The Sedona Conference Journal®

Volume 17 ❖ 2016 ❖ Number One

Articles

The Sedona Conference®

Antitrust Law, Complex Litigation, and Intellectual Property Rights

The Sedona Conference Journal®

Volume 17

■

2016

Number 1

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 and by annual subscription to others ($95; $45 for conference participants and Working Group 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 or mbraman@sedona.net.

Cite items in this volume to "17 Sedona Conf. J. _____ (2016)."

Publisher's Note

Welcome to Volume 17, Number 1, of *The Sedona Conference Journal* (ISSN 1530-4981). The *Journal* contains commentaries prepared by our Working Groups, as well as articles originally presented at our conferences, over the past year. The Sedona Conference was founded in 1997 to provide a forum for advanced dialogue among the nation's leading attorneys, academics, and jurists on cutting-edge issues of law and policy in the areas of antitrust, intellectual property rights, and complex litigation. We host regular season conferences, international programmes, continuing legal education programs under The Sedona Conference Institute (TSCI) banner, and several Working Group meetings each year, providing unique and rewarding opportunities to explore the boundaries of various areas of the law with those who are pushing them. Volume 17, Number 1, of the *Journal* contains one article from our regular season conference on patent litigation (Fall 2015), along with four Working Group commentaries that have been published since the printing of *The Sedona Conference Journal,* Volume 16, in 2015.

We hope that you will find that the papers in this journal reflect the mix of theory and experience found at our conferences and Working Group meetings, including the creativity and constructive irreverence required to challenge traditional thinking. The views expressed herein are those of the authors, and we encourage the submission of counterpoint pieces. Submissions can be sent to comments@sedonaconference.org. If you are interested in participating in one of our regular season conferences, our TSCI programs, and our international programmes, or in joining our Working Group Series, please visit our website for further information (www.thesedonaconference.org).

Craig W. Weinlein
Executive Director
The Sedona Conference
June 2016

The Sedona Conference gratefully acknowledges the substantial contributions of its conference faculties, Working Group Series sustaining and annual sponsors, participants, members and observers, and our advisory board members, whose volunteer efforts and contributions make The Sedona Conference a "thought-provoking and inspiring" experience providing content of immediate benefit to the bench and bar.

The Sedona Conference Advisory Board

Joseph M. Alioto, Esq., Alioto Law Firm, San Francisco, CA

Kevin F. Brady, Esq., Redgrave LLP, Washington, DC

Elizabeth J. Cabraser, Esq., Lieff Cabraser Heimann & Bernstein, San Francisco, CA

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

The Hon. Justice Colin Campbell (ret.), Neeson Arbitration Chambers, Toronto, ON, Canada

The Hon. John L. Carroll (ret.), Cumberland School of Law, Samford University, Birmingham, AL

Joe Cecil, Ph.D., J.D., Federal Judicial Center, Washington, DC

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

Michael D. Hausfeld, Esq., Hausfeld LLP, Washington, DC

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

Hon. Katharine Sweeney Hayden, U.S. District Court, District of New Jersey, Newark, NJ

Ronald J. Hedges, Esq., Ronald J. Hedges LLC, Hackensack, NJ

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. Justice Gilles Letourneau (ret.), Ottawa, ON, Canada

The Hon. J. Thomas Marten, U. S. District Court, District of Kansas, Wichita, KS

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

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

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

The Hon. Kathleen M. O'Malley, Federal Circuit Court of Appeals, Washington, DC

Vance K. Opperman, Esq., Key Investment, Inc., Minneapolis, MN

The Hon. Andrew J. Peck, U.S. District Court, Southern District of New York, New York, NY

M. Laurence Popofsky, Esq., Orrick, Herrington & Sutcliffe LLP, San Francisco, CA

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

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

The Hon. Barbara Jacobs Rothstein, U.S. District Court, District of Columbia, Washington, DC

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, U.S. District Court, District of Colorado, Denver, CO

Daniel R. Shulman, Esq., Gray Plant Mooty, Minneapolis, MN

Robert G. Sterne, Esq., Sterne Kessler Goldstein & Fox P.L.L.C., Washington, DC

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

The Hon. Carl J. West (ret.), JAMS, Los Angeles, CA

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

THE SEDONA CONFERENCE COMMENTARY ON PRIVACY AND INFORMATION SECURITY: PRINCIPLES AND GUIDELINES FOR LAWYERS, LAW FIRMS, AND OTHER LEGAL SERVICE PROVIDERS*

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

Author: The Sedona Conference

Editor-in-Chief: David C. Shonka

Team Leader: Gina M. Trimarco

Drafting Team:

John E. Davis
Tara S. Emory
Jenny-Rebecca Lewis
Jeffrey W. McKenna
Kim Baldwin-Stried Reich
James A. Sherer
Joel Wuesthoff

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members 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 Sustaining 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.

PREFACE

Welcome to the final, November 2015, version of The Sedona Conference *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). The Sedona Conference is a 501(c)(3) research and educational institute that exists to allow leading jurists, lawyers, experts, academics, and others, at the cutting edge of issues in the areas of antitrust law, complex litigation, and intellectual property rights, to come together in conferences and mini-think tanks called Working Groups to engage in true dialogue, not debate, in an effort to move the law forward in a reasoned and just way.

The public comment version of The Sedona Conference *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers* was published in July of this year after more than two years of dialogue, review, and revision, including discussion at several working group meetings. After a sixty day public comment period, during which The Sedona Conference sponsored a public webinar on the Commentary, the editors reviewed the comments received as well as the law and made minor revisions in the wording of Principles 1, 2, 4, and 7 to clarify their meaning. Additionally, minor revisions were made to the comments to the Principles, including some paragraph reorganization. I thank all of the drafting team members for their dedication and contribution to this project. Team members that participated and deserve recognition for their work are: John E. Davis, Tara S. Emory, Jenny-Rebecca Lewis, Jeffrey W. McKenna, Kim Baldwin-Stried Reich, James A. Sherer, and Joel Wuesthoff. Finally, The Sedona Conference thanks Gina M. Trimarco for serving as the Team Leader and David C. Shonka for serving as the Editor-in-Chief.

We hope our efforts will be of immediate and practical assistance to judges, parties in litigation and their lawyers, and database management professionals. We continue to welcome comments for consideration in future updates. If you wish to submit feedback, please email us at comments@sedonaconference.org. 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
November 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Sedona Conference Working Group 1, through its drafting team on Privacy and Information Security, has developed Principles and Guidelines for lawyers, law firms, and other legal service providers. Advances in technology, communications, data storage, and transmission have produced immeasurable societal benefits. However, they have also created unforeseen risks to individual privacy and the security of information that lawyers gather and hold while representing their clients, whether in litigation, in business transactions, or through personal counseling. Personal identities, privacy, confidential client information, work product, and even attorney-client communications have never been more vulnerable to unauthorized disclosures, breaches, loss, or theft than they are today. Yet, the responsibility of all legal service providers to protect such information has not changed. The applicable standards of conduct do not depend on the size or resources of the professional who holds such information.

We recognize, however, that effective privacy and information security does not allow for a one-size-fits-all solution. The nature of the information, the needs of the client, the circumstances in which the information is held, and other factors affect the methods that a reasonably prudent legal service provider should adopt to protect confidential and private information entrusted to its care. In the end, perfect security practices are not required. What is required are well thought-out policies and practices that are both reasonable and appropriate to the circumstances. This Commentary is intended to help all legal service providers—solo practitioners, large law firms, and legal support entities—determine which policies and practices are best suited for each unique situation.

We have divided this Commentary into several discrete sections. Following a brief Introduction and statement of Principles in Section I, Section II identifies some of the major sources of a provider's duty to protect private and confidential information. Section III then describes a process by which legal service providers may conduct thorough security risk assessments, taking into account the information they possess, the vulnerability of that information to unauthorized disclosures, breaches, loss, or theft, and the way in which each provider may mitigate those threats by adopting a structured or layered approach to protect private and confidential information. Finally, Section IV delves into various policies and practices that can address privacy and information security, setting forth processes that can be scaled to the needs and circumstances of an individual legal service provider.

We think the Principles set out in this Commentary provide guidance in protecting private and confidential information. Nonetheless, we recognize that as technology continues to evolve, people will develop new and presently unimagined methods of creating, storing, transmitting, protecting, and even stealing private and confidential information. This of course means that we must all keep Principle 7 below firmly in mind: Legal service providers should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

The principles that inform this Commentary are:

Principle 1: Legal service providers should develop and maintain appropriate knowledge of applicable legal authority including statutes, regulations, rules, and contractual obligations in order to identify, protect, and secure private and confidential information.

Principle 2: Legal service providers should periodically conduct a risk assessment of information within their possession, custody, or control that considers its sensitivity, vulnerability, and the harm that would result from its loss or disclosure.

Principle 3: After completing a risk assessment, legal service providers should develop and implement reasonable and appropriate policies and practices to mitigate the risks identified in the risk assessment.

Principle 4: Legal service providers' policies and practices should address privacy and security in reasonably foreseeable circumstances, and reasonably anticipate the possibility of an unauthorized disclosure, breach, loss, or theft of private or confidential information.

Principle 5: Legal service providers' privacy and information security policies and practices should apply to, and include, regular training for their officers, managers, employees, and relevant contractors.

Principle 6: Legal service providers should monitor their practices for compliance with privacy and security policies.

Principle 7: Legal service providers should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

I. INTRODUCTION AND INFORMATION SECURITY PRINCIPLES

Legal service providers ("LSPs") as well as other professionals[1] rely on communications technology and the rapid, secure sharing of information to conduct business in modern form. The creation and use of electronic information has not only modified business generally, but has also dramatically changed the legal services industry. From the development of international information networks to remote data access and electronic court submissions, technology and law are now integrated, with both positive and negative consequences.

As with all technology, the benefits of an integrated legal practice do not come without new obligations. The new technologies that have transformed the legal industry also threaten privacy, information security, and even the confidentiality of attorney-client communications in ways that were unimaginable a few years ago. This Commentary responds to these challenges with a framework for addressing information privacy and security concerns in the legal industry, and recommends basic steps that all LSPs and Third-Party Service Providers

---

1. As used herein, the term "Legal Service Provider" ("LSP" or "provider") includes lawyers, law firms, and any other person or entity directly engaged in providing legal advice and counsel, and the term "Third-Party Service Provider" ("TPSP") includes the other professionals and organizations who play an integral part in the provision of legal services, such as auditors, outside experts, consultants, and eDiscovery service providers. The term "Legal Services Industry" ("LSI") refers to both LSPs and TPSPs.

Also, as used herein, the term "private information" should be understood broadly to include not just personally identifiable information ("PII"), such as names, addresses, account numbers, and so forth, but also any information about a person that can individually identify them. The term "confidential information" should similarly be understood broadly to include any non-public information about a company or a financial interest whether personally identifiable or not. Questions about the relative sensitivity of various types of private and confidential information are not considered in this Commentary.

("TPSPs") should consider to safeguard the private and confidential information they maintain on behalf of their clients, third parties, and their own organization.

Although societal concerns about privacy and information security have been with us since the days of paper, recent developments in information technology have resulted in new government regulations and oversight, particularly in the health care and financial services industries. The legal profession interacts directly with these industries and, accordingly, this Commentary includes Appendices that highlight the regulations to which both the health care and financial services industries are now subject. Ethical rules, statutes, regulations, and the common law all impose duties on lawyers, and less directly, on much of the legal services industry, to safeguard private and confidential information belonging to clients and third parties. Contracts or retainer agreements may also contain requirements about the safekeeping and handling of confidential information. This Commentary provides some additional steps for both prospective and remedial measures that LSPs should consider.[2]

The discussion in this Commentary is informed by the following guiding principles:

---

2. This Commentary does not address the treatment of confidential information that becomes part of the court record during litigation. That subject was thoroughly treated in *The Sedona Guidelines: Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases*, THE SEDONA CONFERENCE (2007), *available at* https://thesedonaconference.org/download-pub/478. Although that publication is not recent, its observations about the use of protective orders and sealing orders to shield confidential information are still valid, including the balancing tests employed in each situation. However, one may argue that the weight given the potential impact of disclosure of sensitive personal information should be updated in light of the public's greater awareness today about the harm that may result from such disclosure.

Principle 1: Legal service providers should develop and maintain appropriate knowledge of applicable legal authority including statutes, regulations, rules, and contractual obligations in order to identify, protect, and secure private and confidential information.

Comment 1a: Clients and, sometimes, third parties entrust LSPs with private and confidential information, often in electronic form. Electronically stored information is often at risk of loss or unauthorized access because it is mobile, may be accessed remotely, is easily copied (and corrupted), and can involve large volumes of data. LSPs should reasonably protect such private and confidential information while it is in their possession, custody, or control through measures that reasonably guard all the channels through which that data may be accessed. In some circumstances, failure to take reasonable and appropriate steps to protect private and confidential information may expose an LSP to claims for breach of an attorney's professional/ethical obligations to maintain confidentiality of information related to the representation or for violation of various statutory, regulatory, contractual, or common law obligations imposed on the LSP or its client.

Comment 1b: Perfect protection of client data is not possible, practical, or required. LSPs must take reasonable and appropriate measures to protect data, considering factors such as the nature of the data, the risk of unauthorized access, requirements imposed by the client, applicable legal rules, and the costs associated with protecting the data.

Comment 1c: LSPs can take reasonable and appropriate steps to protect and secure private and confidential information by understanding applicable requirements for such information. These requirements arise from many sources, including ethical rules, federal and state statutes and regulations, state common

law, foreign laws, court rules, and contractual requirements. Different levels of protection may be required for information based on many factors, such as the sensitivity of the information, where and how it is stored, and the purpose for which data is entrusted to another party.

Principle 2: Legal service providers should periodically conduct a risk assessment of information within their possession, custody, or control that considers its sensitivity, vulnerability, and the harm that would result from its loss or disclosure.

Comment 2a: The policies and practices employed by an LSP to protect client and third-party private and confidential information will reasonably vary based on the technology at issue and the information to be protected. Each LSP should consider developing a security plan tailored to meet the individual needs of the LSP's information practices, including storage locations, employees, work practices, IT infrastructure, and client security policies, to name a few.

Comment 2b: The following steps can help LSPs create a reasonable and adequate security plan:

- Identify and evaluate the sensitivity of the various types of information within the LSP's possession, custody, or control, and the potential harm that would result from unauthorized disclosure, breach, loss, or theft of that information.
- Identify specific threats and vulnerabilities that could result in unauthorized disclosure, breach, loss, theft, alteration, or unavailability.
- Assess the risk of harm posed by each threat or vulnerability.

The LSP should also consider the integrity, level of sensitivity, and accessibility of private and confidential information. The goal is to keep private and confidential information

free from corruption, accessible only to those who need to use it, and readily accessible when needed.

Principle 3: After completing a risk assessment, legal service providers should develop and implement reasonable and appropriate policies and practices to mitigate the risks identified in the risk assessment.

Comment 3a: After completing a risk assessment of the information in its possession, custody, or control, each LSP should develop and implement a scaled and prioritized plan to protect private and confidential information. This plan should factor in and respond to the sensitivity of different types of information. The plan should also respond to the threats and vulnerabilities identified in the risk assessment and minimize the risks that would result in unauthorized disclosures, breaches, loss, or theft. The policies and practices should also reasonably respond to client-created data privacy and security requirements while enabling the LSP to meet its day-to-day business needs.

In this regard, larger LSPs should consider hiring an information security director or officer and put together a committee with representatives from all interested groups to develop the LSP's policies and practices for accessing information security. Larger LSPs may also consider hiring a separate privacy officer to address specific privacy concerns. Smaller LSPs may wish to hire a consultant to address both information security and privacy and assist in creating the LSP's policies and practices in this area. In the end, what may be most important is that there be a senior level person who has oversight over all parts of the entity, has sufficient expertise to know what needs to be done, has the authority to implement and enforce the plan the LSP develops, and who is held accountable for the success or failure of information security.

Comment 3b: Effective information security practices are an entity-wide concern. The policies should be implemented and enforced systematically from the top to the bottom within the organization, across all departments and units, and among all employees and contractors. An otherwise solid policy can be rendered useless if sound practices in one part of an organization are accompanied by lax practices in another part.

Principle 4: Legal service providers' policies and practices should address privacy and security in reasonably foreseeable circumstances, and reasonably anticipate the possibility of an unauthorized disclosure, breach, loss, or theft of private or confidential information.

Comment 4a: Information technology is complex. Reasonable policies and practices should address the privacy and security of information inside and outside the office environment, while stored, in transit, or accessed remotely. Policies should also address how and when information is shared with third parties, such as outside experts, consultants, TPSPs, co-counsel, adversaries, and courts. LSPs may store confidential information on numerous IT platforms, devices, and media in different locations, some of which may be operated by, or accessible to, third parties such as cloud service providers and their personnel. Confidential information is also routinely transmitted between these platforms and devices. The methods for protecting confidential information while in transit and in storage are as diverse as the threats to the security of such information.

Comment 4b: Accordingly, LSPs should design reasonable policies and practices to address privacy and security in relevant contexts. At a minimum, good policies and practices will: (1) limit access to confidential information to those with a bona fide role-based need for access; (2) provide for physical security; (3) implement information access controls (e.g., multiple factor

authentication, attribute-based access control); (4) consider intrusion detection and prevention technologies; (5) employ appropriate use of encryption technologies; (6) provide for secure back-up/disaster recovery; and (7) ensure the prompt disposition of information that is no longer needed (and hence at risk of theft with no offsetting potential benefit). Most important, LSPs should implement good policies and practices regarding the handling of client and third-party private and confidential information.

Comment 4c: The plan should include a clear incident response procedure to address the unauthorized disclosure, breach, loss, or theft of private and confidential information. The incident response program should include procedures for: (1) reporting each incident to a designated person responsible for implementing the LSP's response plan; (2) identifying the source of the breach; (3) undertaking steps to stop the breach; (4) investigating the extent of any loss or compromise of private or confidential information; (5) providing appropriate notice to the client, relevant law enforcement authorities, and insurers, as necessary; and (6) abiding by applicable data breach notification requirements.

Principle 5: Legal service providers' privacy and information security policies and practices should apply to, and include, regular training for their officers, managers, employees, and relevant contractors.

Comment 5a: Human beings are the weakest link in any information, privacy, or security program. Therefore, a well-designed program to protect private and confidential information will contain robust provisions for training in protecting information. Training that is relevant to recipients should focus on the types of information, legal requirements, and threats that apply to the information the recipient handles, including the

common techniques that data thieves use to gain access to information through deception. Experience has shown that the best and most effective training sessions are interactive and involve testing to confirm that the recipient understands the material. Accordingly, LSPs should seek to conduct or sponsor formal training at regular intervals (ideally annually) for all personnel.

Comment 5b: In addition to formal training, LSPs should institute regular reminders, warnings, tips, and updates to personnel, in order to ensure timely dissemination of information about new rules or threats applicable to the information held by the LSP. The best security practices appear to be those in which LSPs foster a culture and environment in which everyone is vigilant and aware of what is required in order to maintain security, both individually and across the organization.

Principle 6: Legal service providers should monitor their practices for compliance with privacy and security policies.

Comment 6a: Security breaches can come from many sources, internal or external. The cause may be intentional, negligent, or even "benign" (e.g., a hardware malfunction). And they may occur at any time. Also, once they occur, the damage they cause may spread and multiply with incredible speed. Accordingly, to minimize the likelihood of any breach and to mitigate its consequences, LSPs need to be vigilant. Careful real-time monitoring of employee practices can help ensure compliance with the LSP's privacy and security policies and better safeguard information both within an organization and in the hands of any contractor or other third party.

Comment 6b: Organizations differ, often substantially, in size, scope, the nature of the data retained or transferred, and attendant threats, both internal and external. Accordingly, each LSP should establish a mechanism for assessing the various components of its information security environment, program,

and policies, including those relating to physical security, information access controls, intrusion prevention and detection systems, encryption technologies, and the maintenance, transfer, and disposition of information. For some providers, such monitoring may be relatively simple and straightforward. Others may need to employ, depending on their industry or situation specific requirements, standard auditing frameworks, such as SSAE 16 (formerly SAS), the ISO 27000 series standards, or a framework capable of being measured, assessed, and improved with demonstrable and documented criteria and according to a fixed schedule. Of course, as technology changes, so will these lists.

Comment 6c: Ultimately, an organization is responsible for the confidentiality, integrity, and availability of information under its possession, custody, or control. Implementing a reasonable auditing regime that evaluates policies and procedures governing its information assets and properties demonstrates a reasonable and prudent management philosophy to address a complex and evolving field.

Principle 7: Legal service providers should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

Comment 7a: Threats to security and privacy change constantly. The compliance landscape, arising from industry-specific, state, and federal requirements, or obligations that affect the creation, management, transfer, or disposition of information in non-U.S. jurisdictions, challenges organizations at every level. These factors, coupled with constantly evolving technologies, require ongoing vigilance to ensure that the LSP's privacy and security policies and practices remain responsive to changing circumstances.

Comment 7b: To be "reasonable and appropriate," security policies and practices should be current; and the best way to keep them current is to stay abreast of developments, reassess risks, and update the policies and practices as needed. This suggests a need to perform two tasks in tandem: (1) conduct *ad hoc* assessments based on active monitoring of the LSP's actual real-time or near real-time practices; and (2) undertake regularly scheduled (ideally annually) reviews of technological developments that may concern the LSP's current internal practices or supported programs. *Ad hoc* assessments are proactive measures undertaken by, or under the direction of, the person who is responsible for implementing and enforcing the LSP's security policies and practices.

Comment 7c: The person responsible for *ad hoc* assessments must be qualified to do the job directly, or have the authority and budget to engage expert consultants to perform the assessment. Additionally, that person should have the authority to effect change directly to reasonably address any identified defects in the policies or practices. To minimize the possibility of missing important developments, LSPs need to follow-up its assessments with regularly scheduled reviews of the entire security program and, where necessary, update the policies and practices as risks and best practices evolve.

II. SOURCES OF THE DUTY TO PROTECT PRIVATE AND CONFIDENTIAL INFORMATION[3]

The duty to protect privacy applies to all participants in the legal services industry. The principal sources of the duty are found in: (1) ethical rules applicable to attorneys; (2) federal and state statutes and regulations; (3) foreign laws, where applicable; (4) common law; and (5) client choices, including contractual obligations imposed by the client.[4]

A. Ethical Rules Applicable to Attorneys

1. Model Rules 1.1, 1.6, and 1.18

ABA Model Rules of Professional Conduct 1.1 and 1.6 require attorneys using technology to take competent and reasonable measures to safeguard client information. This duty extends to the use of all technology, including computers, mobile devices, networks, technology outsourcing, and cloud computing.

Rule 1.1 requires "[a] lawyer [to] provide competent representation to a client." This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." It includes competence in selecting and using technology. In August 2012, the ABA House of Delegates added a

3. Unless otherwise expressly stated in this Commentary, the term "information" includes both electronically stored information ("ESI"), as well as information in paper or hard-copy form.

4. This Commentary is not intended to establish a "duty of care" imposed upon LSPs. Rather, it is designed to identify issues relating to the protection of client and third-party private and confidential data and, most important, articulate practices that should be considered in protecting such data. To that end the technology and threats in this area are constantly changing. LSPs should adapt their practices to safeguard private and confidential information of their clients and third parties taking into account the evolving technologies and threats.

comment to Rule 1.1 that imposes an additional professional competency responsibility to keep "abreast of changes in the benefits and risks associated with relevant technology" as the changes relate to the law and to legal practice.

Attorneys' use of technology presents special ethical challenges in these areas of competence and confidentiality. The duty of competence requires attorneys to know what technology they need and how to use it. If an attorney lacks the necessary technical competence for security, he or she must consult with someone who has the requisite expertise.

ABA Model Rule 1.6 regarding client confidential information is one of the most challenging ethical responsibilities when it comes to technology. All fifty states and the District of Columbia have an ethical rule prohibiting (subject to certain exceptions) a lawyer from revealing information related to the representation of a client unless the client provides informed consent. The ABA's Comments to Rule 1.6 specifically address a lawyer's obligation to preserve confidentiality, requiring lawyers to act competently to safeguard information relating to the representation of a client. Lawyers have the same duty to safeguard the confidential information of prospective clients, per Rule 1.18.

Twenty-nine states and the District of Columbia have issued comments to Rule 1.6 requiring that attorneys take "reasonable precautions" to prevent unauthorized access to client communications. The comments provide that attorneys generally do not need to take "special security measures if the communication affords a reasonable expectation of privacy," but note that special circumstances may warrant special precautions. Relevant factors include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or a confidentiality agreement. However, many states have issued separate ethics opinions based either upon

Rule 1.1 or state versions of that Rule, in addition to other Model Rules discussed below. These ethics opinions often introduce additional requirements—such as suggesting the type of contractual terms required between a lawyer and cloud service provider, or the types of background investigations that lawyers should require of their cloud providers—as preconditions for ethically arranging to store client information in the cloud. The ABA maintains an online chart listing these opinions.[5]

2. Model Rules 4.4 (a) – (b)

Lawyers also have a duty to protect the confidential information of third parties, including adversaries. Model Rule 4.4 (a) provides that, in representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or knowingly use methods of obtaining evidence that violate the legal rights of such a person, including privacy rights. Rule 4.4 (b) relatedly requires a lawyer to notify the sender if he or she receives a document or electronically stored information relating to the representation of the sending lawyer's client and if he or she knows or reasonably should know that the document was inadvertently sent.

3. Model Rules 5.1, 5.3, and 5.7

Lawyers are responsible for the professionals they hire and should have reasonable checks in place to ensure confidentiality and good hiring practices. Model Rules 5.1 and 5.3 incorporate into the lawyer's professional obligations the duty to supervise the work of subordinate attorneys and non-attorneys, agents, and TPSPs, including those outside the firm. Those rules

5. *See Status of State Review of Professional Conduct Rules*, AMERICAN BAR ASSOCIATION (Sept. 14, 2011), http://www.americanbar.org/content/dam/aba/migrated/cpr/pic/ethics_2000_status_chart.authcheckdam.pdf.

require lawyers with managerial responsibilities to make reasonable efforts to ensure that those working for them act in a manner compatible with the professional obligations of the lawyer. Model Rule 5.7 further extends the lawyer's professional responsibilities to apply to law-related services.

Comment 3 to Model Rule 5.3 expressly refers to a lawyer's use of outside technology services[6] and cautions that the degree of due diligence required to vet and supervise these contractors "will depend upon the circumstances, including the education, experience, and reputation of the non-lawyer, the nature of the services involved, the terms of any arrangements concerning the protection of client information, and the legal and ethical environments of the jurisdictions in which the services are performed, particularly with regard to confidentiality."[7] The state ethics opinions that address the use of cloud services to store client information are not entirely consistent with each other.[8] Lawyers with multi-state practices will be subject to the ethical standards of every state in which they practice. For those lawyers using cloud services for storage of client information, no ethics opinion has yet addressed whether the laws and legal ethics standards of the jurisdiction in which the cloud

6. *See* ABA MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. (2013), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/comment_on_rule_5_3.html.

7. *See* ABA Comm'n on Ethics 20/20, *Report to the House of Delegates Resolution 105C*, AMERICAN BAR ASSOCIATION, http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.authcheckdam.pdf (last visited June 2, 2015).

