by a corporate officer or director attesting that it has not sold garments bearing the subject design since July 22, 2015, and that all relevant responsive documents and information have previously been provided.").

47. *See* Sean Grammel, *Protecting Search Terms as Opinion Work Product: Applying the Work Product Doctrine to Electronic Discovery*, 161 U. PA. L. REV. 2063, 2069 (2013) ("Attorneys develop search terms through an iterative process of assessing the case and gathering information. Lawyers review documents, interview witnesses or key players, and test search terms in a cyclical manner. Through this process, an attorney creates mental impressions about the case and decides which keywords best distill those impressions to produce

Conclusion

Courts should be disinclined to allow discovery on discovery or meta-discovery "in light of the dangers of extending the

---

relevant documents with high recall and precision."). For a sampling of cases where courts ordered a party to explain their search methodology see *In re Facebook Privacy Litig.*, No. 5:10-CV-02389-RMW, 2015 WL 3640518, at *2 (N.D. Cal. June 11, 2015) (requiring plaintiff to "submit a declaration explaining her search in detail, including, but not limited to, all sources searched and all search parameters used"); *Fleming v. Escort, Inc.*, No. 1:12-CV-066-BLW, 2014 WL 4853033, at *6 (D. Idaho Sept. 29, 2014) ("Although the allegations in this case cover events occurring more than 15 years ago, as well as events still occurring today, Escort has produced almost no e-mail in response to Fleming's 65 document requests and 12 interrogatories. Escort argues that its emails are privileged. But Escort has not filed a privilege log, and it is unbelievable that 15 years of emails are all privileged." "Recognizing this, Fleming asked Escort three simple questions: (1) What search terms did you use? (2) What computers or repositories did you search within? and (3) What was the time frame for your search? When Escort refused to provide an answer to these three simple questions, Fleming was forced to file this motion to compel. The Court will grant the motion. There is no way that Fleming—and this Court—can evaluate Escort's claim that it has produced everything unless Escort answers the three questions. This is especially true given Escort's fantastical claim that all the emails it discovered are privileged. Escort's stonewalling is yet another example of vexatious conduct by its counsel Gregory Ahrens and Brett Schatz."); *Alomari v. Ohio Dep't of Pub. Safety*, No. 2:11-CV-00613, 2013 WL 5874762, at *4 (S.D. Ohio Oct. 30, 2013) ("In the event that Defendants maintain that no further responsive documents exist, Defendants and/or Defense counsel are DIRECTED to set forth, in affidavits, the steps they took to locate and produce responsive documents. Defense counsel must execute an affidavit certifying that Defendants have completed a reasonable inquiry in locating and producing responsive documents and that all responsive documents of which they are aware have been produced. The affidavits must confirm that their efforts in locating responsive documents are complete. The Court concludes that full disclosure of Defendants' and Defense counsel's search efforts is necessary here for a number of reasons. First, Defendants have demonstrated a pattern of inexcusable delay and non-responsiveness throughout the discovery phase of this case.").

already costly and time-consuming discovery process ad infinitum."[48] Although no clear standard has emerged, the consensus view from the federal case law appears to dictate that a party should not be required to provide discovery about its production process without good cause.[49] At a minimum, a requesting party has the burden of demonstrating that the discovery response was inadequate.[50] Court decisions on what constitutes inadequacy range across a broad spectrum.[51]

We suggest that a standard as high as the Texas Supreme Court suggests may only encourage discovery abuse. We further suggest that a standard limiting discovery on discovery to instances of bad-faith misconduct or "unlawful withholding of documents"[52] is similarly under-inclusive. Although bad-faith misconduct may be informative on the issue of sanctions, the

48. Catlin v. Wal-Mart Stores, Inc., No. 0:15-cv-00004, 2016 WL 7974070 (D. Minn. Sept. 22, 2016).

49. Brewer v. BNSF Ry Co., No. CV-14-65, 2018 WL 88812 (D. Mont. Feb. 14, 2018).

50. *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 131 (2018).

51. The Sedona Conference, *Commentary on Defense of Process: Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process*, *supra* note 45, at 42–45 (collecting cases requiring some finding of non-compliance with discovery rules; a "material deficiency" in the responding party's discovery process; "bad faith" in the discovery production). There may exist differing standards being proposed even within the Sedona Conference. *See The Sedona Principles, Third Edition*, *supra* note 50, Comment 6.b. (discussing a "tangible, evidence-based indicia . . . of a material failure by the responding party to meet its obligations").