8. *See Cloud Ethics Opinions Around the U.S.*, ABA LEGAL TECHNOLOGY RESOURCE CENTER, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited June 2, 2015). A detailed comparison of these different state ethics opinions is beyond the scope of this paper.

provider's servers are located, also apply to the "foreign" lawyer who arranges for the cloud storage service.[9] Finally, U.S. government attorneys are "subject to State laws and rules, and local Federal court rules, governing attorneys in each State where such attorney engages in that attorney's duties, to the same extent and in the same manner as other attorneys in that State."[10]

B. Federal Statutory Obligations

The U.S. has taken a sectoral approach to privacy issues, which adjusts protections to particular circumstances and regulatory regimens.[11] A comprehensive discussion of all sectoral requirements is beyond the scope of this Commentary. However,

---

9. The laws of non-U.S. jurisdictions where cloud servers are located might also govern the precautions required for protecting client data. A practitioner should carefully consider and discuss with the client the advantages and disadvantages of storing data outside of the client's home state, as well as outside of the U.S. Even aside from the likelihood of different legal and ethical standards applying outside of the U.S., in some non-U.S. jurisdictions where servers might be located, there could be no effective legal protections at all, subjecting client data to the risk of sale to the highest bidder by the cloud service provider, by corrupt employees, or by officials.

10. McDade Act, 28 U.S.C. § 530B(a) (2012), https://www.law.cornell.edu/uscode/text/28/530B (last visited June 2, 2015) ("Ethical standards for attorneys for the Government").

11. A reference to a few of the federal statutes implicating privacy suggests the range and variety of ways in which the federal government addresses the issue:

- Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510
- Driver's Privacy Protection Act (DPPA), 18 U.S.C. §§ 2721–25
- Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681
- Fair Debt Collections Practices Act (FDCPA), 15 U.S.C. §§ 1692–92
- Financial Services Modernization Act (GLBA), 15 U.S. Code §§ 6801–10

the laws and regulations that govern two particular industries, health care and financial services, are worthy of mention because they serve as useful models. Both industries operate within a regulated framework that: (1) imposes security standards on industry members; (2) requires special service contracts between those who collect information from consumers and those who provide services to them; (3) requires notification to consumers when security lapses result in the loss of information pertaining to a non *de minimis* number of consumers; and (4) subjects those who lose data to potential legal liability. It is also worth examining the laws and regulations applicable to these two industries because most LSPs will handle financial or health related information in the course of providing legal services, so it is important to understand the restrictions applicable to such information. Therefore, a brief discussion of the privacy regulations that govern those two industries is included in Appendices A and B.

C. State Regulations

The unauthorized disclosure of personal information may trigger state data breach laws that require notifying consumers, governmental agencies, or both. A data breach may also result in regulatory investigations and penalties. Indeed, many

---

- Health Insurance Portability and Accountability Act (HIPAA), 42 U.S. Code § 300gg
- Stored Communications Act (SCA), 18 U.S.C. § 2701
- Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710

Although it is not exhaustive, this list illustrates the U.S. patchwork of federal privacy laws that imposes different sets of duties. In addition, there are literally "[t]ens of thousands of record retention legal requirements" that are imposed by "the federal government, the fifty states, the District of Columbia, and the U.S. territories." Many of these implicate privacy issues. Peter Sloan, *The Compliance Case for Information Governance*, 20 RICH. J.L. & TECH. 4, ¶ 8 (2014), *available at* http://jolt.richmond.edu/v20i2/article4.pdf.

data breach laws require that notice be provided to the state Attorney General.

Nearly all states, the District of Columbia, Puerto Rico, and the Virgin Islands require notice to their residents in the event a resident's personally identifiable information (PII) is breached. Most of these laws have a "risk of harm" trigger, requiring notice only if it is determined, after a reasonable investigation, that there is a reasonable likelihood of harm to consumers. However, some states, including California and Massachusetts, do not limit the notice requirement in this way.

Apart from the broad definition of PII used in this Commentary (*see supra* note 1), the definition of PII varies among the states and territories, but generally includes a resident's first or last name, combined with one nonpublic identifier, such as a social security number, state ID, driver's license number, credit card number, or bank account number. The majority of these laws are limited to electronic information, but at least six states (Alaska, Hawaii, Indiana, Massachusetts, North Carolina, and Wisconsin) apply the laws to paper records as well.[12]

Some state laws also impose minimum security requirements, including requirements for a written information security program (commonly known as a WISP), and for encryption of personal information that will travel across public networks, be transmitted wirelessly, or be stored on laptops or other portable devices.

LSPs should develop an incident response plan that addresses their potential duties, and be knowledgeable about applicable laws, considering, for example, that these laws may

12. This is a very active area of state-level legislation. Many states are actively enacting and revising these laws, and LSPs therefore need to stay on top of developments. *See, e.g.*, Florida Information Protection Act of 2014 (FIPA) (2014), http://laws.flrules.org/2014/189.

apply to a client's information that is stored on the LSP's network or a cloud provider's network, even if the client and lawyer do not have any other contacts with the state.

D. Foreign Statutory and Regulatory Requirements

International privacy is a dynamic area of the law in which consumers, private entities, and government actors seek to balance the considerable benefits of technological innovations with critical privacy concerns. Disclosures of national security inquiries—the "Snowden effect"—and other large-scale data breaches have forced privacy issues into the forefront and instigated unprecedented activity in the development of data protection regulation. These developments will profoundly affect the way global businesses and their LSPs approach the collection and management of personal information.

The state of the law in the European Union (EU) is in flux even as this Commentary is being completed; and the impending adoption of a new EU data protection regulation will fundamentally change the existing EU framework. On March 12th, 2014, the European Parliament voted to continue revising and strengthening the draft regulation. Among other things, the proposal: (1) implements new protections concerning the transfer of EU citizens' information to non-EU countries; (2) significantly increases the potential fines to corporations in breach of the regulation; (3) guarantees the right to be forgotten; (4) incorporates the theme of information "portability" to support greater control by individuals; (5) unifies inconsistent and diverse nation-specific laws into one "pan European" data protection law; and (6) mandates incorporation of privacy by design into products and services. The General Data Protection Regulation will next be considered by the Council of Europe, which consists of representatives of twenty-eight EU governments.

They are tasked with considering and ultimately, in negotiations with the EU Parliament, agreeing to a single set of proposals.

Equally significant, stronger cross-border privacy rules are also being developed in Latin America and Asia. Countries as diverse as Costa Rica, Brazil, South Korea, Hong Kong, and Singapore have recently adopted, or are considering adopting, broad-based data privacy laws. Canada is also considering significant new privacy legislation.

E. Common Law Liability

A discussion of all potential theories of common law liability for data breaches is beyond the scope of this Commentary. Nonetheless, a few are worth highlighting; these include: (1) legal malpractice; (2) breach of fiduciary duty; (3) breach of contract; and (4) general tort, including class action negligence claims.[13] For example, an LSP who loses a client's confidential information may not only be accused of breaching his or her ethical obligations, but may also be subject to claims of legal malpractice and breach of contractual duty (express or implied) to safeguard client information. Similarly, third parties whose identities are stolen or who are otherwise injured by a loss of sensitive personal information may seek legal redress for their injuries. One need only consider the class actions that have followed major data breaches to appreciate the business case for taking adequate steps to secure sensitive information, no matter whose information it is.

---

13. One study "identified over 86 unique causes of action" from a universe of 231 cases. *See* Sasha Romanosky et. al., *Empirical Analysis of Data Breach Litigation* (Apr. 6, 2013) at 25, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461 (Forthcoming in the Journal of Empirical Legal Studies; Temple University Legal Studies Research Paper No. 2012-30).

F. Client Choices

A broad range of information security decisions may be left to the client's business judgment. The client always has the discretion to make business decisions about which providers to engage based upon risk assessment of the providers' information security. Although the client ultimately pays for the security measures, it is not the only one who is potentially liable for any loss of third-party information.

When counseling clients about security alternatives, the LSP should document any advice and ensure that the client has access to technology experts. Upon request from the client, the LSP should clearly disclose the nature of the security measures and policies of the firm. Any decision by the client to forego security measures that the LSP recommends should be documented. In addition, the LSP should, when appropriate, counsel the client about potential liability insurance coverage issues and be mindful that in some situations (especially those that may expose the LSP to third-party lawsuits) the LSP should consider whether to decline to provide representation.

III. CONDUCTING A SECURITY RISK ASSESSMENT

The touchstone of a sound information privacy and security program is its careful tailoring and scaling to the LSP and its practice. This tailored approach begins with an assessment of risk, considering both the probability and the harm or damage that could be caused by an occurrence.[14] LSPs should determine what privacy and security solutions are appropriate to the circumstances using a risk-based analysis,[15] and subsequently develop and implement a reasonable and appropriate information privacy and security program to mitigate risks.

The Homeland Security Act refers to "information security" as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: A. Confidentiality, B. Integrity, and C. Availability."[16] Thus, to properly assess the risk, an LSP must consider the importance of maintaining the confidentiality, integrity, and availability ("CIA") of the information it possesses.[17] By these terms we mean:

- Confidentiality: protecting the information from disclosure to unauthorized parties;

---

14. *See* National Institute of Standards in Technology, Special Publication 800-30, *Guide for Conducting Risk Assessments*, NIST (Sept. 2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [hereinafter *Guide for Conducting Risk Assessments*].

15. Valerie Fontaine, *The New Lawyer - What size fits me?*, DAILY JOURNAL, Nov. 26, 2013, https://www.dailyjournal.com/public/Pubmain.cfm?seloption=The%20New%20Lawyer&pubdate=2013-11-26&shNewsType=Supplement&NewsId=965&sdivId=&screenHt=680&eid=932352.

16. 44 U.S.C. § 3542(b)(1) (2012), https://www.law.cornell.edu/uscode/text/44/3542 (last visited June 2, 2015).

17. For a more detailed look at how each of these components can be considered and evaluated, *see infra* Table 1 in Section III.C.

- Integrity: protecting information from being modified by unauthorized parties; and
- Availability: ensuring that authorized parties are able to access the information when necessary.

Absent an intentional alteration, information an LSP has on hand should, at all times, be the same information that it either generated or received. If it is private or confidential information, it should be protected from those who do not need to see or use it. Those who must use it, must be able to obtain it quickly whenever they need it.

In security terminology, the basic elements common to almost every risk assessment are:

- Asset Identification and Evaluation: Identify assets and evaluate their properties.
- Risk Profiling and Assessment: Analyze the specific threats and vulnerabilities that pose the greatest risk to information assets.
- Risk Mitigation and Treatment: Develop reasonable responses to the threats and vulnerabilities identified. The practices discussed in Section IV of this Commentary provide a guide for such risk mitigation efforts.

A. Asset Identification and Evaluation

During this first stage, the LSP should identify the types of information it handles generally or will handle in conjunction with a specific representation (e.g., social security numbers, payment card numbers, patient records, designs, and human resources data), evaluate the sensitivity or relative importance of each type of information, and rank by priority which types require protection.

In identifying information assets and developing priorities, LSPs should do the following:

- Consider the sources and nature of the information, along with where it resides or will reside. This may include data created by the LSP and client-created data stored by the LSP—both of which may have different security concerns and security requirements.
- Identify and list where each item on the information asset list resides or will reside within the organization (e.g., file servers, workstations, laptops, removable media, PDAs, phones, databases). If information will be stored outside the organization (such as with a cloud service provider), the LSP should note that as well.
- Categorize information and rank each category based on its degree of sensitivity and risk. For example, an LSP might decide to categorize its information and rank it as follows:
    1. Public information, either belonging to the LSP itself or a client (e.g., marketing campaigns, contact information, public financial reports, etc.)
    2. Internal, but not secret, information belonging to the LSP (e.g., phone lists, organizational charts, office policies, etc.)
    3. Sensitive internal information belonging to the LSP (e.g., business plans, client lists, strategic initiatives, items subject to non-disclosure agreements, etc.)
    4. Confidential client information subject to the attorney-client privilege or work-product protection

5. Regulated information belonging to the LSP or its client (e.g., patient data, classified information, etc.)
6. Compartmentalized internal information belonging to the client or the LSP (e.g., compensation information, certain highly sensitive client information that is not to be generally accessible to all of the LSP's personnel, HR data, etc.)
7. Private or confidential information of a third party (e.g., the LSP may have received private or confidential information pursuant to court discovery)

- Evaluate client requirements. Many clients have their own security requirements and will want their LSPs and TPSPs to comply with them. A growing trend among clients is to require LSPs to self-certify that they meet security requirements and submit to security audits by an independent party.
- Regardless of whether clients have formal requirements for information privacy and security, LSPs should discuss with them the nature of the information expected to be involved in any representation. LSPs should then plan to provide the appropriate level of security.
- Fundamentally, and regardless of the category or ranking chosen, the LSP should rank information assets based on:
    1. the sensitivity of the information;
    2. the threats posed by third parties or internal lapses;

3. the vulnerability of the information to the identified threat; and
4. the amount of harm that would be caused if the information were disclosed or altered. For example, client information with great economic or political value is more likely to be targeted by thieves than information having little or no value to anyone except an individual client.

- Evaluate third-party requirements. Many LSPs receive information belonging to a third party, such as an opponent or witness. The LSP has the same obligations to protect the privacy and confidentiality of that information when it was obtained through the discovery process. This may require the LSP to discuss with its opponent and enter into appropriate written agreements or orders regarding the handling of that information during the litigation and the disposition of that information at the end of the litigation.

B. Risk Profiling and Assessment

During this stage of the risk assessment process, the LSP should rate not only the sources of risks and specific threats (for example, those identified above) facing its most valuable or sensitive information assets, but also the organization and its IT infrastructure more generally.

Sources of risk can include the following:

- The LSP's Physical Infrastructure

  The potential for security problems varies greatly among LSPs. The number of LSP employees and contractors, their relative (in)sensitivity to security issues, the number of offices the

LSP maintains, and the amount and nature of the information the LSP holds all tend to affect the risk of security breaches and influence the level of any necessary privacy and security programs. Understanding confidentiality, integrity, and availability in this context requires an analysis of existing policies and security measures that address information disclosure, unauthorized information release, and appropriate access to data. Using this analysis, LSPs should confirm the reasonableness of existing information security practices and whether they need to implement different or additional measures.

- Existing Firm IT Systems

  An LSP should assess the potential points of weakness or penetration in its existing IT infrastructure as well as that of any third party involved in providing IT services or infrastructure. This assessment should not only look at the formal IT infrastructure of the LSP, but also other systems that may interface with that infrastructure such as smart vending machines; heating, ventilating, and air conditioning systems; or other devices that are in any way connected to the LSP's network and thus offer a potential point of penetration. Weaknesses can also be the result of TPSPs who have access to the LSP's network or who provide contractors to assist the LSP's IT department. Here, a CIA assessment for IT systems may aid the evaluation of the security of the physical and technical infrastructure of the LSP, including its ability to

protect data from intruders and to provide appropriate data access internally. Finally, this analysis should consider LSP disaster recovery locations.

- The Practice Needs of Attorneys (e.g., travel, work from home, remote access)

  Modern legal practice and the level of responsiveness expected by clients require LSPs to access information through extranets, mobile devices, or other devices while working from home or traveling outside the office. However, remote access can increase risk. When performing a risk assessment here, providers should consider whether employees are able to access the information they need while ensuring that data is not modified and is inaccessible to unauthorized people. LSPs should address the potential for data loss via use of BYOD devices, flash drives, cloud applications, or sending data to personal e-mail.

- Vendors or Cloud Storage Providers

  Many LSPs rely on third-party vendors to host data. Similarly, LSPs are moving towards cloud-based service providers or applications that will inevitably store firm, client, and third-party data. The LSP has the same responsibility to ensure the protection of data to the extent that it has engaged the particular vendor or service provider. This may include evaluating the service provider's security and ensuring that any necessary protection is implemented by the vendor or service provider.

When using third-party or cloud services, LSPs should consider storing data in an encrypted form. Two types of cloud encryption services are available, standard shared-key and personal or zero knowledge. With standard encryption, the third-party vendor will know the client's encryption key. Zero-knowledge encryption is considered to be more secure because the vendor will not have the encryption key. The idea is that anyone accessing the data through the vendor will not be able to decrypt it.

- Possession of Valuable Information (client or LSP's)

  The more valuable the information an LSP possesses, the greater the incentive someone has to try to steal it. In this context, providers should analyze and evaluate their inventory of information at frequent intervals to ensure that reasonable security needs are in place.

  When creating a risk profile, LSPs should always keep the CIA assessment in mind.[18] This analysis should include known vulnerabilities; for example: the potential for inadvertent data breach due to employee error or negligence, external hacking, denial of service/loss of access, employee theft, loss of data due to equipment failure, disruption of communications and power, or even natural disasters. For each risk/threat identified, the next step is to assess the probability of the threat actually occurring

18. *See Guide for Conducting Risk Assessments*, *supra* note 14.

and the consequences if the information is lost, stolen, or improperly disclosed.

C. Risk Mitigation and Treatment

Once the sensitivity of information assets has been determined and the sources of risks and threats identified and ranked, an LSP is in a position to make informed decisions regarding how best to protect information. For example, an LSP may decide to store certain client documents in its own document management system for convenient access by a large case team, where such documents contain stale business information that would not have a substantial negative impact if lost. In contrast, the LSP might erect significant access barricades around highly sensitive client trade secrets or the client's customers' private information, where the loss of the information would have severe, or even catastrophic, consequences. There will always be a need to balance convenience and function with security. Too much security can impede the ability of attorneys and TPSPs to do their jobs, while too-little security risks exposing sensitive information belonging to the LSP, its clients, or third parties. For a more detailed look at how varying security objectives might be weighed against varying levels of risk, see Table 1, *infra*.[19]

All LSPs should consider scaling and prioritizing their information security practices to fit their particular circumstances as they are known at the time. The focus should always be on what is reasonable and appropriate. To determine that, an LSP should first evaluate the type of information it has, who uses the information, and how they use it. The LSP should also consider CIA: which of its employees should have access to information,

19. *See also* FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, NIST (Feb. 2004), http://infohost.nmt.edu/~sfs/Regs/FIPS-PUB-199-final.pdf (last visited June 2, 2015).

when they should have it, and whether they have put in place effective measures to prevent unauthorized access. All providers have challenges ensuring security for private and confidential information, but ultimately all need to scale their security programs to meet their own and their clients' needs.

POTENTIAL IMPACT [Table 1]			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C. § 3542(b)(1)]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C. § 3542(b)(1)]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C. § 3542(b)(1)]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

IV. GUIDELINES FOR POLICIES AND PRACTICES THAT ADDRESS PRIVACY AND INFORMATION SECURITY

Information security practices should be scaled to the circumstances of the LSP and the needs of its clients. They may be simple or complex. This section of the Commentary sets out a multi-faceted and layered approach to information security.

Not everything set out in this Section can or should be adopted by everyone. Rather, the Section identifies a variety of policies, practices, and methods that might be used to meet the needs of LSPs and clients. Providers should consider cost, business needs, and strategy, but ultimately the reasonableness of the solution is derived from the results of the LSP's risk assessment described in Section III.

This Section IV describes certain processes and practices by which members of the legal services industry may:[20]

---

20. Of course, there is more than one way to set up a program. For example, the FTC's Standards for Safeguarding Consumer Information direct those subject to the Gramm-Leach-Bliley Act, 15 USC §§ 6801(b), 6805(b)(2), to do the following:

> (a) Designate an employee . . . to coordinate . . . information security;
>
> (b) Identify reasonably foreseeable internal and external risks . . .
>
> (c) Design and implement . . . safeguards to control the risks . . .
>
> (d) Oversee service providers . . .
>
> (e) Evaluate and adjust . . . [the] information security program in light of the results of testing and monitoring [the program]. . . .

16 C.F.R. 3.14.4. The CFTC has issued similar guidance to those subject to its jurisdiction. *See* Gary Barnett, *CFTC Staff Advisory No. 14-21*, U.S. COMMODITY FUTURES TRADING COMMISSION (Feb. 26, 2014), http://www.cftc.gov/ucm/groups/public/@lrlettergeneral/documents/letter/14-21.pdf.

- consider the sources of the sensitive information they maintain and the nature of that information;
- identify those within the organization with a bona-fide need for access to information and limit access to those people;
- address information security policies in three subparts:
    1. information security in the office and on the network
    2. information security for information that travels outside the office or the network
    3. information security for information that is shared with experts, consultants, other service providers, and adversaries (either in negotiations or discovery exchanges);
- plan for the disposition of information after it is no longer needed;
- institute a training program that reaches everyone and incentivizes their compliance; and
- anticipate potential breaches by developing plans for prevention, improving detection and response to incidents, preparing to notify affected parties if the information is jeopardized, and adopting contingencies for promptly resolving any problems.

A. Step 1: Identify the Types and Sources of Information That Must Be Protected

To launch any privacy and information security program, an LSP should first evaluate the type of information it has and collects as well as how it uses that information. LSPs are

repositories of lawyer-created information and client information, as well as information concerning third parties. Information that may be used for litigation may need to be treated differently than information that may be used to facilitate basic legal advice or business transactions. Security precautions for client information may already be addressed in retainer agreements—a salutary practice—particularly, if client information is to be stored off-site, including in the cloud. Security for third-party information may often be governed by contract or court order.

B. Step 2: Determine Those Who Need Access

The LSP should determine who among its members and employees needs to have access to what information and under what circumstances should they have it—keeping in mind that all security breaches and leaks come from one of three possible sources: (1) employees (whether intentionally or inadvertently);[21] (2) lost or stolen media; and (3) intrusions from the outside. The governing information management principle should be "need to know." Only those employees with a specific business purpose requiring access to a particular type of information should have access.

---

21. One article identifies four types of employees who pose risks: the "security softie" who does things he or she should not do; the "gadget geek" who adds devices or software to the system that do not belong there; the "squatter," who uses IT resources inappropriately; and the "saboteur," who hacks into areas where he or she does not belong. The article further notes that "insider threats come from many sources: maliciousness, disgruntled employees, rogue technology, lost devices, untrained staff and simple carelessness." *See* Mark Hansen, *4 types of employees who put your cybersecurity at risk, and 10 things you can do to stop them*, A.B.A. J., Mar. 28, 2014, *available at* http://www.abajournal.com/news/article/war_stories_of_insider_threats_posed_by_unapproved_data_services_and_device.

C. Step 3: Information Security Policies and Practices

This section addresses information security policies and practices in three distinctly different contexts: security in the office and on the network; security for information outside the office or network; and security for information when it is provided to others. In each of these three situations, a fully adequate information security and privacy program can be scaled to meet the specific needs of the LSP and its clients.

1. Security in the Office and on the Network

a. Physical Security of the Office

Policies should provide for physical security of the LSP's office, including when doors should be locked, who has access to main entrances, offices, conference rooms, storage rooms, and other office locations. For example, a policy might specify that office locations, whether desk drawers, file cabinets, or file rooms, that contain confidential information be locked when not in use, and access should be limited to people who need access. A slightly more elaborate plan may require that all access to areas containing confidential information should be tracked, perhaps through sign-in sheets or, more elaborately, through electronic verification such as keycards. An even greater level of security might require that servers or records storage areas should have especially limited employee access, perhaps deploying security cameras inside and outside these areas, or an intrusion alert system. Biometric checkpoints may be warranted in some special circumstances.

b. Network Security

Once an LSP has a single computer connected to a server, WiFi router, or other network-enabled device, it has a network. At a minimum, that network should then be protected against failure, and if it is connected at all to the outside world, it should

be protected against intrusion. Network security requires developing secure infrastructure either in accordance with a client's specific security needs or according to a standard industry benchmark.[22] While the level of security is certainly scalable to fit the circumstances, once a provider moves beyond the most basic level, it will likely need to determine who will monitor the firm network for security breaches, how that monitoring will be accomplished, and how the monitors will be monitored. Policies should describe procedures for regularly monitoring and analyzing network logs and events, and for identifying and addressing potential security breaches. Audits and monitoring are more specifically discussed in Part IV.C.1.h., *infra*.

---

22. Industry certifications can represent a useful benchmark, but LSPs should generally not consider certification, or lack of it, to define the level of security. In addition, providers relying on these or other industry standards to determine third-party security should inquire as to exactly which parts of the third party's business are certified and which are not certified.

ISO is the largest developer of standards in the world. Its membership is drawn from the National Standards Bodies of multiple countries. The International Electrotechnical Commission oversees the development of electrical and electronic Standards for participating countries. The 27000 series has been reserved specifically for information security matters. ISO 27001 is a standard describing the best practice for an Information Security Management System, often referred to as "ISMS." An ISMS is "part of the overall management system, based on a business risk approach, to establish, implement, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, processes and resources." ISO/IEC 27000: 2012.

SSAE-16 (Statement on Standards for Attestation Engagements No. 16) is also a commonly used security standard for data centers, as set forth by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA).

c. Secure Backup

Information security policies should provide for secure backup of provider information and include disaster/recovery plans, including procedures for restoration. LSPs should consider off-site storage of encrypted backup media, and if they backup client information separately from their own information, these backup processes should also have disaster/recovery plans. Such plans would ideally include specific procedures for backup and restoration that are understood, agreed upon, and maintained in compliance with a written agreement among the clients, providers, and third parties (as appropriate). Conducting regular test restores is highly recommended.

d. User Authentication and Permissions

LSPs can only protect private and confidential information that is stored on networks or on devices by requiring those who seek access to the information to show they have authorization to access it. This means that access to information stored on a network, a computer, or a mobile device should require user authentication through such means as passwords or, in the case of multifactor authentication, a password combined with a security question. Similarly, assuming the provider determined, in Step 2, that employee and partner access to certain information should be restricted, then users' access should be limited through permissions for designated levels of sensitive information. For example, an LSP might implement role-based access controls (RBAC) by which its employees' access to information would be determined by the type of information and the employee's role in the organization. Such a system might grant varying rights depending on whether a person is a partner, associate, litigator, secretary, and so forth.[23]

23. For an overview of the subject, *see Attribute Based Access Control (ABAC) – Overview*, NIST, http://csrc.nist.gov/projects/abac (last visited June

No matter how the LSP grants or limits access to particular types of information, access to network areas and devices containing confidential information should be protected at least by "strong" passwords. "The strength of a password is related to its length and its randomness properties."[24] Strong passwords should be of sufficient length and complexity so that they cannot be guessed, e.g., they should contain a combination of capital and lowercase letters, numbers, and special characters. Users should change login passwords regularly. Although at times inconvenient for the user, ideally a network would also lock out a user who has not revised a password within a prescribed interval, or who has failed to enter a correct password after several incorrect attempts.

e. External Media

While there might be valid reasons to use external media such as flash drives, transferring information to portable media can compromise security. The media could introduce viruses or malware to the network. Information copied onto peripheral media can create an additional risk point because the media can easily be transported, lost, or stolen.

2, 2015). For a more detailed review of the topic, *see* David F. Ferraiolo & D. Richard Kuhn, *Role-Based Access Controls,* 15th National computer Security Conference (1992), Baltimore MD, pp. 554–563, *available at* http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf. An alternative, more complicated, system for limited access controls is the attribute based access control (ABAC). For an overview of this method, see *Attribute Based Access Control (ABAC) – Overview*.

24. *See* Meltem Sönmez Turan et. al., *Special Publication 800–132*, *Recommendation for Password-Based Key Derivation*, *Part 1: Storage Applications*, NIST, Appendix A.1 (Dec. 2010), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf [hereinafter *Recommendations for Password-Based Key Derivation*].

Thus, policies should restrict the use of unencrypted external media. LSPs should consider policies that specify when any external media may be used, who may use it, to what devices it may be connected, and how it is to be stored, erased, reused, transferred, and designated for disposal. Such "policies" can take several forms, from written directives to technical measures that preclude transferring or copying information. LSPs should encrypt portable media to restrict unintended access.

f. Remote Access of Provider Network

Many LSPs permit employees to access their network from locations outside the office. This access may be through encrypted connections such as Virtual Private Networks (VPN) or remote access programs in order to maintain privacy and security. Remote access with authentication via two levels of passwords and deployment of access controls through RBAC or attribute based access control (ABAC) should ensure that those with permission to access certain information are the only people who can access it.[25]

LSPs that offer WiFi access in their office should ensure that the network is protected through over-the-air authentication and encryption, and their policies should provide protocols for managing and monitoring the WiFi network. Logging features should be enabled so that there is a record of everything that is copied, in the event that data is wrongfully accessed. Wireless networks should be encrypted and LSPs should not overlook the security of their wireless network (current WiFi Protected Access II (WPA2) provides the highest level of router protection). Guest WiFi should be provided through a separate network with no ability to access the rest of the network.

---

25. *See Recommendations for Password-Based Key Derivation*, *supra* note 24 and accompanying text.

LSPs should train employees to avoid publically available computer systems, such as computers at hotels, when accessing the LSP's network. Unless the system is merely a dumb terminal without capacity to save or further transmit information, any restrictions on further use and dissemination become problematic, and accountability for the information is compromised. Even if the employee is personally trustworthy and loyal, the LSP should consider whether the employee should be allowed to use the devices of friends and family members to access the provider network or use public networks such as cafes or airports. Private or confidential information may be stored on the device and accessed by an unauthorized person.

g. Receipt and Creation of Confidential Information

Although very difficult to achieve in practice, LSPs should consider implementing detailed procedures to track client information from receipt until destruction. Such procedures might establish a central point for receiving and tracking client or case-related information and implement a process for logging information received from the client, no matter whether it arrives on an electronic device or external media, through an online transmission (email, ftp site, web file sharing service, etc.), or in hard copy. Logging the date, sender, recipient, and contents of information received facilitates managing the information. Attaching a label with a unique ID to each piece of any media, device, or hard copy file received may also help manage them throughout the representation. Logging confidential information allows LSPs to begin a chain of custody that reflects access, copying, transfer, and deletion of the files.

LSPs should also consider whether there is a need to distinguish between client-created information that is sent to them and work product that is generated by the LSP. Although LSPs should treat both types of information as confidential, the LSP

may find it easier to create distinct lifecycles for provider-created information and client-created information for the purpose of chain of custody and work management, as well as disposition at the end of a matter.

h. Monitoring and Audits

Oversight is appropriate to ensure that policies are executed correctly to identify remaining areas of risk and to quickly identify breaches. Policies should address who is responsible for audits and how and when audits will be conducted and reported. Monitoring should include all areas of the LSP's business and all processes involving confidential information, although they need not all take place at the same time. Checklists can serve as a useful guide to ensure thoroughness of past and future audits.

In addition, real-time tracking and accounting of client information is necessary to identify breaches quickly and help mitigate problems caused by data loss. Immediate notification of appropriate LSP partners and affected clients, as well as any third parties, such as law enforcement authorities or insurers involved in the transport or loss of information, is essential.

LSPs should also include a requirement for periodic data inventories, e.g., determining what information the LSP has and where it resides. Regular checks on data logs and data inventories provide quality assurance of information security.

2. Security Outside the Office and Network

Whenever information moves, it is vulnerable to being damaged, lost, stolen, or altered. This is true whether a move entails a ride in a cab to the courthouse or a trip around the globe for a meeting. Information security programs should consider the movement of information and the potential risks. Where information is subject to special requirements, the LSP should set

forth a mechanism for alerting the relevant personnel to those requirements.

a. Encryption of Copies and During Transfers

LSP policies should generally require encryption when private or confidential information is transferred. Unless email is encrypted, LSPs may wish to consider alternative ways to transfer particularly sensitive, private, or confidential information. Encryption is more than a useful and convenient information security tool. It is critical for protecting client information, especially when the information is stored on mobile devices, transmitted, or stored remotely. Typically, encryption applies an algorithm to convert data to an unreadable code unless it is decrypted using a password. Provided only the sender and recipient of data know a password, the data will be protected against third parties even if the data is lost or intercepted. LSPs should use encryption to protect client files, especially sensitive information and information that is highly vulnerable. Encryption keys should be stored separately from the encrypted devices or media to ensure security.

Many operating systems and their supporting hardware can be configured to use encryption for all files or for files selected by the user.[26] Several different products are available to provide various levels of encryption capabilities. LSPs need to

26. *See supra* note 23. Encrypting files is a critical practice in many circumstances. LSPs should be mindful, however, that in some circumstances encryption may mask the introduction of malware into the network or obscure the theft of information. *See* KIM ZETTER, COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON, Ch.14 (Crown Publish Group 2014); *see also* Karen Scarfone et. al., *Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices*, NIST (Nov. 2007), http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

be knowledgeable enough about the different encryption capabilities available to select the appropriate options for their needs. Third-party software for encryption is also readily available. Email applications can be set up to encrypt and automatically decrypt emails. Users simply need to exchange public keys and have their private key applied to decrypt messages; however, this key exchange process is burdensome within most standardized email environments and may lead to inconsistent application. Presently, there are third-party services that provide additional capabilities that make key exchange transparent and much easier to use. And mobile devices have encryption options—which can be managed through the device settings—that protect information when the device is locked.

Once information has been encrypted, it may then be securely transmitted through Secure File Transfer Protocol (SFTP), email, or cloud document management services. If information must be transmitted physically, the delivery method should reflect the sensitivity of the information. Highly sensitive information may need to be carried by a private courier or an LSP employee. The method of transport should be considered in avoiding unintended access due to the media being confiscated, lost, or stolen. If information is mailed, it should be sent in a manner so that it can be tracked at all times. Unencrypted sensitive information should never be placed in the mail or turned over to a courier for delivery. All too frequently, packages are lost, opened, or stolen in transit.

b. Mobile Devices

Mobile devices, such as laptops, phones, tablets, and PDAs are a practical necessity for LSPs. However, their portability and access to information also make them a target for information theft, even when they are "safely" located within an office environment. The primary tools for protecting the devices

from theft and intrusion consist of strong passwords, encryption, auto-locking defaults, device-tracing applications, and applications that allow the devices to be wiped remotely.

Through Mobile Device Management (MDM) the LSP can also remotely update mobile devices that are connected to any cellular network. It can thus install remote applications, configure settings, ensure security by updating and running malware detection software at pre-determined times (or on demand), enable device firewalls, disable public file sharing, avoid automatic connections to public WiFi, and even track and wipe lost or stolen devices.

c. Public WiFi

Additional security can be provided by deploying a strong employee-use policy with respect to mobile devices in public places. For example, personnel can be instructed to take special care when working with mobile devices in public by not connecting devices to public WiFi to access or transit client information. LSPs should set guidelines regarding the circumstances, if any, when an employee may use public WiFi to transmit client information.[27] Unencrypted client information

27. *See* Cal. State Bar Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. No. 2010-179 (2010), http://jolt.richmond.edu/wp-content/uploads/13-State-Bar-of-California-Opinion-2010-179-L0563533x7A34B.pdf. California requires attorneys to consider the following factors to determine appropriateness of a wireless communication:

> 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's

sent through public WiFi, including paid or free hotspots, can be easily compromised. Therefore, LSPs should clearly specify when use of public WiFi is and is not permitted and what additional protections are required.[28]

Policies should instruct employees to immediately notify the LSP if a mobile device is lost or stolen so the LSP may wipe or disable the device, as appropriate.

d. General External Use Security Considerations

When working outside controlled environments, employees should be instructed to use screen guards to prevent laptop screens from being viewed by the public, and to avoid discussing sensitive information in public. Employees also should be made aware of the vulnerabilities of blue tooth technology and potential for eavesdropping.

Policies should also instruct employees to immediately notify the LSP if a mobile device is lost or stolen and to subsequently wipe and disable the missing device.

e. BYOD and Personal Device Policies and Practices

Losing a client's business information, trade secrets, or privileged information can get an LSP in trouble with its client and perhaps with the state bar disciplinary counsel as well. Los-

---

instructions and circumstances, such as access by others to the client's devices and communications.

Id.

28. Options for additional protections may include use of virtual private networks (VPNs), which route data through a private connection. When possible, encrypted connections are also preferred through use of "https" addresses instead of "http" for websites and use of a Secure Sockets Layer (SSL) security protocol for applications.

ing sensitive client information that is subject to special regulatory restrictions, such as health related information, may generate regulatory involvement. Personal devices present one of the most significant risks to client information. These devices include home computers as well as mobile devices such as laptops, smartphones, and tablets. The best likely defense against the loss or theft of trade secrets, business information, privileged materials, and other sensitive information may be a strong and strictly enforced policy banning the use of personal devices to transact business or store such information. If an LSP permits its employees to use their personal devices to access private or confidential information, the LSP should consider taking the following steps to lessen the risk of using such devices:

- Allowing the use of *only* those devices that are specifically approved by the LSP's security professionals
- Requiring strong password and encryption policies
- Limiting the employee's ability to create or store LSP or client information directly on the device, by providing access only through secured portals to provider-protected networks. LSPs may also consider "sandboxing" mobile device applications that contain confidential information to shield provider applications from access by other applications or malware on the device.[29]
- Designating types of client information that should not be accessed, transmitted, or stored on a personal device. This may include infor-

29. Sandboxing effectively allows a device to host applications or data from multiple sources while blocking the flow of information or data from one part of the device to another.

mation that is subject to specific statutory protections, information that is otherwise highly sensitive, and information that clients have requested not be accessed by BYOD devices.

- Addressing employee home WiFi networks and devices used to create personal hotspots by requiring that these networks be secured with strong passwords that are not shared and are changed regularly

f. Travel Abroad

LSP personnel should avoid traveling overseas with client information or devices capable of accessing the LSP's IT systems, unless appropriate precautions and safeguards have been taken to account for increased security risks. Because this is a specialized area, LSPs might consider consulting or hiring third parties with expertise in network security involving traveling and transporting data outside the country.

LSPs should specifically address travel to high-risk geographic regions. It may not be possible or advisable for employees to directly access firm systems from high-risk areas. It may also not be advisable to allow employees to carry their normal devices or media with them into high-risk areas lest they be used to infiltrate the provider's systems. LSPs may also consider requiring employees to travel only with devices that do not contain sensitive information and adjusting default device settings on those devices. In addition, LSPs should consider whether WiFi connections are especially risky and adopt a policy of wiping devices both before traveling through foreign customs and before reconnecting them to the provider's network when they return home.

3. Security Among Third-Party Service Providers

The best information security program in the world can be nullified if the information is vested in the hands of another service provider who does not have adequate safeguards in place. For that reason alone, LSPs have a strong incentive to make sure the information they share with their experts, consultants, litigation support specialists, and other providers is well protected.

LSPs, like their clients and other businesses, increasingly rely on TPSPs to process, store, and manage information and IT systems. These TPSPs can include cloud storage providers, online human resource management companies, paper storage and destruction companies, eDiscovery service providers, enterprise-class online productivity services, Software as a Service (SAAS) cloud providers, and providers of outsourced IT staffing and services. Regardless of the TPSP or type of service offered, LSPs should consider following a set of best practices when engaging the services of such a TPSP on its own or on behalf of a client.

a. Understand the Type of Information the TPSP Will Handle

Before entering into an agreement with a TPSP, LSPs should carefully consider the type(s) of information that the TPSP will handle. For example, the following questions should be asked about the information to be accessed, processed, or stored by a TPSP:

- Will the TPSP handle client information, or only information belonging to the LSP itself, such as its own HR information?
- Will the TPSP handle PII, sensitive financial information, trade secrets, or privileged communications and materials?

- Are there any legal or regulatory restrictions imposed on the handling of the information? For example, does the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), or the Payment Card Industry Data Security Standard cover the information?
- Are there any contractual obligations related to the information? For example, will the TPSP handle client information covered by a HIPAA business associate agreement or EU Model Clauses agreement entered into by the LSP?

b. Ensure Compliance with Applicable Legal and Regulatory Requirements

LSPs should understand the legal and regulatory requirements applicable to the type of information that will be accessed, processed, or stored by the TPSP, and ensure that the TPSP is not only capable of meeting these requirements, but also is *contractually obligated* to do so.

c. Understand Geographic and Technical Risks Associated with the TPSP

LSPs should understand where their information will be stored and whether their information will be commingled with information belonging to other customers of the TPSP. TPSPs may store information in a variety of geographic locations, including overseas. The physical location of its information can

subject LSPs to litigation and regulatory oversight in the jurisdiction where information is stored.[30] LSPs must therefore understand and approve where its information will be stored. TPSPs may also commingle the information of their other customers. This is generally *not* a recommended arrangement for LSPs, because its information will be too sensitive to make the risks attendant with commingling acceptable. Thus, LSPs should avoid any arrangement in which information transferred to a TPSP will be commingled.

d. Conduct Due Diligence

A TPSP's viability is critical and LSPs should therefore obtain information about the TPSP's potential conflicts, and its financial stability under non-disclosure agreements. LSPs should also know the scope and policy limits of the TPSP's insurance coverage and ensure that the TPSP performs background checks on its employees and requires employees to sign confidentiality agreements.

e. Review and Approve the TPSP's Own Information Privacy and Security Policies Prior to Executing a Contract

No TPSP should be retained unless it has an appropriate information security and privacy policy. The TPSP's level of security and privacy protections should generally match or exceed those of the LSP. As a general matter, TPSPs should only be retained if they agree to meet an established standard, such

30. *See* Forward Food LLC v. Next Proteins Inc., 2008 WL 4602345 (Sup. Ct. N.Y. Oct. 15, 2008). The court found personal jurisdiction where a company's only contacts in New York consisted of a single visit, a few emails into the state, and a server located in the state containing the corporation's virtual data room.

as ISO 27001 and 27002. At a minimum, the LSP retaining a TPSP should consider contractually mandating each of the following:

1) Physical Security Controls

TPSPs must ensure the physical security of facilities housing sensitive information or from which such information can be accessed, including offices, offsite facilities, and locations of servers. Access to these facilities should be logged. These same recommendations apply to TPSPs that access, process, or store information belonging to the LSP or its clients.

2) Information Access Controls

TPSPs need to have appropriate preventative controls on accessing information, including, but not limited to, multi-factor authentication utilizing complex passwords, compartmentalization of information on the TPSP's systems, and access restricted to 'need to know' individuals.

3) Intrusion Detection Systems

TPSPs must employ an appropriate intrusion prevention system. If the information provided to the TPSP is highly sensitive and contains significant private or confidential information, LSPs should consider requiring the TPSP to employ an intrusion detection and monitoring system.

4) Encryption Procedures

Information sent to a TPSP should be encrypted while in transit to and from the TPSP. LSPs should also consider whether the sensitivity of the information warrants a requirement to encrypt information while it is stored ("at rest") by the TPSP.

5) Secure Disposition of Information

If the TPSP will store information for the LSP, it should agree that it will only use secure methods for disposing of that information or any hardware or media on which that information was stored.

f. Review and Approve the TPSP's Employee Training Program for Information Privacy and Security Prior to Executing a Contract

For both LSPs and TPSPs, proper employee and contractor training programs are essential to maintain information security and privacy. Before entering into an agreement with a TPSP, the LSP should inquire about the TPSP's employee and contractor training programs related to information security and privacy to ensure they are adequate. If the TPSP's training program is inadequate, the LSP should consider mandating the necessary improvements in the contract with the TPSP or finding another TPSP.

g. Ensure Appropriate Safeguards for Intellectual Property

Contracts with TPSPs should protect the intellectual property rights of the LSP and those of its clients. Use of a TPSP should not alter or adversely affect intellectual property rights.

h. Records Management

If a TPSP will store any information belonging to the LSP or its clients, the LSP should consider requiring the TPSP to adhere to the relevant existing records management and retention policies, except when doing so would frustrate the purpose of the TPSP's engagement, or when the TPSP is retained to provide an information archiving service.

i. Mandate Appropriate Information Disposition Upon Termination of the Relationship

The TPSP contract should require the TPSP to adhere to the records' policies of the client and to securely dispose of, or return, all the LSP's information in a useable form, in a timely manner, and upon termination of the relationship. Contractual clauses in which non-payment on the part of the LSP or its client justify refusal or delay in returning or providing access to information are generally not acceptable.[31]

j. Bankruptcy Protection

Careful consideration should be given to what will happen if the TPSP enters into bankruptcy. This scenario can be specifically addressed in the contract to ensure there is no dispute regarding ownership of the information or the media holding the information. Indeed, in certain situations, LSPs may wish to consider purchasing the physical media on which its information will be stored at the outset of the relationship, so there can be no question regarding the right or ability of the LSP to recover media-containing information.

k. Information Backup, Disaster Recovery, Access Continuity, and Incident Response

Before sending information to a TPSP, the LSP should be satisfied that the TPSP has adequate plans and equipment for disaster recovery, backup of the LSP's information, and response to incidents such as data breaches. The LSP should also ensure that the TPSP is contractually obligated to provide access

31. Indeed, even contractual commitments may not always protect a party from the misappropriation of highly sensitive private and confidential information. *See* Complaint, Glaxosmithkline LLC v. Discovery Works Legal, Inc., et al., No. 650210/2013 (Sup. Ct. New York County), filed Jan. 22, 2013.

to its information without excessive down time and will have an appropriate level of technical support available when needed.

l. Obligation to Assist in Discovery

In the event that information under the control of the LSP is in the possession or custody of the TPSP and becomes subject to a litigation hold or discovery obligation, a TPSP should be contractually required to render timely assistance in preserving and collecting information, as appropriate. Accordingly, the TPSP contract should include a clear benchmark for "timeliness" to avoid confusion regarding the degree of delay acceptable in implementing a litigation hold, and preserving and collecting the needed information. Similarly, the agreement should clearly set forth procedures to be followed by the TPSP if it directly receives a subpoena or other civil or law enforcement request for the LSP's information. In most circumstances, the TPSP should be required to immediately notify the LSP and cooperate fully with it in responding.[32]

m. Limitation on Sub-Contracting and Onward Transfers

A TPSP generally should not be permitted to allow a sub-contractor or other third party to access, process, or store the LSP's information without express prior approval for using the particular sub-contractor(s) or allowing the onward transfer(s) of information. Likewise, LSPs should not approve any such arrangements without first confirming that the sub-contractor(s) will be legally bound to comply with the same contractual provisions as the original TPSP.

32. In some situations involving requests from law enforcement authorities, immediate notification may be prohibited.

n. Accountability and Shared Liability

The contract between the LSP and the TPSP should consider proper incentives for compliance by imposing some form of liability on the TPSP for harm resulting from any failure to comply with its obligations under the agreement. LSPs should also consider requiring some form of indemnification of the LSP by the TPSP in the event of a data breach or other contract violation that exposes the LSP to liability. There are many potential mechanisms for imposing such liability, including liquidated damages or indemnification of the LSP by the TPSP.

o. Inspection and Monitoring

The contract should also give the LSP a right to audit the TPSP's compliance with its information, privacy, and security obligations, or to receive copies of the reports of an independent auditor. If the TPSP is concerned about giving the LSP access to its facilities or systems to test it for conflicts and security concerns, the agreement should allow for use of a mutually acceptable third-party "auditor." It is also critical that at least one thorough inspection actually be performed, and not merely permitted in theory. Additionally, parties should negotiate terms which contemplate updates to information privacy and security obligations as related technology and processes evolve.

p. Ensure Appropriate Access Controls for TPSP Personnel Given Access to LSP IT Systems

Where the contract calls for TPSP's personnel to have access of any sort to the LSP's own IT system, the LSP must make sure that it has appropriate safeguards in place. At a minimum, TPSP personnel who will have the ability to access the LSP's IT system should be subject to a background check, monitoring, and logging for unusual activity, and should have access to only the systems necessary to facilitate the purpose for which the

TPSP was engaged. The contract should also address the TPSP's responsibility and role with respect to providing notice and remediation in the event of any loss, theft, or breach of information caused by TPSP personnel.

D. Step 4: Establish Processes for Timely Disposition of Records and Information

LSPs should consider establishing policies, procedures, methods, and technologies suitable for deletion and destruction of client and third-party private and confidential information. Deletion of client information is necessary when directed by a client or triggered by the LSP's information retention policy. In general, information should be deleted when it is no longer needed. This means that LSPs should also ensure timely and thorough deletion of confidential information on devices of departing employees and on retired drives and devices during technology upgrades.

To ensure deletion policies are clearly understood by clients, when appropriate, LSPs should consider including a standard addendum to engagement letters that addresses the retention and disposition of client and third-party information. Such attachments should address standard policies and practices for the LSP handling the deletion of client information at the end of a matter, and provide instructions for the client to communicate its express wishes for the disposition of its information. Mid-matter deletion of certain unneeded documents may also be advisable, if a matter involves particularly sensitive information, and is not subject to a preservation obligation. If the provider plans to retain work product containing confidential client information after a matter has closed, because it has precedential value, the provider should clearly disclose its intention and obtain client consent. Standard policies and practices shared with clients about deletion of the client's files may address:

- whether the provider holds unique copies of documents potentially subject to a legal hold in other matters and whether the client would benefit from the LSP's retention of certain files from the closed matter;
- the level of sensitivity of the client's information held by the LSP;
- whether the client requires the LSP to retain certain documents, and whether other unnecessary files can be segregated and deleted;
- whether the client wants the LSP to send it a copy of the files to be deleted; and
- whether the client wants the LSP to keep copies of certain documents for safekeeping, and, if so, how those files will be stored.

The client retention letter, or a related addendum, should also address the disposition of information if a client becomes unavailable after the close of a matter. In that circumstance, the agreement might allow the client's information to be disposed of following a designated waiting period and in compliance with the LSP's applicable legal and ethical obligations.[33]

The waiting period should be set forth in the LSP's policies and made available to the client in the engagement letter. The addendum and a notice of the commencement of the applicable waiting period should be sent to the client after the matter closes. At the end of the applicable waiting period, the LSP

33. If the period was not determined by agreement between the LSP and the client, state rules may apply. *See, e.g.*, Ethics Op. 283, Disposition of Closed Client files, n. 9, DC Bar (July 1998), https://www.dcbar.org/bar-resources/legal-ethics/opinions/opinion283.cfm [hereinafter Ethics Opinion 283]; *see also* Materials on Client File Retention, ABA, http://www.americanbar.org/groups/professional_responsibility/services/ethicsearch/materials_on_client_file_retention.html (last visited June 3, 2015).

should direct that the client's information be disposed of in accordance with the LSP's legal and ethical obligations, unless the LSP becomes aware of a reason to continue to hold the information, e.g., it becomes potentially relevant to other proceedings involving the client. Policies should set forth procedures for a legal hold of the LSP's information in the event the LSP has an expectation that the files may be relevant in future litigation.

LSP policies should account for whether the LSP may have any legal or other obligation to retain files after a client's matter concludes and whether it may need to retain a copy of any files as a record of the work it did for the client. LSPs may therefore wish to create a deletion schedule where the LSP's work-product is held for a longer period than client-created or client-provided information. If the LSP determines it should keep its work product longer than its retention time, it should hold onto the work-product for only a reasonable period.

In instances where a client does not consent to retention of its confidential information after the close of a matter, the client file retained by the LSP may still contain work product that the LSP wishes to keep as precedent, form, or history (such as legal memoranda, pleading drafts, or case notes).[34] Under these circumstances, the LSP should "sanitize" those documents, removing confidential client information before storing the documents in the LSP's precedent bank or file repository.

Deletion of a client's confidential information should be comprehensive and involve all locations where the information resides.[35] Deletion will likely require efforts by the LSP's IT personnel and by the employees who accessed client information.

---

34. State bar rules and cases differ with regard to whether LSPs or clients own attorney work product. *See* Ethics Opinion 283, *supra* note 33 (raising but not deciding the issue).

35. "Deletion" methods and underlying hardware can differ in degrees of information recoverability. Physical shredding of the storage media

To the extent feasible, the LSP should confirm deletion from all potential locations, including document management systems, shared and private network storage, employee email, employee computers, electronic devices, external storage, backup files, and cloud servers. The LSP should also direct that the same steps be taken by any parties to whom they delivered client information, including opposing parties and TPSPs, as well as other LSPs. LSPs should deliver written confirmation to clients of having exercised reasonable diligence in the deletion of private or confidential information.

E. Step 5: Implement Training Program

People have unfortunate tendencies to lose things, speak at inopportune times, open strange emails, visit inappropriate websites, and so forth. Accordingly, LSPs need to train their owners and employees. Begin with teaching people about written information security and privacy policies that document and standardize the provider's practices for maintaining information security and confidentiality. Training should cover client information generally and identify categories of information that may require additional protection, identify applicable state and federal laws, and explain the nature of the client information held and any contractual obligations applicable to it.

---

is the most secure deletion of information but may be impractical. Therefore, more commonly acceptable standards of deletion include secure overwrite methods. Most drive electronics have built-in secure erase commands that can be activated with software and thoroughly erase the drive. LSPs may also consider using crypto-deletion where overwrite methods are insufficient or impractical, e.g., cloud services. Crypto-deletion involves encrypting information and destroying the encryption key rather than the information, rendering the information unusable. Deletion policies need to account not only for the LSP's technology infrastructure, but also regulations and requirements for specific types of information. For example, crypto-deletion may not be a valid solution for information if there is a strict requirement that the information must be scrubbed.

Information security and privacy policies clearly apply to all personnel who might handle PII or confidential client information. This includes the LSP's most senior people, its owners, managers, employees, contract staff, and other parties engaged by the LSP who can access private or confidential information.

The following elements are features that an LSP can consider including in its training program:

1. Mandatory for All Personnel

An LSP should consider making security training mandatory for all attorneys, paralegals, assistants, secretaries, contract staff, records staff, IT staff, and other personnel, regardless of whether such staff members will have access to sensitive information. Universal mandatory training is beneficial because the nature of IT systems and legal practice makes it highly likely that every employee will encounter private or confidential information at some point during their employment, and even those who do not could still be the source of a security breach that spreads beyond their own computer or office. It takes only one employee holding a door open for someone she does not recognize, or clicking on a link in an email message, to compromise an entire LSP's network.

2. Annual or Bi-Annual Frequency

The nature of security threats and tactics used by hackers and social engineers is constantly changing, as is the underlying technology. Accordingly, LSPs should consider sponsoring training on an annual basis. In addition to formal training on at least an annual basis, periodic reminders or updates might also be sent to all personnel reminding them of best practices and updating them on emerging threats. Besides keeping personnel informed, such regular reminders show that the LSP takes information privacy and security seriously and expects its employees

to do the same. Privacy and security training could also be mandatory for all new hires.

3. Accountability

There should be clear and meaningful consequences for personnel who fail to successfully complete training, or abide by the LSP's privacy and security policies. For example, LSPs who pay bonuses might want to consider reducing bonus compensation for employees who fail to complete training in a specified timeframe. Alternatively, they may wish to consider denying such employee access to the firm's network until training is completed.