52. *See* Brand Energy & Infrastructure Services, Inc. v. Irex Corp., No. 16-2499, 2018 WL 806341 at *2 (E.D. Penn. Feb. 9, 2018) ("Without any showing of bad faith or unlawful withholding of documents . . . , requiring such discovery on discovery would unreasonably put the shoe on the other foot and require a producing party to go to herculean and costly lengths . . . .").

appropriate standards for purposes of a motion to compel are different. A meritorious motion to compel under Federal Rule of Civil Procedure 37(a) is meant to require a party to fully respond to a discovery request, although 100% accuracy has never been required. It is fundamentally different than sanctions under Federal Rule of Civil Procedure 37(c)(1), which address "sandbagging" or holding back evidence and on which courts assess the justification for the late disclosure and prejudice to the requesting party. A Rule 37(a) motion to compel is also fundamentally different than sanctions under Federal Rule of Civil Procedure 37(e), which involve failures to produce ESI that was required to be preserved and now is "lost." Under Rule 37(a), "courts have consistently held that they have the power to compel adequate answers [to discovery requests]."[53]

Courts are correct to deny discovery on discovery when a requesting party merely suspects or believes that a discovery production is not complete. There should be some showing of a specific deficiency in the other party's production.[54] In other words, a requesting party should make a showing that allows a court to make a reasonable deduction that other documents may exist or did exist and have been destroyed before being allowed meta-discovery.[55]

---

53. FED. R. CIV. P. 37 advisory committee's note (1970 Amendment).

54. *Brewer*, 2018 WL 88812 at *2.

55. Freedman v. Weatherford Int'l Ltd., No. 12 CIV. 2121 LAK JCF, 2014 WL 4547039, at *2 (S.D.N.Y. Sept. 12, 2014) ("In certain circumstances where a party makes some showing that a producing party's production has been incomplete, a court may order discovery designed to test the sufficiency of that party's discovery efforts in order to capture additional relevant material."); Orillaneda v. French Culinary Inst., No. 07 CIV. 3206 RJH HBP, 2011 WL 4375365, at *6 (S.D.N.Y. Sept. 19, 2011) ("Indeed, the search and maintenance of a party's information systems may be relevant when a party can 'point to the existence of additional responsive material' or when the docu-

The Texas Supreme Court appears to suggest that some limited meta-discovery may be allowable to determine if a producing party has met its discovery obligations. And no doubt alternatives other than across-the-board imaging and review of hard drives should be explored, but there is a real risk to the effectiveness of the discovery process if courts proceed from the background assumption that meta-discovery is to be discouraged or prohibited. This approach has expressly been rejected by The Sedona Conference. In its September 2016 *Commentary on Defense of Process*, Principle 12 recognizes that reasonable and proportional meta-discovery is sometimes appropriate (such as when testimony raises serious questions about the integrity of preservation and collection efforts).[56]

The goal of a lawsuit should be to secure the "just, speedy, and inexpensive determination" of the case.[57] In some cases, requiring the requesting party to expend additional efforts in the taking of depositions and propounding interrogatories about the discovery process may be unwarranted when it is readily apparent that discovery has been withheld. To require a requesting party, as the *In re Shipman* Court does, to demonstrate that the particularities of a producing party's electronic information storage methodology will allow retrieval of documents that have likely been withheld, and what that retrieval will entail, does not appear to comport with Rule 1.

---

ments already produced 'permit a reasonable deduction that other documents may exist or did exist and have been destroyed.'"); Hubbard v. Potter, 247 F.R.D. 27, 29 (D.D.C. Jan. 3, 2008) (relying upon Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 313 (S.D.N.Y. 2003)).

56. The Sedona Conference, *Commentary on Defense of Process: Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process*, *supra* note 45, Principle 12 at 44.

57. FED. R. CIV. P. 1.

A standard requiring good cause—that may generally be met with a showing of a "material deficiency" in production—coupled with an application of the proportionality factors that Federal Rule of Civil Procedure 26(b)(1) sets forth[58] appears to better achieve the goal of Rule 1, complies with the case law relying on responding parties to search their own records and produce documents, and should be considered for use by litigants and courts when meaningful meet-and-confer sessions fail to resolve a discovery dispute based on an allegedly incomplete production.

58. FED. R. CIV. P. 26(b)(1) ("Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.").

Moving the Law Forward in a Reasoned & Just Way