4. Include Core Content

An ideal training program may include the following content:

a. General Background and a Clear Statement of Importance

Training programs should include a general overview or primer that provides a context for addressing information security and privacy issues. This primer should give examples that demonstrate the significance of these issues and the serious consequences that may result when information is inappropriately handled. These examples should reinforce the direct connection between the LSP's adherence to information and privacy principles and the LSP's reputation and success. This primer will therefore reinforce the serious damages the LSP may likely suffer if it—or its employees—violate laws surrounding information privacy/security or cause data breaches. These are both group and personal efforts, and training should convey that each employee is also personally responsible for maintaining the LSP's standards for privacy and security.

b. LSP Policies

Training should include all aspects of the LSP's information privacy and security policies, including policies regarding the use of social media and the use of mobile devices.

c. General Practices

In addition to explaining the LSP's own information privacy and security policies, training programs can include reasonable practices to maintain information security and privacy, such as those set forth in these Guidelines.

d. Applicable Ethical, Legal, and Regulatory Rules

Training programs should cover legal and regulatory rules applicable to the information held by the LSP.

e. Applicable Contractual Restrictions

If the LSP has access to information that is covered by contractual obligations, such as where a client has imposed additional information privacy or security restrictions on its information through a HIPAA business associate agreement, training should cover and highlight those additional requirements.

f. Role-Specific Requirements

In larger organizations where some employees, such as HR staff, may be exposed to a large amount of highly sensitive information covered by detailed regulatory requirements, additional role-specific training may be warranted for such employees.

g. Interactivity and Real World Scenarios

LSPs may wish to consider implementing training programs that present "real world" scenarios and prompt participants to indicate how they would respond under similar

conditions. For example, such training programs might provide examples of methods successfully employed in the past by hackers and social engineers to bypass security controls and obtain access to private or confidential information. In this way, the trainee can learn from past mistakes made by others and hopefully avoid repeating them.

5. Testing

In order to facilitate accountability and ensure mastery of the training material, LSP's training might also include a test that would be scored.[36] Failure to achieve a minimum score would then require the individual to continue or repeat the training until a satisfactory score was achieved.

6. Additional Messaging and Reminders

Larger organizations should consider supplementing formal training with posters, desk toys, and other aids to remind people on a regular basis of the importance of maintaining privacy and security over the LSP's information.

7. Training for Solo Practitioners and Small Offices

Receiving annual training meeting the above criteria is no less important for solo practitioners and their staff than it is for large law firms. However, it may be impractical for a solo practitioner or small law office to create an internal training program. Instead, such LSPs should consider using an accredited third-party organization; for example, by attending a conference, arranging for an in-house presentation, or employing a web-based solution.

36. This approach is similar to that already used in many training programs about sexual harassment and other HR issues.

F. Step 6: Preparing for the Worst

An information security program is not complete unless it includes provisions for the worst possible scenario. Technical problems and human mistakes are inevitable: a device will almost inevitably be lost or stolen, a critical server will irreparably crash, a social engineer will send a phishing email that someone will click on, or an intruder will breach the firewall and either damage the IT system or steal something, or both. An LSP should prepare and test a data breach response plan that anticipates common incidents.

This plan might consist of the following:

- Training all personnel to follow procedures for reporting and responding to potential information security breaches, including loss of devices or media, inadvertent transmission of information, or the interception or theft of information
- Identifying a person or a team to direct the LSP's response to a breach incident
- Creating a process for conducting a prompt investigation of a suspected breach, including assessing how and when the breach occurred, as well as what information sources have been compromised and what information is contained in those sources (If an investigation would likely require third-party forensic or IT experts, they should be identified beforehand and listed in the LSP's policy.)
- Depending on the risk profile of the LSP, running periodic "fire drills" or "table top" exercises to test the plan under various scenarios

(This will allow for the potential absence of employees who would ordinarily be critical to the successful implementation of the plan.)

- Developing procedures to mitigate damage when a breach is ongoing, bearing in mind that unplugging the affected computer may not necessarily be the best approach to defeat a sophisticated attack or to preserve important evidence (Indeed, in some instances the "obvious" source of the intrusion may only be a decoy meant to distract the security team from the real assault on the LSP's systems.)
- Contingency plans for providing notice to the owners of compromised information, including clients and other interested parties after a breach or loss is confirmed
- Developing procedures to revise and adjust policies after an unauthorized disclosure, loss, or theft breach to avoid future occurrences
- Implementing a system to receive news and updates of reported breaches outside of the LSP, which may affect the LSP's information security[37]
- Notifying appropriate law enforcement authorities and insurers
- Abiding by applicable breach notification regulations

---

37. *See*, *e.g.*, U.S. Department of Homeland Security, US-CERT, https://www.us-cert.gov. In the future, LSPs may also create an anonymous repository through which hacking and threat information could be shared. *See* Matthew Goldstein, *Wall St. and Law Firms Plan Cooperative Body to Bolster Online Security*, N.Y. TIMES, Feb. 23, 2015, *available at* http://www.nytimes.com/2015/02/24/business/dealbook/wall-st-and-law-firms-weigh-cooperation-on-cybersecurity.html.

V. CONCLUSION

LSPs and TPSPs have the responsibility to take reasonable steps to protect private and confidential information, a responsibility that is grounded in the ethics rules applicable to lawyers as well as in federal, state, and common law rules. In some situations, a duty may also arise under the laws of foreign nations. This Commentary is intended to help LSPs assess security risks and provides guidelines for implementing privacy and information security policies.

APPENDIX A: PRIVACY AND SECURITY IN THE HEALTH CARE INDUSTRY

Privacy and security requirements are not new to the health care industry. LSPs who work with health information are subject to rules governing privacy and security as defined in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Clinical and Economic Clinical Health (HITECH). These laws regulate the disclosure of personal information by health care providers and those who provide services to the health care providers, including lawyers. Both HIPAA and HITECH directly affect LSPs who perform work for those covered by the laws and they potentially provide guidance to other LSPs as well. Thus, among other things, HIPAA:

- provides privacy protection for protected health information (PHI);
- mandates security requirements;
- addresses data breaches/breach notification requirements;
- mandates notice of privacy practices;
- governs sales of PHI and regulates sharing of PHI;
- requires consent and bars certain disclosures; and
- mandates Business Associate Agreements for entities that create, receive, store, maintain, or transmit PHI (Business Associates are responsible for their subcontractors), including law firms and other LSPs.

With minor exceptions, a Business Associate (BA) is a person or entity who performs work involving access to PHI on

behalf of, or provides certain services to, a covered entity.[38] Similarly, under the HITECH Act, LSPs and vendors may be considered BAs. HITECH provides that BAs are subject to the HIPAA Security and Privacy rules that apply to electronically stored PHI (e-PHI).

This means that LSPs who possess or work with HIPAA-protected information must impose protections into three safeguard categories: physical safeguards (e.g., physical measures, policies, and procedures to protect the information systems and buildings from natural and environmental hazards, and unauthorized intrusions); administrative safeguards (e.g., developing information security policies and procedures, appointing a security officer, sanctioning violations, and providing regular training);[39] and technical safeguards (e.g., policies and procedures governing access and disposal of electronic PHI).[40]

In addition, the HITECH breach notification procedures require giving notice to every person affected by any breach involving PHI. Such notices must be issued within sixty days of the discovery of the breach, and if the breach involves more than 500 people, the Department of Health and Human Services (HHS) must be notified. Similarly, the regulations require a

---

38. *See* 45 C.F.R. § 160.103, *available at* http://www.hipaasurvivalguide.com/hipaa-regulations/160-103.php; *Health Information Privacy*, *Business Associates*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES (last revised Apr. 3, 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.

39. *Summary of HIPAA Security Rule*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html (last visited September 10, 2015).

40. *HIPAA Security Series*, *Technical Safeguards*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (last visited October 9, 2015).

statement to the media if the breach involves more than 500 individuals.[41] These regulations directly affect those who perform legal services for entities such as hospitals, insurers, or other businesses in the medical industry.

The Administrative Simplification provisions of HIPAA establish a baseline level of standards and requirements for the transmission and handling of health information. The provisions are intended to improve the efficiency and effectiveness of the health care system while protecting patient privacy, and they can be adopted to provide useful benchmarks for LSPs who work outside the HIPAA arena.

The BA concept can have useful application to sensitive information beyond HIPAA.[42] Practical experiences that have been gained in the health care industry provide useful guidance for LSPs seeking to protect client information of any type when sharing it with third parties. This is especially true with respect to BA contracts that ensure PHI will be safeguarded. The BA contract clarifies and limits the permissible uses and disclosures of PHI by the business associate. A BA may use or disclose protected health information only as permitted or required by its business associate contract or as required by law.

Under HIPAA, a BA is directly liable and subject to civil, and possibly criminal, penalties for improperly using and/or disclosing PHI. A BA is also directly liable and subject to civil

---

41. 45 C.F.R. § 164.408, *Health Information Privacy*, *Instructions for Submitting a Notice of Breach to the Secretary*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

42. *See* Iliana Peters, HHS Office for Civil Rights, *Lessons Learned From Recent HIPAA Breaches*, presented at Safeguarding Health Information: Building Assurance through HIPAA Security, Washington, DC (September 3, 2013), http://csrc.nist.gov/news_events/hipaa-2015/presentations/2-7-peters-update-hipaa-compli.pdf.

penalties for failing to safeguard electronic PHI in accordance with the HIPAA Security Rule. Although such statutory liability is not usually available with ordinary service contracts into which LSPs enter, indemnification clauses are, of course, an option. See discussion at Part IV.C.3.n., *supra*. The BA guidance provides a thorough framework to implement similar contracts to help protect non-HIPAA regulated information.

Accordingly, LSPs that handle protected information must enter into BA agreements with their covered clients and establish appropriate administrative safeguards for the protection of the confidential records. The written BA agreement must also provide for the destruction or disposition of all protected information at the end of any engagement. In the event of a breach, which is defined as the "impermissible acquisition, access, use, or disclosure of PHI (paper or electronic), which compromises the security or privacy of the PHI,"[43] the LSP must follow HHS[44] or Federal Trade Commission (FTC)[45] Breach Notification procedures, as appropriate. Application of the BA safeguards to all sensitive information enhances the defensibility of security measures and predictability should anything go wrong.

The Health and Human Services (HHS) Office of Civil Rights (OCR) is responsible for enforcement of the HIPAA Privacy and Security Rules and the confidentiality provisions of

---

43. *Id*.

44. *Health Information Privacy, Breach Notification Rule*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule (last visited June 3, 2015).

45. *Complying with the FTC's Health Breach Notification Rule*, FEDERAL TRADE COMMISSION (Apr. 2010), https://www.ftc.gov/system/files/documents/plain-language/bus56-complying-ftcs-health-breach-notification-rule.pdf.

the Patient Safety Act and Rule. The OCR maintains responsibility for review of entities such as hospitals, pharmacies, health insurance companies, managed health care plans, employer group health plans, and government health plans such as Medicare and Medicaid. Like the OCR, the FTC also plays an important role in the oversight and enforcement of the HIPAA Privacy and Security Rules.

HIPAA established for the first time a set of standards to address the use and disclosure of individually identifiable health information. In coordination with OCR, the FTC promulgated its Health Breach Notification Rules.[46] The FTC breach notification requirements implements § 13402 of the HITECH Act and requires HIPAA-covered entities and their BAs to provide notification following a breach of unsecured, protected, health information. Similar breach notification provisions are implemented and enforced by the FTC for personal health records, pursuant to § 13407 of the HITECH Act (e.g., the FTC Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (2014)).

Outside the healthcare context, the U.S. Commodity Futures Trading Commission (CFTC) Staff Advisory No. 14-21 (Feb. 26, 2014) contains similar useful guidance regarding best practices. Under the HITECH Act, State Attorneys General also maintain legal authority to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules. Toward that end, the OCR developed HIPAA Enforcement Training to help State Attorneys General and their staff use their new authority to enforce the HIPAA Privacy and Security Rules.[47] This guidance can also be useful to

46. *Id*.

47. *Health Information Privacy*, *HIPAA Enforcement Training for State Attorneys General*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES,

LSPs in understanding the process by which State Attorneys General may review and investigate HIPPA-related complaints.

The HIPAA privacy rule governs how a legal service provider is expected to handle the use or disclosure of PHI. In general, when State law is "more stringent,"[48] then State law will supersede the HIPAA privacy rule. Conversely, if a HIPAA state law is less stringent, then federal HIPAA rules apply. State law is considered to be "more stringent" than the HIPAA Privacy Rule if it relates to the privacy of individually identifiable health information and provides either greater privacy protections for individuals' PHI, or greater rights to individuals with respect to that information, than does the Privacy Rule.[49] The definition of the "more stringent" standard is set out at 45 C.F.R. § 160.202.

Finally, the National Institute of Standards (NIST) in collaboration with the National Cybersecurity Center of Excellence (NCCoE) has developed and released a first draft of a cybersecurity practice guide to help organizations of all kinds and sizes deploy technical standards that promote the secure collection, storage, processing, and transmission of PHI contained on mobile devices. Organizations can use some or all of the NCCoE guide to help them implement health care industry standards

---

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html (last visited September 10, 2015).

48. For a definition of what is considered to be a 'more stringent' HIPAA state standard, *see* 45 C.F.R. § 160.202, *available at* http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec160-203.pdf (last visited June 3, 2015).

49. *Health Information Privacy*, *State Attorneys General*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/ (last visited June 3, 2015).

and best practices, as well as those in the NIST Framework for Improving Critical Infrastructure Cybersecurity.[50]

50. The draft guide is available to download in sections from NIST *at* https://nccoe.nist.gov/projects/use_cases/health_it/ehr_on_mobile_devices:

SP 1800-1a: Executive Summary

SP 1800-1b: Approach, Architecture, and Security Characteristics

SP 1800-1c: How-To Guide

SP 1800-1d: Standards and Controls Mapping

SP 1800-1e: Risk Assessment and Outcomes

These standards provide valuable guidance to LSPs who are working to establish healthcare eDiscovery standards for the collection, production, and transmission of PHI.

APPENDIX B: PRIVACY AND SECURITY IN THE FINANCIAL SERVICES INDUSTRY

A. Financial Services Defined

Law firms and other LSPs in the U.S. also face a complex blend of security and privacy regulations and guidelines relating to financial information collected or used by financial institutions. The term "financial institution" is broad and potentially includes not only banks and brokerages but also check-cashing businesses, data processors, mortgage brokers, non-bank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers. The common denominator here is the range and sensitivity of personal data typically collected or held by these financial institutions, which includes names, addresses, phone numbers, bank and credit card accounts, income and credit histories, and social security numbers.

Much of the regulatory activity surrounding financial services stems from the individual and systemic importance, and significant risks associated with the handling, of such information. The wide range of potential actors, the extensive access by many LSPs to confidential financial information, and specific references to service providers in the relevant rules, have led to elevated regulatory scrutiny of the financial services sector and raised its litigation risk profile.

B. LSPs Are Particularly Vulnerable to Loss of Confidential Information

LSPs are commonly entrusted with highly sensitive and valuable financial information, both directly by their clients and because of their work with other parties. With such access comes a high level of scrutiny and risk. Wrongdoers often consider LSPs to be weak links in the information security chain and

therefore are easy targets. According to Mary Galligan, the former head of the cyber division in the New York City office of the U.S. Federal Bureau of Investigation, "as financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it's a much, much easier quarry."[51] Similarly, Richard Vallanueva, special agent for the United States Secret Service Electronic Crimes Task Force, states that hackers are increasingly targeting law firm escrow accounts as the path of least resistance. Mandiant, a specialized security firm, estimated in 2012 that eighty major U.S. firms were hacked each year.[52] That number may, in fact, be too low. While law firms are reticent to make public such breaches of security, Bloomberg reported in 2012 on the deliberate infiltration by China-based hackers of the computer networks of seven different Canadian law firms, as well as the Canadian Finance Ministry and Treasury Board.[53] The hackers stole important information in what appears to have been an attempt to derail a $40 billion acquisition of a potash producer by an Australian mining company.[54]

Confidential client information held by law firms has also received attention from governmental actors. Documents revealed by Edward J. Snowden showed that, in the course of representing the government of Indonesia in trade negotiations with the U.S., at least one global law firm's privileged client communications were intercepted by an Australian governmental security agency, which passed them on to the U.S. National

51. Michael A. Riley & Sophia Pearson, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, BLOOMBERG TECHNOLOGY (Jan. 31, 2012), http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.

52. *Id*.

53. *Id*.

54. *Id*.

Security Agency (NSA).[55] According to the *New York Times* article, "[o]ther documents obtained from Mr. Snowden reveal that the NSA shares reports from its surveillance widely among civilian agencies."[56]

Financial institutions have taken notice, and they are increasingly subjecting law firms to exacting data security and handling requirements and examination. These standards may vary slightly according to the nature of the information received, but baseline compliance on a number of security and confidentiality measures is growing as a measure of continued relationship success. Accordingly, whether viewed from a legal, business, or ethical standpoint, law firms need to consider the wide variety of threats to the security of the information they possess and take reasonable steps to safeguard their systems and clients' information from accidental or intentional breach. In particular, where the firm works with financial institutions, these issues should be considered early in the relationship because later scrambling efforts may be insufficient for a continued client relationship.

1. GLBA Privacy Rule

There is a growing body of law and regulation governing financial services information security and privacy. Foremost is the Financial Services Modernization Act of 1999 (the "Gramm-Leach-Bliley Act," or GLBA). The GLBA requires financial institutions to implement privacy and security protections to ensure the protection of consumers' information. In a form and structure similar to HIPAA, the GLBA created separate but interdependent obligations designed to minimize the risk associated

55. *See* James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES, Feb. 15, 2014, *available at* http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html.

56. *Id*.

with third-party access and use of financial data. The GLBA provides for the implementation of standards to limit the purposeful disclosure of and protection against unauthorized access to consumers' "nonpublic personal information." The privacy rule focuses on notification, opt-out rights, and limits on use and disclosure. The security rule addresses security risks. In 2003, the FTC created separate rules for privacy and security to require financial institutions to "explain their information-sharing practices to their customers and to safeguard sensitive data."[57] The FTC and its regulatory cousins, the FRB, OCC, FDIC, SEC, NCUA, OTS, and CFTC[58] collaborated to develop, through consumer testing, "privacy notices that consumers can understand

57. *Gramm-Leach-Bliley Act*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited June 3, 2015).

58. The Federal Reserve Board (FRB) is the governing body of the Federal Reserve System. *See* http://www.federalreserve.gov/. Office of the Comptroller of the Currency (OCC) "charters, regulates, and supervises all national banks and federal savings associations as well as federal branches and agencies of foreign banks." *See* http://www.occ.gov/. The Federal Deposit Insurance Corporation (FDIC) provides deposit insurance for depositors. *See* https://www.fdic.gov/. The U.S. Securities and Exchange Commission (SEC) acts to "protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation." *See* http://www.sec.gov/. The National Credit Union Administration (NCUA) regulates, charters, and supervises federal credit unions. *See* http://www.ncua.gov/. The Office of Thrift Supervision (OTS) was formerly tasked with providing support for federally and state-chartered savings banks and savings and loans associations; OTS ceased operations on October 19, 2011. The U.S. Commodity Futures Trading Commission (CFTC) operates to "protect market participants and the public from fraud, manipulation, abusive practices and systemic risk related to derivatives—both futures and swaps—and to foster transparent, open, competitive and financially sound markets" by policing the derivatives markets. *See* http://www.cftc.gov/index.htm.

and use to compare financial institutions' information collection and sharing practices."[59]

The GLBA distinguishes between consumers and customers, and imposes different obligations to provide privacy notifications to each. A consumer is an "individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons." In contrast, a "customer is a consumer with a continuing relationship with a financial institution." This distinction is important, because only customers are entitled to receive a financial institution's privacy notice automatically, while consumers may receive a privacy notice from a financial institution only if, and when, a company shares the consumer's information with unaffiliated organizations.

2. GLBA Security or Safeguards Rule

The security or "Safeguards" Rule applies to those "significantly engaged in providing financial products or services to consumers, including check-cashing businesses, data processors, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers."[60]

---

59. *Financial Privacy Rule: Interagency Notice Research Project*, FEDERAL TRADE COMMISSION (Apr. 15, 2010), http://www.business.ftc.gov/documents/0496-financial-privacy-rule-interagency-notice-research-project; for an example of congressional actions to tighten up security and breach notification laws, *see U.S. Congress Ready To Enact Data Security And Breach Notification Rules After Recent Consumer Data Breaches*, JONES DAY (Feb. 20, 2014), http://www.jonesday.com/us-congress-ready-to-enact-data-security-and-breach-notification-rules-after-recent-consumer-data-breaches-02-14-2014.

60. *See Safeguarding Customers' Personal Information: A Requirement for Financial Institutions*, FEDERAL TRADE COMMISSION (May 2002), https://www.ftc.gov/system/files/documents/plain-language/alt115-safeguarding-customers-personal-information-requirement-financial-institutions.pdf.

The FTC requires a written information security plan and delineates five core program components for safeguarding information, with the actual design and ultimate implementation dependent on, and appropriate to, variations in size, complexity, nature and scope of activities, and the sensitivity of customer information. Similar to HIPAA's Business Associate relationship, the Safeguards Rule explicitly requires financial institutions to include security safeguard language in their contractual relationships with service providers, including law firms. Covered financial institutions must:

- designate the employee or employees to coordinate the safeguards;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks;
- design a safeguards program, and detail the plans to monitor it;
- select appropriate service providers and require them (by contract) to implement the safeguards; and
- evaluate the program and explain adjustments in light of changes to its business arrangements or the results of its security tests.[61]

61. *Safeguarding Customers' Personal Information: A Requirement for Financial Institutions*, FEDERAL TRADE COMMISSION (May 2002), https://www.ftc.gov/system/files/documents/plain-language/alt115-safeguarding-customers-personal-information-requirement-financial-institutions.pdf (last visited June 3, 2015) (citing to FTC Safeguards Rule 16 C.F.R. Part 314 and http://www.nacua.org/nacualert/docs/GrammLeachBliley_Act/16_CFR_314.pdf).

While the FTC explicitly allows flexible implementation of the rules and programs, it also provides both general and specific guidance to financial institutions. Considerations proposed by the FTC include, but are not limited to, the following:

- Employee training and management
- Encryption and password protocols
- Robust preventative and reactive auditing for data at rest, in transit, and during use
- Individual, network, and Web-based programs and controls
- Proper and secure disposition of confidential information[62]

The FTC has also issued a variety of publications designed to provide more granularity around its general safeguards.[63]

In much the same fashion as HIPAA, LSPs in contact with information covered by GLBA must implement administrative, technical, and physical safeguards that are documented and audited. These "umbrella" categories do not create a bright line of "reasonableness" for assessing or auditing information security and privacy safeguards, although they do provide sufficient detail within a flexible framework—tailored to the nature of the information at issue—to guide LSPs within the scope of the GLBA.

---

62. *Financial Institutions and Customer Information: Complying with the Safeguards*, FEDERAL TRADE COMMISSION (Apr. 2006), http://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

63. *See*, e.*g.*, *Protecting Personal Information, A Guide for Business*, FEDERAL TRADE COMMISSION (Nov. 2011), http://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

3. Enforcement

Regulatory enforcement of these regulations and others relating to financial sector security and the privacy of consumer information vary greatly depending on the nature and size of the institution. The FTC has authority to enforce the law with respect to "financial institutions" that are not covered by the federal banking agencies, the OCC, the SEC, the CFPB, and the FDIC. The FTC uses its FTC Act Section 5 authority when enforcing the Safeguard Rule of the Gramm-Leach-Bliley Act to determine whether a company's information security measures were reasonable and appropriate.[64] The OCC, SEC, CFPB, FDIC, and various state regulatory agencies, also have enforcement capabilities in this area.

The authority to regulate and enforce information and security protections for LSPs is both express and implied. On April 13, 2012, the CFPB issued a bulletin defining its enforcement power, with a particular emphasis on the impact of service providers to financial institutions. The bulletin noted CFPB's goal to ensure compliance with "Federal consumer financial law," including GLBA and its implementing regulations, the Privacy Rule and the Safeguards Rule, noting that legal responsibility for the conduct of service providers in addressing these rules "may lie with the supervised bank . . . as well as with the supervised service provider." The CFPB expects supervised banks to have an effective process for managing the risk of their service providers, including reviewing and monitoring the service providers' policies, procedures, internal controls, and training materials.

64. Jennifer Woods, *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5*, ABA, http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html (last visited June 3, 2015).

The OCC also addressed third-party risk on October 30, 2013, highlighting the following:[65]

- Risk management should be commensurate with the level of risk and complexity of its third-party relationships.
- Regulated entities should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the third-party business relationship includes:
    1. plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party;
    2. proper due diligence in selecting the third party;
    3. written contracts that outline the rights and responsibilities of all parties;
    4. ongoing monitoring of the third party's activities and performance;
    5. contingency plans for terminating the relationship in an effective manner;
    6. clear roles and responsibilities for overseeing and managing the relationship and risk-management process;
    7. documentation and reporting that facilitates oversight, accountability, monitoring, and risk management; and

65. OCC BULLETIN 2013-29, Third-Party Relationships, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Oct. 30, 2013), http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

8. independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

Shortly after addressing third-party risks, the OCC developed a set of "heightened expectations" to strengthen governance and risk-management practices at large banks and federal savings institutions to enhance the agencies' supervision of those institutions. On January 16, 2014, the OCC issued proposed guidelines pursuant to section 39 of the Federal Deposit Insurance Act that enhance and formalize these expectations. These expectations include:

- roles and responsibilities definition relating to the three lines of defense; and[66]
- strategic plans from critical stakeholders on risk management Risk Appetite Statement.

---

66. *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of 12 CFR Parts 30 and 170*, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Jan. 10, 2014), http://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-4a.pdf:

> i) The first line is provided by the business units—comprising the business units, support functions, and embedded operational risk staff.
>
> ii) The second line is provided by the risk management function—comprising the operational risk management function and the compliance functions. To qualify in this category, the risk management function usually demonstrates the qualities detailed in the operational risk management function section.
>
> iii) The third line is the audit function. A number of TSA firms have outsourced their audit function. The underlying arrangements and effectiveness of an outsourced audit function should be assessed for its suitability.

The FDIC has also issued its own guidelines ("Interagency Guidelines") for information security standards, as required by Section 39 of the FDIC Act and Section 501 and 505(b) of the GLBA. These guidelines address administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. The Security Guidelines set forth specific requirements that apply to a financial institution's arrangements with service providers.

An institution must:

- exercise appropriate due diligence in selecting its service providers;
- require its service providers by contract to implement appropriate measures designed to meet the objectives of the Security Guidelines; and
- where indicated by its risk assessment, monitor its service providers to confirm that they have satisfied their obligations under the contract described above.[67]

A service provider is *any* party that is permitted access to a financial institution's customer information through the provision of services directly to the institution. Examples of service providers include a person or corporation that tests computer systems or processes customers' transactions on the institution's behalf, document-shredding firms, transactional Internet banking service providers, and computer network management firms. LSPs are generally engaged directly by the institution and

67. *See Interagency Guidelines Establishing Information Security Standards*, FDIC (Apr. 20, 2014), https://www.fdic.gov/regulations/laws/rules/2000–8660.html; *see also Interagency Guidelines Establishing Information Security Standards*, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, n. 2 (Aug. 2, 2013), http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm#fn2.

so would likely fall within the definition of service provider and, therefore, assume the obligation and expectation of compliance with the detailed FDIC security guidelines.[68] Another potential benchmark for reasonableness of which LSPs should be aware is a separate initiative led by large financial institutions to standardize third-party risk assessments.

The Shared Assessments Program is rooted in ISO 27001 and uses a Standard Information Gathering program (SIG) to collect details about a service provider's controls (people, process, and procedures), and is supported by a verification protocol to ensure accurate assessment and reporting. The Shared Assessments was created by the Bank of America Corporation, The Bank of New York Mellon, Citibank, JPMorgan Chase & Company, U.S. Bankcorp, and Wells Fargo & Company in collaboration with leading service providers and the Big Four accounting firms to help financial services companies assess service providers. In 2014, the Shared Assessments issued results of its Vendor Risk Management Survey, with a third of the responses coming from financial institutions. The survey was based on the following eight vendor risk categories:

1. Program Governance
2. Policies Standards Procedures
3. Contracts
4. Vendor Risk Identification and Analysis

68. On a related note, agency-reporting requirements on privacy breaches are now accompanied by disclosure obligations for cybersecurity risks and cyber incidents. On October 13, 2011, the SEC Division of Corporation Finance issued guidance on disclosure obligations relating to cybersecurity risks and cyber incidents. The guidance applies to domestic and non-U.S. SEC registrants to assist registrants in preparing disclosures under the Securities Act of 1933 and the Securities Exchange Act of 1934. *CF Disclosure Guidance: Topic No. 2*, U.S. SECURITIES AND EXCHANGE COMMISSION (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

5. Skills and Expertise
6. Communication and Information Sharing
7. Tools, Measurement, and Analysis
8. Monitoring and Review[69]

CONCLUSION

Both the health care services and financial services industries are subject to laws and regulations that: (1) impose security standards on industry members; (2) require special service contracts between those who collect information directly from consumers and those who provide services to them; (3) require notification to consumers when security lapses result in the loss of information pertaining to a non-*de minimis* number of consumers; and (4) subject those who lose data to potential legal liability. Keeping abreast of the best and current practices in these industries may be informative to the LSPs in establishing processes and programs for not only dealing with information obtained from those industries, but also for treating privacy-related and other confidential information obtained from others.

69. Shared Assessments, https://www.sharedassessments.org/ (last visited June 3, 2015).

THE SEDONA CONFERENCE COMMENTARY ON PROTECTION OF PRIVILEGED ESI*

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

Author: The Sedona Conference

Editor-in-Chief: John J. Rosenthal

Team Leaders: David M. Greenwald & Patrick L. Oot

Drafting Team:

Denise E. Backhouse
Kevin F. Brady
Arthur C. Fahlbusch
Adrian Fontecilla
Daniel K. Gelb
Goutam U. Jois
Colleen M. Kenney
Jessica Ross
Matthew M. Saxon
Christopher J. Spizzirri
Ariana J. Tadler
Pamela Williams

Judicial Participants:

Hon. Joy Flowers Conti
Hon. John M. Facciola
Hon. Audrey G. Fleissig
Hon. James C. Francis
Hon. Frank Maas
Hon. Andrew J. Peck
Hon. Lee H. Rosenthal
Hon. Thomas J. Shields
Hon. Karla R. Spaulding

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members 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 Sustaining 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.

PREFACE

Welcome to the final, December 2015, version of The Sedona Conference *Commentary on Protection of Privileged ESI*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). The Sedona Conference is a 501(c)(3) research and educational institute that exists to allow leading jurists, lawyers, experts, academics, and others, at the cutting edge of issues in the areas of antitrust law, complex litigation, and intellectual property rights, to come together in conferences and mini-think tanks called Working Groups to engage in true dialogue, not debate, in an effort to move the law forward in a reasoned and just way.

The public comment version of The Sedona Conference *Commentary on Protection of Privileged ESI* was published in November 2014 after more than two years of dialogue, review, and revision, including discussion at two of our Working Group 1 meetings. After nearly a four month public comment period, during which The Sedona Conference sponsored a public webinar on the Commentary, the editors have fully considered and incorporated into this final version as appropriate the extensive comments received. I thank all those who submitted comments as well as the drafting team members for their dedication and contribution to this project. Special acknowledgement goes to Denise E. Backhouse, Kevin F. Brady, Arthur C. Fahlbusch, Adrian Fontecilla, Daniel K. Gelb, Goutam U. Jois, Colleen M. Kenney, Jessica Ross, Matthew M. Saxon, Christopher J. Spizzirri, Ariana J. Tadler, and Pamela Williams. I also thank the following Judicial Observers for their participation and assistance in creating this Commentary: Hon. Joy Flowers Conti, Hon. John M. Facciola, Hon. Audrey G. Fleissig, Hon. James C. Francis, Hon. Frank Maas, Hon. Andrew J. Peck, Hon. Lee Rosenthal, Hon. Thomas J. Shields, and Hon. Karla R. Spaulding. Finally, I especially want to recognize David M. Greenwald and Patrick

L. Oot for serving as the Team Leaders and John J. Rosenthal for serving as the Editor-in-Chief and Steering Committee Liaison.

We hope our efforts will be of immediate and practical assistance to judges, parties in litigation and their lawyers, and database management professionals. We continue to welcome comments for consideration in future updates. If you wish to submit feedback, please email us at comments@sedonaconference.org. 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
November 2015

TABLE OF CONTENTS

THE SEDONA PRINCIPLES ON PROTECTION OF PRIVILEGED ESI

Principle 1: Parties and their counsel should undertake to understand the law of privilege and its appropriate application in the context of electronically stored information.

Principle 2: Parties, counsel, and courts should make use of Federal Rule of Evidence 502(d) and its state analogues.

Principle 3: Parties and their counsel should follow reasonable procedures to avoid the inadvertent production of privileged information.

Principle 4: Parties and their counsel should make use of protocols, processes, tools, and technologies to reduce the costs and burdens associated with the identification, logging, and dispute resolution relating to the assertion of privilege.

INTRODUCTION

Since the discovery of electronically stored information ("ESI") has become common practice after the adoption of the 2006 Amendments to the Federal Rules of Civil Procedure (Fed. R. Civ. P.), we have witnessed the explosion of the sheer volume of information now subject to discovery. The ever-expanding volume of ESI complicates producing parties', especially large organizations', ability to identify, exclude from the production, and log documents subject to a claim of attorney-client privilege or work-product protection.[1] The resulting reality is that it is difficult if not impossible, even with the best processes and technology, to prevent the unintentional production of privileged materials in a large ESI production.[2]

Privilege logs "have emerged as a staple of discovery" in litigation, presumably per the requirements of Rule 26(b)(5).[3] Despite the flexibility provided by the Fed. R. Civ. P., and the admonition in the 1993 Advisory Committee Notes to Rule

---

1. *See* Hearing of the Advisory Comm. on Evidence Rules 86–88 (Jan. 29, 2007); http://www.uscourts.gov/rules-policies/archives/committee-reports/advisory-committee-rules-evidence-may-2007 (testimony of Patrick Oot, Director of Electronic Discovery & Senior Counsel, Verizon, stating that total contract and outside counsel privilege review costs in a regulatory investigation exceeding $7 million could have been avoided using Rule 502 and culling strategies to cull out and prioritize privilege review).

2. *See* Judson Atkinson Candies, Inc. v. Latini-Hohberger Dhimantec, 529 F.3d 371, 388 (7th Cir. 2008) ("Where discovery is extensive, mistakes are inevitable . . ."); MVB Mortg. Corp. v. F.D.I.C., No. 2:08-cv-771, 2010 WL 582641, at *4 (S.D. Ohio Feb. 11, 2010) ("In the context of the exchange of information during discovery, it is inevitable that errors will be made and privileged documents will sometimes be produced inadvertently. The recent amendments to Fed. R. Evid. 502 reflect this reality.").

3. Hon. John M. Facciola and Jonathan M. Redgrave, *Asserting and Challenging Privilege Claims in Modern Litigation: The Facciola-Redgrave Framework*, 4 FED. CTS. L. REV. 19, 22 (2009).

26(b)(5) that document-by-document logs may be unduly burdensome when numerous documents are withheld, parties often prepare document-by-document privilege logs.[4] In complex litigation, preparation of these logs can consume hundreds of thousands of dollars or more, and rarely "enable other parties to assess the claim" as contemplated by Rule 26(b)(5). Nor do the logs achieve the other goal of the rule—to "reduce the need for *in camera* examination of the documents."[5] Indeed, many judges will acknowledge that resolving privilege challenges almost always requires the *in camera* examination of the documents, and the logs are of little value when trying to determine the accuracy of either the factual or legal basis upon which documents are being withheld from production. In short, the procedure and process for protecting privileged ESI from production is broken.

On September 19, 2008, the President signed into law a solution to this problem—Federal Rule of Evidence (Fed. R. Evid.) 502 ("Rule 502").[6] Rule 502 was intended to address waiver of privilege claims and reduce the cost of civil discovery. Rule 502 accomplishes this in three principal ways. *First*, Rule 502(a) limits subject matter waiver to voluntary disclosures and eliminates subject matter waiver for inadvertent disclosures. *Second*, Rule 502(b) precludes waiver for inadvertent disclosures when the privilege holder took reasonable steps to prevent the disclosure and took prompt steps to rectify the error. *Third*, Rule

4. *See* DAVID M. GREENWALD, ROBERT R. STAUFFER, & ERIN R. SCHRANTZ, TESTIMONIAL PRIVILEGES, VOLUME 2 § 1:69 n.8 (Thomson Reuters 2012) [hereinafter TESTIMONIAL PRIVILEGES].

5. 1993 Advisory Committee Notes to FED. R. CIV. P. 26(b)(5).

6. *See infra* Appendix B for a discussion of the Rulemaking and Legislative History of Rule 502 citing Patrick L. Oot, *The Protective Order Toolkit: Protective Privilege with Federal Rule of Evidence 502*, 10 SEDONA CONF. J. 237 (2009).

502(d) enables federal courts to "order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding." Under this third prong, federal courts may enter orders, such as non-waiver provisions in protective orders and confidentiality orders, that will avoid any questions about whether the waiver was inadvertent or whether the holder of the privilege took reasonable steps, and the order will be binding in the case in which the order was entered and also control waiver issues in other federal and state proceedings regarding a disclosure covered by the order.[7]

Notably, Rule 502(d) permits courts to enter orders that provide that a disclosure does not constitute a waiver—regardless of the actions taken by the producing party. In sum, courts may enter orders that provide greater protection than is provided in subsections (a) and (b) of Rule 502. By reducing the risk of waiver, such an order provides parties and their counsel with a blank canvas to design and implement creative mechanisms to limit the risk of waiver for the disclosure of privileged information and reduce the tremendous cost of identifying and logging privileged documents. Thus, a federal court could enter a Rule 502(d) order to prevent waiver without regard to the reasonableness of the procedures used to identify privileged documents. Rule 502(d) also permits the parties to agree that there will be no waiver even if there is no privilege review, thereby permitting the parties to agree to use a "quick peek" or "make available production" without waiving privilege or protection.

Given the potential to eliminate the possibility of waiver and reduce the cost of privilege review, some commentators

7. Several states have adopted analogues to Fed. R. Evid. 502 (Rule 502), which to varying degrees enable litigants to minimize the cost of discovery in state court proceedings. *See infra* Appendix F.

have stated that the failure to at least ask for the entry of a Rule 502(d) order is tantamount to malpractice.[8] Despite such statements, the bench and the bar have been largely ignorant of the rule and have failed to take advantage of its protections. As Judge Paul Grimm has noted with respect to Rule 502: "to date it has not lived up to its promise . . . because parties have overlooked it and courts have not construed it consistently with its purpose . . . ."[9]

This Commentary is an attempt by The Sedona Conference to breathe some needed life into the understanding and use of Rule 502 by: (i) reminding counsel of the basics of the law on privilege in the context of modern document productions; (ii) encouraging parties, lawyers, and the courts to consider employing Rule 502(d)-type orders in every complex civil matter;

---

8. *See, e.g.*, Monica Bay, *On Stage*, LAW TECH. NEWS (April 1, 2013) (quoting U.S. Magistrate Judge Andrew J. Peck) ("I'll give you a fairly straight takeaway on 502(d). In my opinion it is malpractice to not seek a 502(d) order from the court before you seek documents.").

9. Paul W. Grimm, Lisa Yurwit Bergstrom & Matthew P. Kraeuter, *Federal Rule of Evidence 502: Has It Lived Up To Its Potential?*, XVII RICH. J.L. & TECH. 8 (2011); *see also* Smith v. Allstate Ins. Co., 912 F. Supp. 2d 242, 247–48 (W.D. Pa. 2012) ("Curiously, neither [defendant] in its motion nor Plaintiff in her response reference Fed. R. Evid. 502(b) or discuss its factors as they relate to the instant case [involving inadvertent production]. Accordingly, some information that would be helpful in resolving this issue is not before the Court."); Swift Spindrift, LTD v. Alvada Insurance, Inc., No. 09 Civ. 9342(AJN)(FM), 2013 WL 3815970, at *4 (S.D.N.Y. July 24, 2013) ("Perhaps this omission [to mention Rule 502] should not be a surprise since remarkably few lawyers seem to be aware of the Rule's existence despite its enactment nearly five years ago."); Hon. L. Rosenthal, The Phillip D. Reed Lecture Series, Evidence Rules Committee Symposium on Rule 502, Panel Discussion, *Reinvigorating Rule 502* (Oct. 5, 2012) ("Rule 502 is underutilized"); Richard Marcus, *The Rulemakers' Laments*, 81 FORDHAM L. REV. 1639, 1644 (2013) ("The reality is that not very many lawyers have used these very flexible tools."); *id.* at 1645 ("The much larger problem, however, is that lawyers simply have not noticed the rule").

(iii) articulating a "safe harbor" presumption that protects parties from claims of waiver in connection with the inadvertent production of privileged materials, provided that there is adherence to certain basic best practices in the context of ESI privilege review; (iv) encouraging cooperation among litigants to lower the cost and burden of identifying privileged information; and (v) identifying protocols, processes, tools, and techniques that can be used to limit the costs associated with identifying and logging privileged material, and avoiding or resolving disputes relating to the assertion of privileges.

PRINCIPLES AND COMMENTARIES

I. Principle 1. Parties and their counsel should undertake to understand the law of privilege and its appropriate application in the context of electronically stored information.

Commentary

Comment: Attorneys have a professional obligation to understand the law of privilege in the context of electronically stored information. That ethical duty arises from several provisions in the professional rules, including the following:

- **Duty of Confidentiality:** "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by [certain specific exceptions, e.g., to prevent death or substantial bodily harm]." ABA Model Rules of Prof'l Conduct R. 1.6(a) Confidentiality of Information (2009). "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." ABA Model Rules of Prof'l Conduct R. 1.6(c) Confidentiality of Information (2009). Virtually all states have the same or similar rules regarding a lawyer's duty of confidentiality.
- **Duty of Competence:** "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." ABA Model Rules of Prof'l Conduct R. 1.1 Competence

(2009). "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing legal study and education and comply with all continuing legal education requirements to which the lawyer is subject." ABA Model Rules of Prof'l Conduct R. 1.1, cmt. 8 (2012) (emphasis added).

- **Duty of Supervision:** ABA Model Rules of Prof'l Conduct R. 5.1 Responsibilities of Partners, Managers, and Supervisory Lawyers (2009) requires those with managerial authority to make reasonable efforts to ensure that the firm and its lawyers follow the Rules of Professional Conduct. *See also* Rule 5.3(a) Responsibilities Regarding Non-Lawyer Assistants: "A lawyer has a duty to supervise a law firm or department's junior members, paralegals, support staff, and any third-parties for whose work the lawyer is responsible."

Many judges who have conducted *in camera* reviews of documents withheld from production under claims of privilege come to the conclusion that many litigants and their counsel have little understanding of the law of privilege or how to apply that law in the context of the production of ESI. A detailed discussion of the attorney-client privilege is beyond the scope of this Commentary. There are lengthy treatises devoted to the law of privilege. In addition, the law varies by jurisdiction, and applying the law to specific situations requires a thorough understanding of the factual nuances of each unique situation. However, practical guidance about identifying and protecting privileged ESI cannot start without a basic review of the law of privilege and, in particular, what may legitimately be deemed

privileged and how to avoid waiving the privilege. Only with this basic understanding can parties avoid the common practices of claiming privilege for ESI that is not privileged and waiving privilege of ESI.

A. Attorney-Client Privilege

Fed. R. Evid. 501 provides for the application of federal common law of privilege when jurisdiction is based on a federal question.[10] In most cases brought under the federal courts' diversity jurisdiction, and in other federal proceedings "with respect to an element of a claim or defense as to which state law supplies the rule of decision," state law of privilege applies.[11] State law regarding privilege issues, of course, also applies in state court proceedings. Each jurisdiction has its own articulation of the privilege, and there are considerable differences among jurisdictions regarding the scope and application of the privilege.

However, there are generally four common elements across jurisdictions: (1) a communication, (2) made between privileged persons, (3) in confidence (and kept in confidence),

---

10. Fed. R. Evid. 501 provides in pertinent part:

> [T]he privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law.

See also TESTIMONIAL PRIVILEGES, *supra* note 4, at § 1:3.

11. TESTIMONIAL PRIVILEGES, *supra* note 4, at § 1:3.

and (4) for the purpose of obtaining or providing legal assistance for the client.[12] The privilege protects communications, but it does not permit a party to resist disclosure of the facts underlying the communications.[13] Key aspects of these elements are discussed below.

Persons. Communications between "privileged persons" *may* include those between employees, in-house counsel or outside counsel, and any of the company's subsidiaries or affiliates, and any combination of them. These could be communications: (i) from employees to counsel; (ii) from counsel to employees; (iii) between counsel; (iv) between employees or their functional equivalents;[14] or (v) with qualified agents of counsel or the client (e.g., employees or counsel of an agent, confidential litigation consultant, or informal consulting expert).[15] It is important to note that the nature and scope of the privilege varies jurisdiction-by-jurisdiction, and certain jurisdictions limit the extent and/or existence of any claim of privilege, for example, between non-lawyer employees, or with functional equivalents and/or affiliated entities.

Scope of the Privilege. The attorney-client privilege, once established, is absolute unless waived. In order to qualify for the attorney-client privilege, a communication must have been made for the primary purpose of facilitating the rendering of legal advice.[16] If not, it will not be privileged, even if made by a

---

12. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 (2000); *see also* TESTIMONIAL PRIVILEGES, *supra* note 4, at § 1:5.

13. TESTIMONIAL PRIVILEGES, *supra* note 4, at § 1:13.

14. *Id.* at § 1:31 (*In re Bieter* doctrine is often limited to small corporate entities).

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

16. *In Re* Vioxx Products Liability Litigation, 501 F. Supp. 2d 789, 798 (E.D. La. 2007).

lawyer or in confidence. Thus, for example, a document authored by a company in-house attorney and sent to an employee would not be privileged if the communication related to business or personal matters, and not legal advice. The inquiry is whether a lawyer is being asked to render (or is rendering) some sort of legal, rather than business, advice. Such questions are often more easily answered in the affirmative when dealing with confidential communications between a client and outside legal counsel. As to communications between in-house legal counsel and company employees (or their functional equivalents), the standards for determining which company representatives may seek or obtain legal advice on behalf of a corporation vary among jurisdictions. The majority of courts today employ a "functionality" or "subject-matter" test which extends the attorney-client privilege to include a company lawyer's communications with any corporate employee so long as the communication relates to the subject matter for which the company is seeking legal representation.[17] Because in-house counsel may play multiple roles in a corporation, *some* courts apply additional scrutiny to assertions of privilege involving communications with in-house counsel, requiring in-house counsel to make

17. *See, e.g.*, *id*. at 796. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 73 (2000); *see also* TESTIMONIAL PRIVILEGES, *supra* note 4, at § 1:26 n.5. Note: Some states continue to employ the more restrictive "control group" test, which designates only upper-level management as clients of the corporate counsel. *See, e.g.*, Alaska (*see* Manumitted Cos. v. Tesoro Alaska Co., 2006 U.S. Dist. LEXIS 57658, at *7 (D. Alaska Aug. 16, 2006)); Illinois (*see* Consolidation Coal Co. v. Bucyrus-Erie Co., 89 Ill. 2d 103 (1982); Sterling Fin. Mgmt., L.P. v. UBS PaineWebber, Inc., 336 Ill. App. 3d 442, 449 (2002)); Hawaii (HAW. REV. STAT. § 626-1); Maine (ME. R. EVID. 502(a)(2)). Many other states have yet to specifically decide which test to apply. *See* Brian E. Hamilton, *Conflict, Disparity, and Indecision: The Unsettled Corporate Attorney-Client Privilege*, 1997 ANN. SURV. AM. L. 629, 630 (1997). The control group test has been explicitly rejected for use by federal courts. *See* Upjohn Co. v. United States, 449 U.S. 383, 390–92, 66 L. Ed. 2d 584, 101 S. Ct. 677 (1981).

a "clear showing" that communications were made for a legal, rather than a business purpose.[18]

Confidential. In order to be privileged, a communication must be made and maintained in confidence. Communications contained in public documents, such as final press releases and corporate annual reports, are not privileged. Also, as a general rule, if an attorney-client communication is disclosed to independent third parties (not including qualified agents of privileged persons), the communication is no longer confidential for purposes of applying the privilege.

The party asserting a privilege or protection has the burden of establishing that withheld information qualifies for protection.[19] It is, therefore, necessary for lawyers to understand the elements of privilege and to be able to articulate how each element of the privilege is satisfied for withheld information.

B. Work-Product Protection Generally

The work-product protection was originally predicated on common law, but the doctrine was codified in Rule 26(b)(3). Similar protections are found in state common law or state analogues to Rule 26(b)(3).[20] Whereas the attorney-client privilege provides an absolute privilege from discovery if established and maintained, the work-product protection provides *qualified* protection against compelled disclosure "for tangible material (or

18. *See, e.g., Vioxx*, 501 F. Supp. 2d at 799. ("While this expanded role of legal counsel within corporations has increased the difficulty for judges in ruling on privilege claims, it has concurrently increased the burden that must be borne by the proponent of corporate privilege claims relative to in-house counsel.").

19. TESTIMONIAL PRIVILEGES, *supra* note 4, at § 1:62 n.5 (attorney-client privilege), and at § 2:8 n.2 (work-product protection).

20. State court analogues to Fed. R. Civ. P. 26(b)(3) are not all as broad as the federal rule. *See, e.g.*, ILL. SUP. CT. R. 201 (protecting only opinion work product).

its intangible equivalent) prepared in anticipation of litigation or for trial."[21] In order to invoke such protection under Rule 26(b)(3), the materials must constitute: (i) a document (or tangible thing that would be otherwise discoverable); (ii) prepared by or for a party (or a party's representative); and (iii) in anticipation of litigation[22] or for trial. To establish that a document was prepared in anticipation of litigation, a party must demonstrate that the threat of litigation was "reasonably anticipated." Opinion work product, which includes the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative, is entitled to near-absolute protection.[23] Fact work product may be discovered only upon a "show[ing of] substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means."[24] When fact work product and opinion work product are mixed, a court may order that opinions or mental impressions be redacted where production of fact work product is required.[25]

Scope of Protection. Work-product protection is "distinct from and broader than the attorney-client privilege."[26] Provided

---

21. FED. R. EVID. 502(g)(2).

22. The term "litigation" as used herein and in the work-product context extends to adversarial proceedings in which the parties have the right to either: (1) cross-examine witnesses, or (2) present evidence or information to counter an opposing party's presentation. "Litigation," therefore, is defined broadly to include criminal and civil trials as well as other adversarial proceedings such as administrative hearings, arbitration, and grand jury proceedings. TESTIMONIAL PRIVILEGES, *supra* note 4, at § 2:14 n.9.

23. TESTIMONIAL PRIVILEGES, *supra* note 4, at § 2:22 nn.5–6.

24. FED. R. CIV. P. 26(b)(3)(ii).

25. TESTIMONIAL PRIVILEGES, *supra* note 4, at § 2:7 n.2, and at § 2:34 n.10.

26. United States v. Nobles, 422 U.S. 225, 238 n.11, 95 S. Ct. 2160, 2170, 45 L. Ed. 2d 141, 153 (1975).

the materials were prepared in anticipation of litigation or for trial, work-product protection will extend not only to those materials prepared by attorneys, but also to materials prepared by a party or by others at that party's or an attorney's direction. For example, materials prepared by a consultant hired by the lawyer to assist in trial preparation are generally covered by work-product protection (unless that consultant has been retained to testify at trial).[27] In addition, materials prepared by a party, without the involvement of an attorney, may be protected work product so long as the materials were prepared in anticipation of litigation or for trial.[28]

Confidentiality. Whereas the attorney-client privilege is generally waived whenever a privileged communication is disclosed outside the privileged circle of client and attorney, work product is only waived when disclosed to an adversary or to someone who substantially increases the opportunities for potential adversaries to obtain the information (a "conduit").[29] Disclosure to another person who has an interest in the information but who is not reasonably viewed as a conduit to a potential adversary will not be deemed a waiver of work-product protection.[30]

---

27. *In re* Cendant Corp. Sec. Litig., 343 F.3d 658, 664–65 (3d Cir. 2003).

28. *See, e.g.*, Angel Learning, Inc. v. Houghton Mifflin Harcourt Pub. Co., No. 1:08–cv–01259–LJM–JMS, 2010 WL 1579666, at *1 (S.D. Ind. April 19, 2010) (work-product doctrine applies to documents prepared by a party in anticipation of litigation, even where counsel is not directly involved in preparing the documents; "counsel's lack of involvement in preparing the documents has absolutely no bearing on the work-product inquiry; a party can create work product just like its counsel can, so long as the materials are prepared for litigation purposes.").

29. TESTIMONIAL PRIVILEGES, *supra* note 4, at § 2:28 nn.1–2.

30. *See, e.g., In re* Grand Jury Proceedings, 43 F.3d 966, 970 (5th Cir. 1994); Westinghouse Elec. Corp. v. Republic of Philippines, 951 F.2d 1414, 1428 (3rd Cir. 1991*);* Chase v. City of Portsmouth, 236 F.R.D. 263, 269 (E.D.

C. Common Law Waiver Prior to Rule 502

Even if a document satisfies all the requirements for the attorney-client privilege or work-product protection, that privilege/protection may nevertheless be lost through waiver. Typically, a party's disclosure of a privileged document to third parties who do not share a confidential relationship with the disclosing party (i.e., the third parties are not agents or representatives of the disclosing party or its legal counsel) constitutes waiver. Similarly, disclosure of work product to an adversary or to another party in a manner that materially increases the likelihood of disclosure to an adversary typically results in loss of the work-product protection. Furthermore, under the common law, disclosure of a privileged communication to a third party may waive the privilege with respect to the communication itself, and also with respect to other privileged communications on the same subject matter which fairness requires must be revealed ("subject matter waiver").[31]

Va. 2006); 8 CHARLES ALAN WRIGHT, ATHUR R. MILLER, MARY KAY KANE, RICHARD L. MARCUS & ADAM N. STEIMAN, FEDERAL PRACTICE & PROCEDURE § 2024 (3d ed. 2015).

31. *See* GFI, Inc. v. Franklin Corp., 265 F.3d 1268, 1272–73 (Fed. Cir. 2001) (under Fifth Circuit law, voluntary waiver of attorney-client privilege extends to all communications pertaining to the same subject matter); U.S. v. Workman, 138 F.3d 1261, 1263 (8th Cir. 1998) ("The waiver covers any information directly related to that which was actually disclosed."); United States v. Jones, 696 F.2d 1069 (4th Cir. 1982) (voluntary disclosures to a third party waive the privilege not only for the specific communication disclosed but also for all communications relating to the same subject matter); *In re* Omnicron Grp. Securities Litig., 226 F.R.D. 579 (N.D. Ohio 2005) (although internal investigation materials were otherwise privileged, production to a litigation adversary of a PowerPoint presentation summarizing the investigation, which had been presented to the Board of Directors, broadly waived the privilege over underlying documents created as of the time of the presentation).

Prior to the adoption of Rule 502, courts generally followed one of three distinct approaches to waiver based on inadvertent disclosures: (1) the strict approach, (2) the "middle" approach, or (3) the lenient approach.[32] Under the strict approach, adopted by the court in *In re Sealed Case*,[33] any document produced, either intentionally or otherwise, lost its privileged status.[34] Under the lenient approach, a party had to knowingly waive privilege; a determination of inadvertence ended the inquiry.[35]

The majority of courts applied the "middle" approach, using a case-by-case analysis to determine the reasonableness of the precautions taken to protect against disclosure and the actions taken to recover the inadvertently disclosed material. The Restatement (Third) of the Law Governing Lawyers ("the Restatement") at § 79 lists several of the factors frequently used by courts to analyze inadvertent waiver pursuant to the middle approach:

(1) the relative importance of the communication (the more sensitive the communication, the greater the necessary protective measures);
(2) the efficacy of precautions taken and of additional precautions that might have been taken;
(3) externally imposed pressures regarding the timing or the volume of required disclosure, if any;
(4) whether the disclosure was by act of the client or lawyer or by a third person; and

32. Gray v. Bicknell, 86 F.3d 1472, 1483 (8th Cir. 1996).

33. 877 F.2d 976 (D.C. Cir. 1989).

34. *Gray*, 86 F.3d at 1483; *see also In re* Grand Jury, 475 F.3d 1299 (D.C. Cir. 2007) (reaffirming the approach taken in *In re* Sealed Case).

35. *Gray*, 86 F.3d at 1483.

(5) the degree of disclosure to non-privileged persons.[36]

Judge Paul Grimm, a thought leader in this area, authored a number of very important ESI-related decisions, two of which are "must reads" in understanding the problems associated with protecting waiver of privilege in the digital information era. In *Hopson v. Mayor of Baltimore*,[37] Judge Grimm was the first jurist to address in detail the issue of whether anything less than a full document-by-document privilege review was reasonable given the volume of ESI and the time necessary to complete such a review. In what became the precursor to Rule 502, Judge Grimm discussed the need for a court to enter an order regarding the scope and process of privilege. In addition, Judge Grimm noted, in pre-Rule 502 decisions, that the issuance of such an order was essential to protecting against subject matter waiver of attorney-client privilege or work-product immunity because compliance with that order would not result in the waiver of any privilege or work-product claim for inadvertently produced privileged material.

Three years later, Judge Grimm penned *Victor Stanley, Inc., v. Creative Pipe, Inc., et al.*,[38] the seminal decision on the use of search methodology for conducting privilege review. In emphasizing the need for a uniform approach to the law of waiver and an order implementing a non-waiver agreement, Judge Grimm focused on the methodology employed by the producing party to identify privileged documents. In *Victor Stanley*, Judge Grimm found that because the defendants had used a poorly designed search protocol with no test to ascertain the validity of the protocol, the privilege was waived. In particular,

36. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 79 cmt. h (2000).

37. 232 F.R.D. 228 (D. Md. 2005).

38. 250 F.R.D. 251 (D. Md. 2008).

Judge Grimm noted that the defendants were at fault for "having failed to take reasonable precautions to prevent the disclosure of privileged information, including the voluntary abandonment of a non-waiver agreement that the Plaintiff was willing to sign." Four months after Judge Grimm issued the *Victor Stanley* decision, in September 2008, Rule 502 was enacted. Rule 502 provides significant protections against waivers of privilege. But Rule 502 was preceded by clawback agreements, and the Fed. R. Civ. P. codification of those agreements, as discussed next.

D. Federal Rule of Civil Procedure 26—Codification of the Clawback Procedure

The 2006 Amendments to Rule 26(b)(5) addressed the inherent cost and burden associated with identifying and logging privileged materials, including those arising from the increasing volumes of ESI by codifying the practice of many litigants to include in standard confidentiality agreements and protective orders a clawback procedure, whereby parties could seek the return of inadvertently produced privileged documents.

Specifically, Rule 26(b)(5) codified a procedure through which a party who has inadvertently produced privileged or work-product information may nonetheless assert a protective claim to that material. The rule provides that once the party seeking to establish the privilege or work-product claim notifies the receiving parties of the claim and the grounds for it, the receiving parties must return, sequester, or destroy the specified information. Fed. R. Civ. P. 26(b)(5) provides in relevant part:

> (5) Claiming Privilege or Protecting Trial-Preparation Materials.
> (B) Information Produced. If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material,

> the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.

Since the rule is a procedural one, it did not and could not address whether and under what circumstances inadvertent production would constitute a waiver of the privilege. In this regard, the Committee Note clearly states that the rule does not address whether the privilege or protection was waived by the production, but simply prohibits the receiving party from using or disclosing the information, and requires the producing party to preserve the information, until the claim is resolved.[39]

The 2006 Amendments also added a provision to Rule 26(f) requiring the parties to discuss the issue of privilege as part of developing a discovery plan. Rule 16(b) was also amended to allow the court to enter an order regarding any agreements the parties reached regarding issues of privilege or trial-preparation material protection.[40] While Rule 26(b)(5) was a tremendous step forward in the Rules process, it did not provide a substantive change in waiver law or provide a mechanism for parties to obtain protection from possible waiver rulings. The resolution

39. FED. R. CIV. P. 26(b)(6) Advisory Committee Notes to the 2006 Amendments.

40. *See* FED. R. CIV. P. 16(b).

of this problem would have to wait two years until the amendment of the Federal Rules of Evidence.

E. Federal Rule of Evidence 502

Federal Rule of Evidence 502 was signed into law on September 19, 2008, and is a substantial departure from the traditional approach to waiver of the attorney-client privilege and the work-product protection. The rule applies with respect to disclosures, both voluntary and inadvertent, in federal proceedings, and to federal offices and agencies. The rule itself limits the scope of waiver, and Rule 502(d) gives a federal court the power to bind parties and the courts in all other state and federal proceedings with respect to disclosures made in the federal proceeding in which the order was entered.[41]

Thus, Rule 502 reflects an effort by Congress to enable litigants to minimize the extraordinary cost of civil litigation in federal proceedings, particularly the cost of e-discovery, without risking broad waiver of privilege in either federal or state proceedings. Rule 502 provides:

> (a) Disclosure Made in a Federal Proceeding or to a Federal Office or Agency; Scope of a Waiver: When the disclosure is made in a federal proceeding or to a federal office or agency and waives the attorney-client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a federal or state proceeding only if: (1) the waiver is intentional; (2) the disclosed and undisclosed communica-

41. A number of states have enacted Rule 502 analogues, although there are differences among the state rules. *See infra* Appendix F for a discussion of state law analogues to Rule 502.

tions or information concern the same subject matter; and (3) they ought in fairness to be considered together.

(b) Inadvertent Disclosure: When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).

(c) Disclosure Made in a State Proceeding: When the disclosure is made in a state proceeding and is not the subject of a state-court order concerning waiver, the disclosure does not operate as a waiver in a federal proceeding if the disclosure: (1) would not be a waiver under this rule if it had been made in a federal proceeding; or (2) is not a waiver under the law of the state where the disclosure occurred.

(d) Controlling Effect of a Court Order: A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding.

(e) Controlling Effect of a Party Agreement: An agreement on the effect of disclosure in a federal proceeding is binding only on the parties to the agreement, unless it is incorporated into a court order.

> (f) Controlling Effect of This Rule: Notwithstanding Rules 101 and 1101, this rule applies to state proceedings and to federal court-annexed and federal court-mandated arbitration proceedings, in the circumstances set out in the rule. And notwithstanding Rule 501, this rule applies even if state law provides the rule of decision.
> (g) Definitions: In this rule: (1) "attorney-client privilege" means the protection that applicable law provides for confidential attorney-client communications; and (2) "work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial.

1. Limiting the Scope of Waiver for Voluntary Disclosures

Rule 502(a) significantly limits the scope of waiver with respect to undisclosed privileged communications or information in the context of a federal proceeding or disclosure to a federal office or agency. Specifically, Rule 502(a) eliminates subject matter waiver for inadvertent disclosures and minimizes the likelihood of subject matter waiver for intentional disclosures: "It follows that an inadvertent disclosure of protected information can *never* result in a subject matter waiver." Explanatory Note to Rule 502(a) (emphasis added). The Rules Committee explained that subject matter waiver is "reserved for those unusual situations in which fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary."

The Advisory Committee explained the very narrow circumstances in which waiver beyond the disclosed information is appropriate:

> [Rule 502(a)] provides that a voluntary disclosure in a federal proceeding or to a federal office or agency, if a waiver, generally results in a waiver only of the communications or information disclosed; a subject matter waiver (of either privilege or work product) is reserved for those unusual situations in which fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary . . . . Thus, subject matter waiver is limited to situations in which party intentionally puts protected information into the litigation in a selective, misleading and unfair manner . . . . The language concerning subject matter waiver—"ought in fairness"—is taken from Rule 106, because the animating principle is the same. Under both Rules, a party that makes a selective misleading presentation that is unfair to the adversary opens itself to a more complete and accurate presentation.

Rule 502 was intended to limit instances of subject matter waiver. There have not been many decisions that have addressed the circumstances in which subject matter waiver is appropriate under Rule 502(a). Influenced in part by Rule 502(a)'s requirement that there be a fairness balancing analysis before there can be a finding of subject matter waiver with respect to disclosures made during litigation, the Federal Circuit remanded a case and directed the trial court to conduct a fairness analysis before determining whether a pre-litigation disclosure resulted in subject matter waiver.[42]

---

42. Wi-Lan, Inc. v. Kilpatrick Townsend & Stockton LLP, 684 F.3d 1364, 1369 (Fed. Cir. 2012) ("If a party who expressly waives privilege during

The Advisory Committee Notes[43] are clear that in order for there to be subject matter waiver, disclosure must be voluntary and fairness must require subject matter waiver.[44] The legislative history supports the position that there should be no subject matter waiver unless a disclosure is voluntary and "a party's strategic use" of the disclosed privileged or protected information in litigation "obliges that party to waive the privilege regarding other information concerning the same subject matter so that the information being used can be fairly considered in context."[45]

---

litigation receives the protection of a fairness balancing test, as per Rule 502(a), should the same protection be made available to a person whose waiver occurred pre-litigation? . . . We conclude that the Ninth Circuit would find fairness balancing to be required.").

43. According to the Advisory Committee Notes, Rule 502 was submitted "directly to Congress because of the limitations on the rulemaking function of the federal courts in matters dealing with evidentiary privilege." The Advisory Committee Note also explains that the Note "may be incorporated as all or part of the legislative history of the rule."

44. In *Bear Republic Brewing Co. v. Central City Brewing Co.*, 275 F.R.D. 43, 50 (D. Mass. 2011), the court, while acknowledging the clear intention of both the Advisory Committee Notes and the legislative history to require a fairness analysis before finding subject matter waiver, nevertheless held that Rule 502(a)'s language requires a finding of subject matter waiver whenever there has been an intentional disclosure of privileged information. According to the court, a fairness analysis is relevant only with respect to the scope of the subject matter waiver. The *Bear Republic* decision demonstrates a minority view. More prevalent is the view that the purpose of Rule 502(a) is to limit subject matter waiver to rare circumstances, not to maintain the common law approach that subject waiver occurs whenever privileged information is disclosed to third parties.

45. 154 CONG. REC. H7818-7819 (September 8, 2008) (Statement of Congressional Intent Regarding Rule 502 of the Federal Rules of Evidence), 2008 WL 4133109; 23 WRIGHT & GRAHAM, FEDERAL PRACTICE AND PROCEDURE § 5438, 849–51 (Supp. 2011). *See also* Lott v. Tradesmen Int'l, Inc., No. 5:09-CV-183-KKC, 2013 WL 308853 (E.D. Ky. Jan. 25, 2013) (fairness does not require finding of subject matter waiver where disclosed privileged

If courts properly construe Rule 502(a), parties and their lawyers may now conduct a cost-benefit analysis regarding the resources that they will spend to screen for privilege, and whether to produce arguably privileged but otherwise insignificant documents rather than spend significant time and money fighting the issue in response to motions to compel. As discussed with respect to Rule 502(d) below, parties can further decrease the risk of uncertainty regarding waiver by having the court enter an order pursuant to Rule 502(d) that not only addresses the "clawback" process for inadvertently produced material, but is tailored to the needs of a specific case.

2. Voluntary Disclosures to Federal Offices and Agencies

Rule 502(a) applies not just to disclosures in a federal proceeding, but also to disclosures to federal offices and agencies whether or not there is a pending federal proceeding. Therefore, Rule 502(a) limits the scope of waiver for disclosures that parties choose to make pursuant to a voluntary disclosure of potential wrongdoing, or in response to an informal investigation by the federal government.

It is imperative, in this context, that counsel be familiar with the history of Rule 502. At one point, the Department of Justice took the position that it could insist that parties subject to its investigations or prosecutions forfeit their attorney-client or work-product privileges in order to secure favorable treatment. This led to the proposal that this policy be prohibited and the Rule 502, then being considered, create a new common law privilege which would permit a party to make a complete disclosure of all of its privileged information to the government

---

emails would not be admitted into evidence and would not be considered by the court).

without any fear that the information would be available to anyone else ("selective waiver").[46]

A rule codifying the selective waiver doctrine was necessary, because the vast majority of circuits that had considered the question had concluded that there could be no such thing as a "selective" waiver of the privilege. In the absence of the ability to selectively disclose privileged information to the government, disclosure to the government meant waiver as to all third party litigants.[47]

The effort to create this new privilege failed and, as a result, the prohibition against a selective waiver remains in most jurisdictions. Indeed, the Advisory Committee acknowledges as much in its notes to Rule 502.[48]

Production of documents to the government outside of litigation raises a procedural quandary for the producing party: while Rule 502(a) limits the scope of waiver with respect to disclosures to federal offices or agencies, the certainty of Rule 502(d) likely will not be available, because no federal court can bind other state and federal proceedings unless the disclosures were made in connection with litigation before the court. As a result, if several cases are later filed relating to the subject matter

---

46. For an excellent analysis of this history, *see* Appendix A, Martin R. Lueck & Patrick M. Arenz, *The DOJ's Evolving Position on Requests for Waiver of the Attorney-Client Privilege & Work Products Materials during Corporate Investigations* (2009).

47. *See id.* at 7–8; *see, e.g., In re* Qwest Commc'ns Int'l Inc. Sec. Litig., 450 F.3d 1179 (10th Cir. 2006) (declining to adopt selective waiver privilege and holding production to government waived privilege as to third-party civil litigants).

48. "The rule makes no attempt to alter federal or state law on whether a communication or information is protected under the attorney-client privilege as an initial matter. *Moreover, while establishing some exceptions to waiver, the rule does not purport to supplant applicable waiver doctrine generally*." FED. R. EVID. 502 Advisory Committee Note.

of the disclosures, each of those courts may have an opportunity to rule on waiver, creating a significant risk of inconsistent and unpredictable outcomes.

What if the parties obtain a Rule 502(d) order that applies to disclosure of all privileged documents—allowing a party to clawback privileged documents at any time without risk of waiver? Does this essentially create a selective waiver doctrine, and would that Rule 502(d) order be valid?

There are several arguments against this strategy, at least with respect to an order that effectively allows selective waiver by not limiting the order to inadvertently produced documents. Another party, who wants the privileged information given to the government, can argue that the party that made the disclosure has done indirectly what it could not do directly—get the very exemption from the no selective waiver rule that the drafting committee rejected. Additionally, it could be argued that the conferral of jurisdiction was collusive and constituted a fraud upon the court if it were unaware of the agreement the parties had made. If that argument were accepted by another court, then the court that issued the order lacked jurisdiction over the subject matter since the dispute was not a true case or controversy and jurisdiction was procured by a fraud upon the court.[49]

In the absence of dispositive authority, counsel may nevertheless conclude that having such an understanding with the government may be worth running the risk that the Rule 502(d) order that the parties secure by their understanding will ultimately be set aside. For example, the risk of subsequent litigation may be so slim that counsel can conscientiously advise her client that weighing that risk against what could be the prohibitive costs of review still renders this kind of agreement a legitimate strategy. It should be recalled that the privilege belongs

49. FED. R. CIV. P. 60(b)(4).

to the client and a fully advised client can waive it and run whatever risk that client sees fit to run.

3. "Use" vs. "Disclosure"

There is a significant limitation to Rule 502(a). It applies to "disclosures," but it does not purport to apply to "use" of privileged information by a producing party. "Use" includes not just the affirmative use of a produced privileged document as an exhibit in support of summary judgment or at trial, but also when a party puts "at issue" privileged information.[50] Although disclosure of a privileged document may not result in subject matter waiver, a producing party's use of that document may force the application of Rule 502(a) compelling the production of otherwise privileged information that "ought in fairness to be considered" with the document that party used.[51]

This issue is particularly important as parties consider whether to produce privileged information to the government. Although Rule 502(a) specifically applies to disclosures to federal offices and agencies, some may assert that such disclosures are "use" of privileged information to the extent that a party makes the production to obtain cooperation credit or otherwise obtain leniency from the government.

---

50. TESTIMONIAL PRIVILEGES, *supra* note 4, at § 1:88.

51. *See* Shinogi Pharma, Inc. v. Mylan Pharmaceuticals, Inc., No. 10-1077, 2011 WL 6651274 (D. Del. Dec. 21, 2011) (the doctrine that reliance on the advice of counsel waives the attorney-client privilege remains unaffected by Rule 502); *see also* Graff v. Haverhill North Coke Co., No. 1:09-cv-670, 2012 WL 5495514 (S.D. Ohio Nov. 13, 2012) (voluntary disclosure of the final version of an investigation report that concluded that the producing party was in compliance with the law, and the assertion of an affirmative defense that it was compliant, put the report "at issue" in the litigation. Defendant, therefore, was required to produce draft versions of the report and any email communications with counsel regarding the report).

If the courts were to find that most voluntary disclosures to government agencies constituted "use," it would effectively read the protections out of Rule 502(a). As the United States Supreme Court has emphasized, in order to be effective, the scope of the attorney-client privilege must be predictable.[52] Uncertainty regarding whether disclosure—of some otherwise privileged or protected information developed during a corporate internal investigation—will lead to wholesale loss of the privilege for the entirety of the investigation makes it less likely that a company will risk disclosing what may be helpful information for the government's investigation.

In order to give Rule 502(a) its intended reach, the best approach is to reserve the waiver required by that rule for only those situations in which it is clear that a party disclosing privileged information to the government is attempting to "cherry pick" in an effort to mislead the government. The act of disclosure itself, without evidence that the disclosing party has "intentionally" provided the privileged or protected information in a "selective, misleading and unfair manner," should not constitute "use" of the information, and should not result in waiver of anything other than the limited waiver in Rule 502(a). A finding of such a waiver following disclosure to the government should be an unusual exception, not the norm.

---

52. *See* Upjohn Co. v. United States, 449 U.S. 383, 393 (1981) ("But if the purpose of the attorney-client privilege is to be served, the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected. An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all. The very terms of the test adopted by the court below suggest the unpredictability of its application.").

II. Principle 2. Parties, counsel, and courts should make use of Federal Rule of Evidence 502(d) and its state analogues.

Commentary

Comment 2(a): Rule 502(d) provides parties with a vehicle to ensure that the production of ESI does not result in waiver regardless of the circumstances of its production.

Rule 502(d) provides: "A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding." An agreement among the parties on the effect of disclosure in a federal proceeding, however, binds only the parties to the agreement, unless it is incorporated into a court order.[53]

Rule 502(d) gives a federal court broad power to enter an order ruling that the parties' conduct in a proceeding before the court does not result in waiver. A Rule 502(d) order may address not only inadvertent waiver, but also instances in which intentional disclosure will not result in waiver. Thus, a Rule 502(d) order can be crafted to expedite discovery and save costs by obviating the risk that disclosure will result in waiver. Moreover, once a court has entered a Rule 502(d) order establishing the rules that will govern the production of privileged documents, the order eliminates the need to refer to Rule 502(b), or to establish the elements set forth in that rule.[54]

---

53. FED. R. EVID. 502(e). It is important to recognize that a Rule 502(d) is "available not only to litigants, but also to third-parties" who are producing information, for instance, pursuant to a subpoena. Thomas C. Gricks, *The Effective Use of Rule 502(d) in E-Discovery Cases*, THE LEGAL INTELLIGENCER (Oct. 25, 2011).

54. *See* Rajala v. McGuire Woods, LLP, No. 08-2638-CM-DJW, 2013 WL 50200 (D. Kan. Jan. 3, 2013) (Rule 502(d) order is designed to allow the parties and the court to defeat the default operation of Rule 502(b) in order to reduce costs and expedite discovery); Brookfield Asset Mgmt., Inc. v. AIG

To date, Rule 502(d) has mostly been used to establish under what circumstances, if any, the production of privileged information can constitute or not constitute grounds for waiver.[55] The parties could agree that the unintentional or inadvertent production of privileged information cannot result in a waiver regardless of whether the producing party undertook the reasonable efforts to preclude its production. Similarly, the parties could also agree that the intentional production of privileged information does not result in a waiver. For example, one party might agree to produce certain "privileged" documents such as legal opinions explaining the basis of its actions. Under a 502(d) agreement, the parties might agree that the production of those documents would not constitute a broader waiver of any claim to privilege over similar documents or similar communications.[56]

Fin. Prods. Corp., No. 09 Civ. 8285(PGG)(FM), 2013 WL 142503 (S.D.N.Y. Jan. 7, 2013) (Maas, J.) (holding that party that, due to vendor error, produced privileged material contained in the metadata of redacted documents had "the right to claw back the [documents], no matter what the circumstances giving rise to their production were" because "the parties at [the Court's] urging had entered into a Rule 502(d) [order]"); s*ee also* United States v. Daugerdas, No. S3 09 CR 581(WHP), 2012 WL 92293 (S.D.N.Y. Jan. 11, 2012) (denying defendant's motion to unseal privileged document produced by defendant's employer pursuant to Rule 502(d) order in criminal case, explaining that allowing the document to be unsealed for use in a private arbitration proceeding between defendant and employer regarding legal fees incurred in connection with the criminal case would defeat the purpose of the 502(d) order).

55. S.E.C. v. Bank of Am. Corp., 2009 WL 3297493 (S.D.N.Y. Oct. 14, 2009) (entering order pursuant to Rule 502(d) to limit waiver to documents actually disclosed to government and adopting parties' definition of subject matter of the disclosed documents).

56. Shinogi Pharma, Inc. v. Mylan Pharmaceuticals, Inc., No. 10-1077, 2011 WL 6651274 (D. Del. Dec. 21, 2011) (the Rule 502(d) order provided that, if the producing party elected not to rely on the disclosed opinions, the receiving party was required to return or destroy all copies of the opinions and,

Once entered by the court, the Rule 502(d) order provides the producing party with protection from a claim of waiver by the opposing party. Most importantly, Rule 502(d) provides that such an order is enforceable in all other federal and state proceedings.[57] Prior to the adoption of Rule 502, these arrangements were enforceable as to the parties to a specific federal proceeding,[58] but there was no certainty that a confidentiality agreement, protective order, or even a ruling by the court that there had been no waiver would be followed by other courts involving different parties.[59] By incorporating such agreements in a court order pursuant to Rule 502(d), the parties can be certain that such a non-waiver order will control waiver issues regarding that disclosure in other matters.

Comment 2(b): Absent good cause shown by one of the parties, courts should enter Rule 502(d) clawback/non-waiver orders as a matter of course when parties fail to appropriately consider and agree upon the entry of such orders.

---

pursuant to Rule 502, "the production of the opinions would not result in a waiver of the attorney-client privilege or work-product protection in this or any other subsequent litigation.").

57. Whitaker Chalk Swindle & Sawyer, LLP v. Dart Oil & Gas Corp., 4:08-CV-684-Y, 2009 WL 464989 (N.D. Tex. Feb. 23, 2009) (issuing Rule 502(d) order to protect disclosure in suit over attorney's fees from waiving privilege in ongoing state court proceedings).

58. Rainer v. Union Carbide Corp., 402 F.3d 608, 625 (6th Cir. 2005), *amended on reh'g* (Mar. 25, 2005) (enforcing an "Agreed Protective Order" signed by all of the parties and finding no waiver); Employers Ins. Co. of Wausau v. Skinner, No. CV 07-735(JS)(AKT), 2008 WL 4283346, at *7 (E.D.N.Y. Sept. 17, 2008) (parties' confidentiality agreement prevented waiver of privilege); Minebca Co. v. Pabst, 370 F. Supp. 2d 297, 300 (D.D.C. 2005) ("Simply put, the language of the Protective Order trumps the case law.").

59. *See* Hopson v. Mayor and City Counsel of Balt., 232 F.R.D. 228 (D. Md. 2005).

A Rule 502(d) order is designed to allow the parties and the court to defeat the default operation of Rule 502(b) in order to reduce costs and expedite discovery.[60]

Parties should take it upon themselves to carefully craft and submit for approval to the court a Rule 502(d) order setting forth under what circumstances, if any, the production of a privileged document would constitute waiver.[61] There is no requirement that the parties agree to have a Rule 502(d) order entered. The court has the power to enter a Rule 502(d) order where parties are unable or unwilling to suggest or agree to the entry of such an order. The Advisory Committee Notes state "a confidentiality order is enforceable whether or not it memorializes an agreement among the parties to the litigation. Party agreement should not be a condition of enforceability of a federal court's order."

By way of example, in *Rajala v. McGuire Woods*, the court had the "authority to enter a clawback provision [even when] not all the parties agreed to one."[62] The Court recognized that "an order containing a clawback provision is not dependent on

60. Several courts and pilot projects have created and published sample Rule 502(d) Orders. *See, e.g., infra* Appendix E, Peck, M.J., Model Rule 502(d) Order (S.D.N.Y.).

61. *See infra* Appendix D, Sample Model Order. The parties' initiative is especially important in light of the fact that "few districts have emphasized Rule 502 in local rules, guidelines, or amended forms." Thomas Y. Allman, *Local Rules, Standing Orders, and Model Protocols: Where the Rubber Meets with (E-Discovery) Road*, 19 RICH. J. L. & TECH. 8, 38 (2013); *but see* Local Rules W.D. Wash. CR 26(f)(1)(H) (requiring counsel to discuss "procedures for handling inadvertent production of privileged information and other privilege waiver issues pursuant to Rule 502(d) or (e) of the Federal Rules of Evidence").

62. No. 08-2638-CM-DJW, 2010 WL 2949582, at *4–5 (D. Kan. July 22, 2010) (Waxse, M.J.).

the agreement of the parties."[63] The Court referenced the Statement of Congressional Intent regarding Rule 502, which explains that a court may enter such an order on its own motion.

The Court found that such an agreement was appropriate given that plaintiff sought broad discovery, including voluminous ESI, from defendant. The Court observed that the order could reduce the resources and time spent on discovery disputes.[64] Finally, the Court noted if the producing party abused the 502(d) order by engaging in a "document dump," the plaintiff could still seek appropriate relief.[65]

Comment 2(c): Regulatory agencies should enter into Rule 502(d)-type agreements to facilitate the production of information in the regulatory setting.

The protections of Rule 502(d) orders are not available with respect to the production of information to federal and state agencies in regulatory proceedings because those proceedings are outside of formal litigation proceedings. However, WG1 of the Sedona Conference encourages federal and state agencies to enter into agreements with parties producing information to regulatory agencies that would set forth whether and under what circumstances the government may have the ability to later claim the production of privileged information constitutes a waiver. By doing so, the agencies provide a mechanism that will allow parties to potentially expedite a production to the agency without the fear that the unintentional production of a privileged document would result in a later claim of privilege waiver. Indeed, some federal agencies have already recognized

63. *Id.* at *4.

64. *Id.* at *6.

65. *Id.* at *7.

the potential benefits of such a rule.[66] Parties availing themselves of such agreements, however, must do so knowing that these agreements cannot preclude a third-party in another action from arguing that the production of the privileged information to the government agency—intentionally or unintentionally—constituted a waiver of the privilege.

Comment 2(d): Rule 502(d) orders should be considered to facilitate *consensual* "quick peek" and "make available" productions in order to promote judicial economy without fear of any later claim of waiver.

With the agreement of the producing party, Rule 502(d) can also be used creatively by the parties to facilitate the production of information without any privilege review, subject to an assurance that privileged documents produced through such a production will be returned without a later claim of waiver. This practice is often referred to as a "quick peek" or "make available production." Such productions may be particularly appropriate with respect to categories of documents that are unlikely to have any privileged information. In a commercial contract dispute, for example, where thousands of form contracts are required to be produced that are unlikely to have any privileged information, a Rule 502(d) order could be crafted to allow for the production of such information without the fear of waiver.

Parties have, on occasion, used such "quick peek" or "make available" productions on a wholesale basis for their entire production. Such productions should only be undertaken with a producing party's clear understanding of the risks and

66. *See, e.g.*, Int'l. Trade Comm. Proposed Rule, 19 C.F.R. § 210.27(e), 77 Fed. Reg. at 60, 952–56 (proposing procedure to address inadvertent disclosures); Fed. Trade Comm. Rule 16 C.F.R. § 2.11(d) (allowing for retrieval of inadvertently disclosed privileged material).

informed consent. In particular, even though a Rule 502(d) order can require the return of such privileged documents and ensure there is no waiver, once it is produced, the opposing party knows its contents. In addition, parties and the courts should be cognizant that a Rule 502(d) order should not be used as a cost-shifting tool allowing the producing party to make a "data dump" and requiring the requesting party to identify privileged documents. Courts have also rejected proposed Rule 502(d) orders that attempt to improperly shift the burden for asserting privilege.[67]

Courts and litigants can creatively use Rule 502(d) orders in instances where the producing party bears a larger burden—taking into account the volume of ESI to be reviewed and produced, and where the producing party agrees to the production without a privilege review. For example, in *Radian Asset Assur., Inc. v. Coll. of the Christian Bros. of N.M.*,[68] the court entered a Rule 502(d) order over the objection of the plaintiff because the defendant was amenable to producing all of the voluminous ESI in response to the plaintiff's requests, provided that the court entered a Rule 502(d) order. The court recognized that, "by ordering the College to turn over the CSF ESI unreviewed, the court is in effect forcing Radian Asset to bear the cost of that review if it wants certain data," but the court rejected the plaintiff's objection about the Rule 502(d) order being an impermissible cost-shifting order because "[s]uch a protective order is not, however, a traditional cost-shifting order." Moreover, the court clarified that it was only relying on Rule 502(d) to protect

67. *See* Chevron Corp. v. Weinberg Group, No. 11-409 (D.D.C. Oct. 26, 2012) (Facciola, M.J.) (rejecting an order that would have required receiving party to indicate its intention to use a document, then seek a ruling from the court that the document may be used; instead, finding that it was producing party's burden to assert and establish privilege).

68. No. CIV 09-0885JB/DJS, 2010 WL 4928866 (D.N.M. Oct. 22, 2010).

the defendant's privilege and not as its authority to order the production of documents. The court also agreed with plaintiff that Rule 502 is a "not a cost shifting tool." Ultimately, the court struck a balance by ordering the plaintiff to undertake some review of hard drives to identify the one that belonged to a particular custodian but ordering that the defendant produce that hard drive and large volumes of other ESI subject to the Rule 502(d) order. Therefore, *Radian Asset* provides support for defending the entry of a Rule 502(d) order over any objection.

Comment 2(e): Rule 502(d) does not authorize a court to require parties to engage in "quick peek" and "make available" productions and should not be used directly or indirectly to do so.

Although Rule 502(d) provides broad powers to a federal court, it does not give the court the power to order parties to produce privileged information where there has been no finding of waiver. For example, although a court may enter a Rule 502(d) order *allowing* the parties to engage in a "quick peek" process, the court cannot *order* a "quick peek" process over the objection of the producing party.[69]

It is well-established that a court may not compel disclosure of privileged attorney-client communications absent

69. *See* Martin R. Lueck & Patrick M. Arenz, *Rule 502(d) & Compelled Quick-Peek Productions*, 10 SEDONA CONF. J. 229 (2009).

waiver or an applicable exception.[70] Indeed, due process is implicated when privileged communications are required to be disclosed, even for *in camera* review.[71]

Notably, courts have acknowledged limits to their authority to order an *in camera* review. For example, in *United States v. Zolin*, the United States Supreme Court held that a court cannot compel a party to disclose privileged communications for *in camera* inspection without the requesting party making a showing of a factual basis adequate to support a good-faith belief that a reasonable person would conclude a review of the privileged communications may reveal evidence of a crime or fraud.[72] The court recognized that a blanket rule allowing *in camera* review "would place the policy of protecting open and legitimate disclosure between attorneys and clients at undue

70. *See, e.g.*, *In re* Dow Corning Corp., 261 F.3d 280, 284 (2d Cir. 2001) ("compelled disclosure of privileged attorney-client communications, absent waiver or an applicable exception, is contrary to well established precedent" and "we have found no authority . . . that holds that imposition of a protective order . . . permits a court to order disclosure of privileged attorney-client communications."); *In re* General Motors Corp., 153 F.3d 714, 716 (8th Cir. 1998) ("the district court may not compel disclosure of allegedly privileged communications to the party opposing the privilege" unless crime/fraud exception applies); *see also* Chase Manhattan Bank, NA v. Turner & Newhall, PLC, 964 F.2d 159, 163 (2d Cir. 1992) (issuing writ vacating discovery order that required party to produce documents subject to a claim of attorney-client privilege prior to a ruling on the merits of the objection).

71. *See, e.g.*, U.S. v. Zolin, 491 U.S. 554, 571 (1989) ("There is also reason to be concerned about the possible due process implications of routine use of *in camera* proceedings."); *In re* Grand Jury Proceedings (Doe), No. 91-56139, 1993 WL 6598, at *3 (9th Cir. Jan. 15, 1993) ("although the attorney-client privilege is not itself a constitutional right, this and other courts have found the Due Process Clause implicated in cases [pertaining to *in camera* review]") (internal citations omitted).

72. 491 U.S. 554, 572 (1989).

risk."[73] The court in *Zolin* also noted that its test would be even more stringent if a party sought outright disclosure of the privileged communication, and not just *in camera* review.[74]

Rule 502 contains no provision that grants the court the authority to compel a "quick peek" production or other disclosure of privileged information absent a finding of waiver. Indeed, Rule 502 was designed to protect producing parties, not to be used as a weapon impeding a producing parties' right to protect privileged material. Compelled disclosure of privileged information, even with a right to later clawback the information, forces a producing party to ring a bell that cannot be un-rung. As one court recognized, "regardless of how painstaking the precautions, there is no order . . . which erases from defendant's counsel's knowledge what has been disclosed. There is no remedy which can remedy what has occurred, regardless of whether or not the precautions were sufficient."[75]

The court's analysis is directly on point here. There are many ways in which a producing party may be prejudiced by compelled disclosure of privileged information. For instance, after viewing privileged material, a party may submit a request for admission to elicit the material or tailor a deposition question to do the same. Or a party may adjust its settlement position in light of its review of the privileged information. These concerns would inevitably erode the goal of the attorney-client privilege, which is "to encourage full and frank communication between attorneys and their clients and thereby promote

73. *Id.* at 571.

74. *Id.* at 572.

75. International Digital Systems Corp. v. Digital Equip., 120 F.R.D. 445, 449 (D. Mass. 1988).

broader public interests in the observance of law and administration of justice."[76]

Courts also should not employ Rule 502(d) indirectly to compel a result that is not permitted directly under the rule. For example, some courts have separately entered 502(d) orders protecting parties from claims of waiver by the production of privileged documents as well as Rule 16(b) scheduling orders with aggressive document production deadlines that do not provide the parties with a reasonable period of time to review the documents for privilege. In these instances, the courts caution the parties that there will be dire consequences for missing the deadline and they, therefore, should consider all means available to achieve a timely document production, including the use of a "quick peek" or "make available" production. In essence, the courts are attempting to indirectly compel a result that it is not directly permitted under Rule 502(d)—a result that was never intended by the rule.

III. Principle 3. Parties and their counsel should follow reasonable procedures to avoid the inadvertent production of privileged information.

Commentary

Comment 3(a): Rule 502(b) provides a uniform statutory approach to the issue of inadvertent production and waiver, eliminating the three common-law approaches in determining whether there has been an inadvertent waiver.

---

76. Upjohn Co. v. U.S., 449 U.S. 383, 393 (1981) ("if the purpose of the attorney-client privilege is to be served, the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected. An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all.").

Rejecting the common-law approach to waiver, Rule 502(b) adopts a three-part test to determine whether the disclosure results in an inadvertent waiver:

> (b) Inadvertent Disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).

Rule 502 overrules approaches previously applied in federal courts that are inconsistent with the plain language of the rule.[77]

Comment 3(b): Rule 502(b) applies only to the unintentional production of privileged ESI that is not otherwise addressed in a Rule 502(d) order.

Rule 502(b) requires that a disclosure be "inadvertent."[78] Although courts often combine the analysis of inadvertence with whether reasonable steps were taken to avoid disclosure—because the effort taken to prevent disclosure is evidence that a party did not intend to disclose privileged material—a finding of inadvertence is an independent threshold question. Where a party intentionally discloses a privileged document but later re-

77. *See, e.g.*, Amobi v. D.C. Dep't of Corr., 262 F.R.D. 45, 52 (D.D.C. 2009) (noting that Rule 502 "overrides the long-standing strict construction of waiver" in the D.C. Circuit).

78. *Amobi*, 262 F.R.D. 45 (D.D.C. 2009).

thinks the wisdom of the disclosure, the initial disclosure is not inadvertent. Inadvertence means "mistaken."[79]

Comment 3(c): Prior to litigation, corporations should take reasonable steps to protect their privileged information by ensuring that: (i) employees are trained on what communications and activities can be protected under a claim of privilege; (ii) privileged communications are identified; and (iii) tools are utilized to ensure the appropriate management of privileged information.

The ability to identify and segregate privileged information is greatly facilitated by the identification, labelling, and management of that information prior to litigation. The following are examples of best practices regarding the identification and handling of privileged information prior to litigation that may facilitate the identification and segregation of privileged information during the collection, review, and logging process:

- **Train Employees on the Scope of Privilege and Waiver.** Most non-lawyers and many lawyers do not understand the nature and the scope of the attorney-client privilege or work-product protection. Training those individuals, espe-

79. *Id.; see* Francisco v. Verizon S., Inc., 756 F. Supp. 2d 705 (W.D. Va. 2010) (production of notes after careful analysis, partial redaction, and designation as confidential was not inadvertent despite producing party's subsequent discovery that the notes reflected communications with the party's general counsel); Silverstein v. Fed. Bur. Of Prisons, No. 07-cv-02471, 2009 WL 4949959 (D. Colo. Dec. 14, 2009) (rejecting government's assertion that production of privileged memorandum was inadvertent and finding that government had intentionally produced privileged memorandum to obtain litigation advantage and, only on the eve of a Rule 30(b)(6) deposition, sought to retrieve the memorandum and deny plaintiff discovery regarding the document). *See also Amobi*, 262 F.R.D. at 53 (adopting simple test for inadvertence: was the disclosure unintended?).

cially those who interact with the legal department or whose roles involve privileged communications or work-product activity, will facilitate the identification and designation of privileged information.

- **Use legal titles.** Attorneys who are acting as such, even those who work in departments outside the legal department, should use legal titles, such as "counsel," "associate general counsel," "senior litigation counsel," etc. The company's organizational chart should reflect these legal titles and, when appropriate, indicate direct or dotted line reporting to the legal department.
- **Identify when acting as an attorney.** Written communications should state that: (i) in-house counsel has been asked to provide legal advice and (ii) the communication is for the purpose of obtaining information to enable the attorney to provide legal advice.
- **Educate clients to request legal advice and to maintain confidentiality.** The assertion of the attorney-client privilege is bolstered when the corporate client specifies a request for legal advice in an initial communication. In order to avoid waiver, clients should be instructed to maintain privileged materials in confidence and not distribute them without approval from counsel.
- **Educate employees about the risk of commingling legal and business advice.** There is a risk that commingling legal and business advice will waive otherwise applicable privileges. A court may determine that a document reflecting both

business and legal advice is not "predominantly" or "primarily" legal in nature.[80] The risk of waiver is increased where a document is prepared for simultaneous review by both legal and non-legal personnel.[81]

- **Limit distribution of privileged materials to those employees who need to know the information for legal purposes.** Waiver may occur within an organization when otherwise privileged materials are circulated to persons not assisting in furnishing information to the lawyer

---

80. *See, e.g.*, Phillips v. C.R. Barc, Inc., 290 F.R.D. 615, 629 (D. Nev. 2013) (in order to determine whether the primary purpose is to provide legal advice, courts will look at a number of factors, including "whether the legal purpose so permeates any non-legal purpose 'that the two purposes cannot be discretely separated from the factual nexus as a whole'"); Visa U.S.A., Inc. v. First Data Corp., 2004 WL 1878209 (N.D. Cal. 2004) (documents prepared for a dual purpose will not be privileged if the documents had a "clear, readily separable business purpose.").

81. "The attorney-client privilege does not attach . . . to documents which were prepared for simultaneous review by both legal and non-legal personnel within the corporation. This rule applies to the document as a whole because each communication within that document was provided to non-legal personnel for their review. Thus, those communications cannot be said to have been made for the primary purpose of seeking legal advice." United States v. Chevron Corp., No. C 94-1885 SBA, 1996 U.S. Dist. LEXIS 8646, at *6, 1996 WL 444597 (N.D. Cal. May 30, 1996) (internal citations omitted); *see also In Re*: Vioxx Products Liability Litigation, 501 F. Supp. 2d 789, 809 (E.D. La. 2007) ("We accepted the possibility that addressing communications to both lawyers and non-lawyers could reflect the seeking of legal advice from the lawyers and that the non-lawyers were simply being notified about the nature of the legal services sought. Facially, however, it appeared far more probable that the non-lawyers were being seen [sic] the communications for separate business reasons.").

or acting upon legal advice received from the lawyer.[82]

- **Label privileged and work-product protected documents.** Apply the appropriate privilege legend to every privileged record. Privileged communications should, at a minimum, be labeled as "Privileged & Confidential." Privileged records that are protected under the work-product doctrine may also contain a "Work Product" label. In addition to demonstrating the intention to keep the document confidential, proper labeling of privileged and protected ESI will make it easier and less expensive to identify these documents with technology-assisted review in the event of discovery. Note: Such labels should not be used indiscriminately where documents are not legitimately privileged or protected.

Comment 3(d): Parties and counsel should identify and implement "reasonable" steps to prevent disclosure of privileged ESI during the collection, identification, and review process.

The central issue under Rule 502(b) is whether the disclosing party took reasonable steps to prevent disclosure. As

82. TESTIMONIAL PRIVILEGES, *supra* note 4, at §1:83; *see* Upjohn Co. v. United States, 449 U.S. 383, 390–92, 66 L. Ed. 2d 584, 101 S. Ct. 677 (1981) (holding that attorney-client privilege could protect communications between company's lawyer and company employee, where lawyer needed employee's information to adequately advise the company); *Vioxx*, 501 F. Supp. 2d at 796 (the privilege protects communications between those employees and corporate legal counsel on matters within scope of their corporate responsibilities, as well as communications between corporate employees in which prior advice received is being transmitted to those who have a need to know in the scope of their corporate responsibilities).

Judge Grimm pointed out: "The analytical methods are reasonable, even though operators cannot guarantee the methods will identify and withhold from production every privileged or protected document. Reviewing courts must remember that the bellwether test under Rule 502(b)(2) is *reasonableness*, not *perfection*."[83]

The rule itself does not set forth criteria for what is reasonable, opting instead for a "flexible" approach, according to the Rule's Advisory Committee Note: "[Rule 502] does not explicitly codify [the multi-factor] test, because it is really a set of non-determinative guidelines that vary from case to case. The rule is flexible enough to accommodate any of those listed factors."[84]

Here, Judge Grimm's opinion in *Victor Stanley* is again applicable. Judge Grimm recognized the importance of employing proper methods when searching for privileged documents.[85] Moreover, the opinion questioned whether simply running a keyword search would be sufficient. Judge Grimm strongly indicated that a qualified expert should be involved in determining the proper search methodology, observing that "[w]hile keyword searches have long been recognized as appropriate and helpful for ESI search and retrieval, there are well-known limitations and risks associated with them, and proper selection

83. Paul W. Grimm, Lisa Yurwit Bergstrom & Matthew P. Kraeuter, *Federal Rule of Evidence 502: Has It Lived Up To Its Potential?*, XVII RICH. J.L. & TECH. 8 (2011).

84. FED. R. EVID. 502(b) Advisory Committee Notes.

85. Victor Stanley, Inc., v. Creative Pipe, Inc., et al., 250 F.R.D. 251, 262 (D. Md. 2008) ("Use of search . . . retrieval methodology, for the purpose of . . . withholding privileged or work-product protected information from production, requires the utmost care in selecting methodology . . .").

and implementation obviously involves technical, if not scientific knowledge."[86] Judge Grimm also noted that courts most likely will require some reliable source (such as a qualified expert or learned treatise) if asked to resolve an issue related to the appropriateness of a search methodology.[87] Thus, before employing a particular search methodology, parties should consider consulting a qualified expert in the field, so that they are prepared to adequately defend their methodology if challenged.[88] While this is an important step in the process, it also adds to the overall cost and time associated with searching for privileged information.

In light of the uncertainty surrounding the "reasonableness" standard,[89] Judge Grimm suggested following best practices as described by The Sedona Conference.[90]

To avoid a potential waiver of privilege, and to avoid the damage that can be caused by an inadvertent production whether or not the production results in a waiver, the parties and their counsel should design and implement a reasonable and auditable procedure for the identification and logging of

---

86. *Id.* at 260.

87. *Id.* at 261 n.10.

88. *See id*. ("opinions regarding specialized, scientific or technical matters are not 'helpful' unless provided by someone with proper qualifications.").

89. Adding to the uncertainty, some courts have indicated that taking some reasonable steps is not sufficient to preserve privilege; rather a party must take *all* reasonable steps. *See* ReliOn, Inc. v. Hydra Fuel Cell Corp., No. 06-607-HU, 2008 WL 5122828, at *2 (D. Or. Dec. 4, 2008) ("the court deems the privilege waived if the privilege holder fails to pursue all reasonable means of preserving the confidentiality of the privileged matter").

90. *Victor Stanley*, 250 F.R.D. at 262 ("[C]ompliance with [t]he Sedona Conference Best Practices for use of search and information retrieval will go a long way towards convincing the court that the method chosen was reasonable and reliable.").

privileged documents. Consideration should be given to the factors outlined below.

- **Collection Process to Include Steps to Identify Privileged ESI.** Simply asking record owners if they worked with counsel on the issues relevant to the claims and defenses of the case can help identify ESI that may be privileged. Similarly, discussions with in-house counsel may help build the list of search terms, including names of attorneys, that would make the privilege review more efficient and accurate.
- **Written Document Review Protocol to be Used for Managing Privileged Records.** Design and implement a written document review protocol that includes a detailed discussion of the law of privilege for the jurisdiction(s) at issue. An experienced senior attorney on the review team should be charged with oversight responsibilities in the creation and implementation of this protocol.
- **Education and Training of the Review Team.** Education and training of the review team is a critical step with respect to the appropriate application of the attorney-client and work-product privileges. The training should include a detailed discussion on basic privilege law. It might also include using sample documents from the production to assist the review team in the identification of privileged materials.
- **Escalation Process for Privilege Calls.** The review procedure should also have an escalation process whereby questions regarding the scope and application of privilege calls to specific documents can be directed to an experienced senior

attorney with the oversight responsibilities mentioned above.

- **Segregation of Privileged Information.** Information that is under review for privilege (or already determined to be privileged) should be segregated from the document review collection to avoid any unnecessary comingling with the remainder of the production.
- **Quality Control and Sampling Process.** A quality control and sampling process under the direction of an experienced senior attorney should be designed and implemented to ensure that privileged documents have been appropriately identified. Such a process is likely to reflect whether the review team is over-designating or under-designating documents for privilege. Quality control and sampling may also identify the need for retraining the review team regarding the nature and extent of privileged documents found within the document population. This quality control and sampling process should be conducted throughout the privilege review process. Prior to the production of the non-privileged documents, additional quality control and sampling of the production should be undertaken to ensure that privileged documents have not been inadvertently included in the production set.
- **Advanced Analytical Software Applications and Linguistic Tools in Screening for Privilege and Work Product.** The Advisory Committee Notes expressly stated that whether a party used analytical software applications and linguistic tools in screening for privilege and work

product is a factor to consider in determining whether "reasonable steps" were undertaken to prevent inadvertent disclosure.[91] At a minimum, best practices would dictate the proper selection and good faith implementation of search terms to identify and potentially screen out for further review potentially privileged documents. In addition, the producing party should consider the feasibility of using more advanced analytical tools to help identify privileged documents, including near duplicate, threading, clustering, concerting, and technology-assisted review software/engines.

- **Contemporaneous Documentation of the Privilege Review Processes.** In order to defend the methodology used to search for privileged information before a court, even in *in camera* review, a party should be prepared to demonstrate that the procedures and processes that were undertaken to identify and log privileged documents were contemporaneously documented.
- **Transparency of Process.** As part of the meet and confer process, a party should consider disclosing to the opposing party the methodology that it will use to implement the privilege review process.

Comment 3(e): A party that claims that it inadvertently produced privileged documents should be entitled to a rebuttable presumption that it took "reasonable steps" to prevent the disclosure where: (i) it disclosed the reasonable steps as part of the Rule 26(f) meet and confer process; (ii) the opposing party

91. FED. R. EVID. 502(b) Advisory Committee Notes.

did not timely object to the procedure with specificity to the extent that it could; and (iii) the producing party in good faith adhered to the disclosed reasonable steps in the review of privileged ESI.

In the event that the parties are unable to agree to the terms of a Rule 502(d) order as part of the Rule 26(f) process, the parties should at least discuss and attempt to agree upon the procedure that each side will employ to prevent the inadvertent disclosure of privileged information. Absent such agreement, it is incumbent upon each party to at least articulate any objection it may have to the opposing party's proposed procedure that will be used to prevent the inadvertent disclosure of privileged information.

In order to facilitate cooperation, a producing party should be entitled to a rebuttable presumption that it took "reasonable" steps to prevent the disclosure of privileged information pursuant to Rule 502(b)(2) provided it can show that: (i) the disclosure of the methodology was part of the Rule 26(f) meet and confer process; (ii) the producing party implemented the disclosed methodology in good faith; and (iii) the opposing party failed to timely object to the extent that it could (i.e., at a minimum before the day that the production is required either by agreement or court order). The producing party would still be required to demonstrate the other two elements of Rule 502(b). The non-producing party has the ability to rebut the presumption with evidence demonstrating that the procedure used could not have been "reasonable" given the facts surrounding the production of the inadvertently produced privileged information.

Comment 3(f): Parties should undertake to notify one another immediately upon the discovery of inadvertently produced privileged ESI.

The clock for "promptness" does not start ticking until the producing party knows or should have known about the inadvertent disclosure. A court's interpretation of the word "prompt" may depend on whether the inadvertently produced material is discovered at a deposition or in another setting. Several courts have adopted a strict interpretation of "prompt." Therefore, if an inadvertently produced privileged document is used by the receiving party at a deposition and its disclosure adversely affects the producing party's case or would lead to the disclosure of other privileged documents, counsel for the producing party should object immediately to the use of the document and instruct the deponent not to answer questions about the document. An "immediate" objection and instruction prevents the witness from testifying about the document and unquestionably satisfies Rule 502(b)(3)'s requirement for promptness. While an immediate objection will undoubtedly meet the standard for "promptness," courts differ in their response when an objection is not immediate.

A court's interpretation of "prompt" may vary when counsel discovers the inadvertent disclosure outside the deposition setting. For instance, in *Heriot v. Byrne*,[92] the court found no waiver where the producing party discovered the inadvertent disclosure before a deposition and notified the receiving party of the vendor's error within twenty-four hours of discovery of the error.[93]

Comment 3(g): It is the obligation of the producing party to rectify the error promptly, including seeking the return privileged documents.

---

92. 257 F.R.D. 645 (N.D. Ill. 2009).

93. *See, e.g., In re* Actos (Pioglitazone) Products Liability Litigation, MDL Docket No. 6:11-MD-2299 (W.D. La. July 10, 2012) (Doherty, J.) (Case Management Order) (requiring that the producing party notify the receiving party of the inadvertent production within *ten* days).

The Advisory Committee Notes provide that Rule 502(b) "does not require the producing party to engage in a post-production review to determine whether any protected communication or information has been produced by mistake." Instead, the rule requires the producing party "to follow up on any obvious indications that a protected communication or information has been produced inadvertently."

When a privileged document surfaces in litigation, the producing party should use the procedures outlined in Rule 26(b)(5)(B)[94] as a starting point.[95] If the receiving party does not return or sequester the privileged communication, then further action is required by the producing party. Specifically, the producing party should promptly follow up with the receiving party or seek court intervention.[96] These steps should be taken

---

94. The procedures set out in Fed. R. Civ. P. 26(b)(5)(B) are as follows: If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim.

95. Neither Fed. R. Evid. 502(b) nor Fed. R. Civ. P. 26(b)(5)(B) provides guidance on how quickly the receiving party must return privileged documents to the producing party. Thus, the parties themselves should consider entering into an agreement dictating the procedures and timing governing the return of privileged documents. If a Rule 502(d) order has been entered then these procedures should be included in that order. Thomas C. Gricks, *The Effective Use of Rule 502(d) in E-Discovery Cases*, THE LEGAL INTELLIGENCER (Oct. 25, 2011).

96. Luna Gaming–San Diego, LLC v. Dorsey & Whitney, LLP, No. 06-cv-2804, 2010 WL 275083, at *6 (S.D. Cal. Jan. 13, 2010) ("Failing to take affirmative steps to retrieve the document, beyond merely asking for it at depositions, also waives the privilege").

without delay.[97] For larger productions, courts may be more forgiving when determining promptness of the actions taken.[98]

IV. Principle 4. Parties and their counsel should make use of protocols, processes, tools, and technologies to reduce the costs and burdens associated with identification, logging, and dispute resolution relating to the assertion of privilege.

Commentary

In 1993, Rule 26 was amended to add subdivision (b)(5), requiring a producing party to "notify other parties if it is withholding material otherwise subject to disclosure under the rule or pursuant to a discovery request because it was asserting a claim of privilege or work product protection."[99] The Advisory Committee Notes added that the failure to notify the other party could result in either sanctions under Rule 37(b)(2) or waiver of the privilege.[100] The stated purpose of the amendment was to provide an opposing party with information to "evaluate the applicability of the claim [of privilege]."[101] The rule did not attempt to define the information that should be provided but the Advisory Committee Notes stated: "Details concerning time,

97. Kmart Corp. v. Footstar, Inc., No. 09-C-3607, 2010 WL 4512337, at *2 (N.D. Ill. Nov. 02, 2010) ("Liberty Mutual did not file this motion until twelve days after the deposition. . . . a reasonable step would be to file a motion within a matter of days.").

98. *See, e.g.*, United States v. Sensient Colors, Inc., No. 07–1275, 2009 WL 2905474 (D. N.J. Sept. 9, 2009) (In a production consisting of 45,000 documents, the court stated "only eight work days [after the inadvertent disclosure], plaintiff confirmed its error and notified defendant that Rule 26(b)(5)(B) should be followed. The Court finds that these actions were timely and reasonable").

99. FED. R. CIV. P. 26(b)(5).

100. FED. R. CIV. P. 26(b)(5) Advisory Committee Note to the 1993 amendments.

101. *Id.*

persons, general subject matter, etc. may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected, particularly if the items can be described by categories. A party can seek relief through a protective order under subdivision (c) if compliance with the requirement for providing this information would be an unreasonable burden. In rare circumstances, some of the pertinent information affecting applicability of the claim, such as the identity of the client, may itself be privileged; the rule provides that such information need not be disclosed."[102] The amendment to this rule resulted in the rise of the modern privilege log.

With this said, the current method used by most parties for identifying privileged documents and for creating privilege logs appears to be a broken process.[103] Privilege logging is arguably the most burdensome and time consuming task a litigant faces during the document production process. Further, the deluge of information and rapid response times required by pressing dockets have forced attorneys into using mass-production techniques, resulting in logs with vague narrative descriptions. In some instances, the text of privilege logs "raise[] the term 'boilerplate' to an art form, resulting in the modern privilege log being as expensive to produce as it is useless."[104]

---

102. *Id.*

103. Report of the Special Committee on Discovery and Case Management in Federal Litigation of the New York State Bar Association, June 23, 2012, at 73 ("Most commercial litigation practitioners have experienced the harrowing burden the privilege log imposes on a party in a document-intensive case, especially one with many e-mails and e-mail strings.").

104. Chevron Corp. v. Weinberg Group, No. 11-406, 2012 WL 4480697 (D.D.C. Sept. 26, 2012) (Facciola, M.J.). In *Chevron*, the Court noted the trend toward mechanically produced logs with boilerplate information that fails to adequately describe the documents and the nature of the privilege claimed. The Court ordered a detailed privilege log and that unprotected documents

The process of logging is further complicated by the lack of a uniform standard applied by the courts regarding the adequacy of the content of privilege logs. The Fed. R. Civ. P. provide the following guidance on what information is to be included in an adequate privilege log:

> [A party must] describe the nature of the documents, communications, or tangible things not produced or disclosed and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.[105]

But the 1993 Advisory Committee Notes recognized that the specific information provided in asserting the privilege *may vary* depending on the volume of the materials involved.[106]

---

be turned over, and the Court warned that parties would be "ruthlessly" held to their Rule 26 obligations. On reconsideration, the court again criticized the use of "machines [to] produce privilege logs without human beings intervening to use the English language." *Id*. The court observed that the "mechanical language" made it impossible to determine whether a document was actually privileged. *Id.* In partially denying the motion, the court held that "failures by respondent to adequately and accurately identify the documents for which it is claiming privilege should not be grounds for reconsidering." *Id.*

105. FED. R. CIV. P. 26(b)(5)(A)(ii). In 2006, the Advisory Committee acknowledged that the review of ESI has only increased the risks of waiver and the potential burden of avoiding such waiver. FED. R. CIV. P. 26(b)(5) Advisory Committee Note.

106. *See* FED. R. CIV. P. 26(b)(5) Advisory Committee Note ("Details concerning time, persons, general subject matter, etc., may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected, particularly if the items can be described by categories.").

In applying Rule 26(b)(5)(A)(ii), courts have differed on what constitutes a reasonable logging exercise.[107] Some courts have even published standing orders and guidance or local rules for logging privileged information.[108] Courts have also

107. *See In re* Rivastigmine Patent Litig., 237 F.R.D. 69 (S.D.N.Y. 2006) (Defendants in this multidistrict patent litigation moved to compel production of numerous communications that Plaintiffs claimed were protected by the attorney-client privilege. Court found the categorical log inadequate for, among others reasons: failure to identify specific legal professionals protected by the privilege under foreign law, i.e., patent attorneys as opposed to law firms generally, to which the privilege would apply. In response to the inadequacy of the log, the Court ordered that the underlying documents be produced in their entirety). *But see* United States v. Magnesium Corp. of America, No. 01-00040, 2006 WL 1699608 (D. Utah June 14, 2006) (Court found that a detailed privilege log was not necessary when the documents to be logged (generated over the previous 5 years) would number in the thousands and when it "seem[ed] clear that most of the documents at issue would be protected from disclosure by the work product privilege, the attorney-client privilege, or the joint defense privilege.").

108. *See* S.D. Ala. Categorical Logs: 1998 Introduction to Civil Discovery Practice Sec. I.K(2) introduces the required contents of a privilege log as follows: "For documents (individually or by category): [list of required data points.]" Sec. I.K(5) states that "Any agreement between the attorneys to waive or to alter the contents of the privilege log is normally accepted, so long as it does not delay the progress of the case or otherwise interfere with Court management." http://www.alsd.uscourts.gov/sites/alsd/files/Discovery_Practice.PDF; *see also* N.D. Cal. Model Stipulated Order Re: Discovery Par. 8(c) provides: "Communications may be identified on a privilege log by category, rather than individually, if appropriate." http://www.cand.uscourts.gov/filelibrary/1119/Model%20Stip%20E-discovery%20Order. The following N.D. Cal. Magistrate Judges' standing orders allow privilege logs to contain privilege information "for each document or for each category of similarly situated documents." Laporte Standing Order Par. 2(g); Ryu Standing Order Par. 13; Westmore Standing Order Par. 19.

placed the burden on litigants to meet and confer about the logging methodology.[109] Other courts have provided specific guidance to exclude post-complaint data from logging and production.[110] Courts have also considered the burden of logging individual email strings.[111] The Federal Trade Commission has

---

109. District of Delaware Default Standard for Discovery, Including Discovery of Electronically Stored Information ("ESI") 1(d)(i) requires parties to confer on "alternatives to document-to-document logs": The parties are to confer on the nature and scope of privilege logs for the case, including whether categories of information may be excluded from any logging requirements and whether alternatives to document-by-document logs can be exchanged. No privilege logging of "information generated after the filing of the complaint." Default Standard 1(d)(ii), http://www.ded.uscourts.gov/sites/default/files/Chambers/SLR/Misc/EDiscov.pdf.

110. Del. Chancery Categorical Logs: 2013 discovery guidelines allow parties to agree to categorical logs. It may be possible for parties to agree to log certain types of documents by category instead of on a document-by-document basis. Categories of documents that might warrant such treatment include internal communications between lawyer and client regarding drafts of an agreement, or internal communications solely among in-house counsel about a transaction at issue. These kinds of documents are often privileged and, in many cases, logging them on a document-by-document basis is unlikely to be beneficial. "The Court generally does not expect parties to log post-litigation communications." As for logging email chains, it recommends that "parties should attempt to agree on the procedures that both sides will use." It also advocates for the involvement of senior lawyers, particularly senior Delaware counsel, in the process. *See* http://courts.state.de.us/chancery/rulechanges.stm; http://courts.state.de.us/chancery/docs/CollectionReviewGuidelines.pdf; http://courts.delaware.gov/chancery/docs/CompleteGuidelines.pdf.

111. S.D.N.Y. Pilot § II.E. For purposes of creation of a privilege log, a party need include only one entry on the log to identify withheld emails that constitute an uninterrupted dialogue between or among individuals; provided, however, that disclosure must be made that the emails are part of an uninterrupted dialogue. Moreover, the beginning and ending dates and times (as noted on the emails) of the dialogue and the number of emails within the dialogue must be disclosed, in addition to other requisite privilege

provided guidance for working with staff to reduce the burden of privilege logging.[112] Even state bar associations are considering strategies to reduce the burden of logging.[113]

Comment 4(a): Producing parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for the identification and logging of ESI withheld from production on the grounds of privilege.

Sedona Principle 6 provides that "[r]esponding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their

---

log disclosure, including the names of all of the recipients of the communications.

112. 77 FED. REG. 59301 (FTC comments on the 2012 revision of Rule of Practice 2.11 (dealing with withholding materials requested by the Commission) notes FTC's discretion to allow categorical privilege logs: "Parties should bear in mind that, as provided in paragraph (b), staff may relax or modify the specifications of paragraph (a), in appropriate situations, and as the result of any agreement reached during the meet and confer session. Under certain circumstances, less detailed requirements (for example, allowing documents to be described by category) may suffice to assess claims of protected status. This revision is designed to encourage cooperation and discussion among parties and staff regarding privilege claims. Consistent with existing practices, the Commission also codified in this rule its existing authority to provide that failure to comply with the rule shall constitute noncompliance subject to Rule 2.13(a). Paragraph (b) elicited no comments and is adopted as modified.").

113. NY State Bar Faster-Cheaper-Smarter (FCS) Working Group Proposes adoption of Fed. R. Evid. proposals regarding categorical privilege logs, categories of documents to exclude, metadata-based indexing, and email chain categorization. *Report of the Faster-Cheaper-Smarter Working Group of the Commercial and Federal Litigation Section of the New York State Bar Association*, 12–14, NEW YORK STATE BAR ASSOCIATION, *available at* http://nysbar.com/blogs/nybusinesslitigation/FCS%20Report%20-%20Final.pdf. In addition to metadata-based indexing, they suggest taking small samples of indexed documents for *in camera* review by the court, and then generalizing production or logging from these samples. *Id*.

own electronically stored information."[114] Inherently, this principle also applies in the context of the identification, segregation, and logging of privileged ESI. In this regard, the identification of privileged information is, in large part, a fact-based inquiry. It is the responding party that has access to those facts and is best situated to identify whether particular ESI is subject to a claim of privilege. Similarly, the responding party is also best situated to determine the procedures, methodologies, and technologies appropriate for identifying and logging privileged material.

Comment 4(b): Parties should cooperate to reduce the burdens and costs associated with the identification, logging, and dispute resolution relating to the assertion of privilege with respect to the review of ESI.[115]

In July 2008, The Sedona Conference released *The Sedona Conference Cooperation Proclamation*, which states:

> The costs associated with adversarial conduct in pre-trial discovery have become a serious burden to the American judicial system. This burden rises significantly in discovery of electronically stored information ("ESI"). In addition to rising monetary costs, courts have seen escalating motion practice, overreaching, obstruction, and extensive,

114. The Sedona Conference, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, THE SEDONA CONFERENCE (2nd Ed, 2007), *available at* https://thesedonaconference.org/download-pub/81.

115. This comment is not intended to draw into question Sedona Conference Principle 6 for Electronic Document Production which remains a bedrock principle, and, in the context of the assertion of privilege, the responding party is best situated to evaluate the foundation upon which any claim of privilege is made as well as the procedures, methodologies, and technologies for the identification of electronically stored information withheld from production on the grounds of privilege.

> but unproductive discovery disputes—in some cases precluding adjudication on the merits altogether—when parties treat the discovery process in an adversarial manner. Neither law nor logic compels these outcomes.[116]

The Cooperation Proclamation challenges lawyers to rethink their litigation roles and strategies. The Proclamation notes that lawyers have a duty "to strive in the best interest of their clients to achieve the best results at a reasonable cost, with integrity and candor as officers of the court." Cooperation in the area of the identifying, logging, and dispute resolution surrounding the assertion of privilege with respect to the review of ESI has the potential to reduce the parties' risk and costs, while promoting judicial economy.[117]

To this end, parties should utilize Rule 502 to attempt to agree upon protocols, processes, tools, and technologies to limit the costs and burdens of the identification, review, and logging of privileged information.[118] Outlined herein are examples of

---

116. The Sedona Conference, *The Sedona Conference Cooperation Proclamation*, 10 SEDONA CONF. J. 331, 331 (2009 Supp.).

117. *See also* The Sedona Conference, *Cooperation Guidance for Litigators & In-House Counsel*, THE SEDONA CONFERENCE, at 15 (March 2011), *available at* https://thesedonaconference.org/download-pub/465 (Cooperation Point #12 provides: "Reaching agreement to minimize the cost of privilege reviews may now be easier under Federal Rule of Evidence 502."). The parties should be guided by the concept of reasonableness embodied in Fed. R. Evid. 502, The Sedona Conference commentaries, and case law. They should balance the chance of inadvertent production with the burden of eliminating inadvertent production.

118. John Rosenthal & Patrick Oot, *Protecting Privilege with Rule 502*, REAL EDISCOVERY, Winter 2010, at 8 (suggesting that any protective order between the parties address not only inadvertent disclosure but also cost-effective privilege logging processes).

strategies that some parties, commentators, or courts have either adopted or urged their adoption, which can dramatically reduce the cost and burden associated with privilege review and logging. The strategies listed are by no means exhaustive, and there are certainly other strategies that parties can design and pursue to facilitate the identification and logging of privileged ESI.

Exclusion of custodians from the logging process. Certain custodians are only likely to have information relevant to the claims and defenses of a particular matter that came to their attention after the litigation commenced or as part of the litigation process. The information they possess, therefore, is likely to be privileged. Examples of such custodians might include outside litigation counsel or in-house counsel responsible for the litigation. The burden of identifying and logging privilege information can be substantially reduced by not having to identify and log privileged information from such custodians.

Exclusion of documents generated after the date the litigation commenced. Another strategy to reduce the burden of privilege review is to omit the requirement to identify or log privileged information generated by or sent to the litigation team after the date of the filing of the lawsuit or when litigation is reasonably anticipated. Many documents generated after that date often fall within work-product protection as they relate to the prosecution or defense of the litigation. Some court rules expressly exclude these records from the privilege log obligation. Of course, each litigation varies and there may very well be categories of relevant information generated after the date of the commencement of the litigation that should be produced.

Use of objective privilege logs. One strategy that has been used with some success is the use of objective privilege logs. Under this strategy, the producing party agrees to run a set of

privilege-screener search terms.[119] For any ESI that is identified by the screening process, the producing party provides in the first instance a list of documents that are claimed to be privileged in the form of the objective metadata (author, recipient, date created, document title, etc.) that is generated from the litigation support system. The receiving party can then designate documents or categories of documents on the objective privilege log that it would like the producing party to review in greater detail and provide a traditional Rule 26(b)(5)(A)(ii) log for those entries/categories.[120] The producing party then has the burden of logging those entries and supporting any claim of privilege. This procedure has been used successfully in complex litigation, resulting in substantial cost savings to the parties.[121]

Foregoing logging of documents with privilege redactions. Another strategy to reduce the burden of privilege logging might be to forego logging documents produced with privilege redactions while providing extracted field text from the topmost email to the receiving party. If the author, recipient, and subject information *within* the email chain is also left unredacted (so that this information is available for lower emails in the thread),

---

119. Designing screener terms should take into consideration the nature of the privileged documents and persons involved in privileged communications. It is recommended that the terms be tested against the data set to ensure that they are reasonably designed to identify potentially privileged documents, without undue false positives or false negatives.

120. Alternatively, an objective log could be produced after conducting a first pass review for responsiveness and privilege. The receiving party could then designate documents or categories of documents on the objective privilege log that it would like the producing party to review in greater detail and provide traditional Rule 26(b)(5)(A)(ii) log entries/categories.

121. The procedure was originally designed by John Rosenthal and William Butterfield and later endorsed by Magistrate Judge Facciola in *In re Rail Freight Fuel Surcharge Antitrust Litig*, MDL No. 1869, Misc. No. 07-489 (October 8, 2009) (D.D.C.).

it seems that a privilege log would be largely redundant of information already available within the document and supplied in the metadata. Parties would have to consider this option within the context of Rule 26(b)(5)(A), which requires that a party provide sufficient information to allow other parties to assess its privilege claim. However, opposing parties' Rule 26(b)(5)(A) concerns may be able to be addressed by including some type of privilege claim field with the produced metadata or, depending on the technology available, inserting a short description of the privilege claim within the redaction box.

Agreeing to a hierarchical privilege or staged review of privileged ESI. One strategy to consider is to agree to review certain documents individually for privilege whereas other categories are reviewed on a sampling basis. Similarly, agreeing to a staged privilege review in which certain materials are reviewed for privilege and produced or logged first and other materials are reviewed and produced or logged later, if necessary.

Agreeing to a quick peek procedure. A voluntary quick peek provision with appropriate protection for waiver under Rule 502(d) may be appropriate in circumstances or with certain types of ESI such as form contracts or documents.

Categorical approach to identification and logging of privileged ESI. Litigants might also consider excluding certain categories of documents from privilege logs. Under this approach, in lieu of logging at least some portion of the privileged documents, parties would identify categories for privileged documents, provide sufficient information about the privilege claim as well as the general subject matter of the category, and then agree or not agree that such categories should be formally logged. This approach was first discussed by Patrick Oot and Anne Kershaw

in their testimony before the Federal Rules Committee regarding the adoption of Rule 502.[122] The approach was later expanded upon and formalized by U.S. Magistrate Judge John Facciola of the District of Columbia and Jonathan Redgrave in a law review article suggesting the Facciola-Redgrave Framework, described as follows:

> The Framework involves the formal and informal exchange of information to substantiate the categories, with the goal of eliminating many potential disputes. They then propose a requirement of a detailed description for the information withheld as privileged which remains subject to dispute so that the necessity of in camera review is reduced to a minimum. The preparation of this more detailed log for a narrowly targeted population will be more useful and, in effect, much less burdensome because the number of documents which must be logged has been reduced to a minimum.[123]

The Facciola-Redgrave Framework also sets out proposed limitations for logging the "last-in-time" email in each string where each embedded component of the email is available, and exact duplicates. This approach works particularly well in complex litigation, where many of the privileged documents can be categorized together by subject matter, date, author, or recipient.[124]

---

122. See also Patrick L. Oot, *The Protective Order Toolkit: Protective Privilege with Federal Rule of Evidence 502*, 10 SEDONA CONF. J. 237 (2009).

123. Hon. John M. Facciola and Jonathan M. Redgrave, *Asserting and Challenging Privilege Claims in Modern Litigation: The Facciola-Redgrave Framework*, 4 FED. CTS. L. REV. 19, 22 (2009).

124. Some courts have found categorical logging to comply with the requirements of Fed. R. Civ. P. 26(b)(5). *See, e.g.*, GenOn Mid-Atlantic LLC v.

Comment 4(c): Litigants should use appropriate information search and retrieval methods leveraging processes and technology to improve quality and efficiency in protecting privilege during the discovery process.

Counsel has affirmative ethical duties to understand the risks and benefits of new technologies and to protect confidential client information from unnecessary disclosure.[125] Software that offers significant improvements in addressing the discovery of ESI can also be harnessed to assist in managing the sometimes "harrowing burden" of addressing privilege review and log preparation.[126] At this stage there is no "magic bullet"; ultimately, privilege review and document-by-document logging and redaction remain intensely manual processes. However, a

---

Stone & Webster, 2011 U.S. Dist. LEXIS 133724 (S.D.N.Y. Nov. 10, 2011) (accepting category logs if a document-by-document listing would be unduly burdensome and if a more detailed description would offer no significant material benefit in determining the privileged nature).

125. *See* 2012 Technology and Confidentiality Amendments to ABA MODEL RULES OF PROF'L CONDUCT, R. 1.1 Competent Client Representation ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice including the benefits and risks associated with relevant technology") and R. 1.6 Confidentiality of Information ("A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."). *See also*, The Sedona Conference, *Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-Discovery*, 15 SEDONA CONF. J. 217 (2014) at Practice Points 4 & 8.

126. In selecting appropriate technology, counsel should evaluate the data set. For example, scanned paper sources and unsearchable image files offer more limited opportunities to leverage advanced technology, but privilege analysis will be enhanced by rendering these files searchable by applying Optical Character Recognition (OCR) processing. *See, e.g.*, Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251 (D. Md. 2008) (party claiming inadvertent production of privileged materials erroneously assumed certain .pdf files were not searchable and failed to render other files searchable through optical character recognition (OCR) processing).

well-developed privilege review and logging protocol leveraging available technologies can alleviate the burden. Combining such a protocol with the protection of Rule 502(d) and incorporating the agreed-upon protocol into the parties' discovery plan minimizes the risk of dispute and waiver. The following is a discussion of some of those technologies.

A. Use of Search and Retrieval Technologies Generally

In a leading case assessing the reasonableness of a producing party's privilege and work-product screening and review process, *Victor Stanley, Inc. v. Creative Pipe*,[127] Judge Grimm considered whether a party's efforts in conducting pre-production privilege screening and review were sufficient to protect it from a finding of waiver under pre-Rule 502 standards. On the limited record provided by defendants (the producing party), the court found that defendants' efforts were inadequate. Judge Grimm noted that the

> [u]se of search and information retrieval methodology for the purpose of identifying and withholding privileged or work-product protected information from production, requires the utmost care in selecting methodology that is appropriate for the task because the consequence of failing to do so, as in this case, may be the disclosure of privileged/protected information to an adverse party, resulting in a determination by the court that the privilege/protection has been waived.[128]

Drawing on The Sedona Conference *Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-*

127. *Victor Stanley, Inc.*, 250 F.R.D. 251.

128. *Id.* at 262.

Discovery and the flaws outlined by Judge Grimm in *Victor Stanley* in the defendants' search methodology, certain principles can be extrapolated to provide broader guidance in developing standards for assessing reasonableness under Rule 502(b)(2):

- **Anticipate the need to explain and substantiate search and retrieval methodology.** Expect to be required to account for the chosen methodology to the court and parties in legal proceedings, including explaining: reasons for the specific choice of search and retrieval methods in the given legal context, the credentials of those who helped design the strategy and searches that were conducted, and the overall process in which the use of data search and retrieval technology was embedded.
- **Establish quality control measures for assessing the reliability and accuracy of results.** Provide evidence that search results were tested and verified, including through statistically valid sampling techniques.
- **Perform due diligence in selecting technology and services and remain alert to evolving technologies and methods.**
- **Assess data types in selecting appropriate technology and protocols to assist with privilege detection and analysis.**

B. Search Terms

Despite what appears to be an attack on the use of search terms in the context of document review, the use of appropriately crafted and tested search terms can be used to improve the

thoroughness of privilege detection and to create workflow efficiencies.[129] One method is to run general and matter- or entity-specific privilege ontology searches against potentially responsive data, highlighting terms to facilitate privilege review. A general privilege ontology includes common legal terminology that may indicate the presence of privilege. Terms typically found in a general privilege ontology search range from individual words (for example: privilege, privileged, legal) and phrases ("work product," "voir dire") to complex Boolean search logic constructions (privileged /2 confidential; ((A C or AC) /3 (privilege*) or (communication*)). The scope of the general privilege ontology search and exact search syntax will depend on the review platform being used and the level of searching it can support. Terms can also be designed to identify potentially privileged materials from non-domestic sources and in languages other than English. For example, search terms for data including U.K. materials might include local names for an attorney and variant spellings (solicitor, barrister, counselor, QC).

For non-English sources, a case team can work with a legally-trained fluent speaker to develop appropriate terms. For example, search terms used to capture words for attorney in various European languages include: abogad*, advogad*, advokat*, avvocat*, Rechtsanwaelt*, and Rechtsanwalt*. A customized ontology can be developed on a case- and entity-specific

129. For example, one court has commented in this context that although it is "universally acknowledged" that keyword searches are helpful for search and retrieval of ESI, "all keyword searches are not created equal," referencing the "growing body of literature that highlights the risks associated with conducting an unreliable or inadequate keyword search or relying exclusively on such searches for privilege review." Privilege ontologies are often both over-broad and too narrow in identifying privileged records. These issues can be addressed through iterative review and revision of terms supplemented by systematic testing and sampling.

basis. For a company, this may include the names and email addresses of known in-house and outside counsel from the appropriate time period, along with individual email addresses (jdoe@xylaw.com) and general domain names (*@xylaw.com). Software programs that report email domain names in a data set can be used to build searches designed to identify counsel. Some corporate legal department email addresses include an identifying term and this metadata can help with detection. Terms can also be designed to identify data relating to other known litigation and legal issues reflected in the data set.

Search terms might also be used to screen out and segregate documents that are likely to contain privileged material. Records that do not contain privileged terms might be prioritized for review as they are more likely to yield non-privileged documents that can be expedited for production. And records that do not contain privilege terms may be directed to less experienced reviewers, while documents containing privilege terms and data for custodians who are attorneys can be assigned to a more experienced review team.

C. Advanced Search Methodologies

Advanced technologies may further enhance privilege detection and reduce the review burden. For review purposes, email threading and near-duplicate programs can be used to identify records related to those containing privileged ontology terms, allowing entire conversations or successive drafts of documents to be batched for streamlined analysis. Functionality that supports computer-aided review can be harnessed to identify privileged records.

Concept or clustering engines can be used to identify records related to privileged records. These techniques can be especially valuable as pre-production quality control measures when run against the putative production set to locate records

that may not have been recognized as being privileged in the regular review process.

Specific pre-production analysis software is also available for this purpose, running fuzzy hash value and other searches against the data set and load file to detect for qualitative analysis, suspicious records, and metadata included in the production before a transfer is made.

At this stage, few courts have been called on to analyze the use of advanced analytical software in discovery in general, and fewer still have evaluated its application in the context of protecting privilege and work-product protection. Those courts that have assessed the adequacy of a producing party's use of search technology in the context of privilege and work-product protection have generally found the efforts wanting.[130] Nevertheless, analysis and commentary surrounding these cases with mostly negative outcomes are instructive and provide guidance in developing standards under Rule 502(b)(2) for using technology to help establish that "reasonable steps" were taken to prevent disclosure.

D. Technology-Assisted Review

Numerous authors and ESI vendors have advocated Technology-Assisted Review ("TAR") as a means to potentially reduce the burden on privilege identification and review. Using TAR, a training set comprising a subset of the producing party's documents is fed into a set of algorithms to extrapolate or identify ESI that is similar to the training set. Commentators have

130. *See, e.g.*, *Victor Stanley, Inc.*, 250 F.R.D. 251 (finding that privilege/protection was waived by defendants' "voluntary production" to plaintiff); s*ee also* Paul W. Grimm, Lisa Yurwit Bergstrom & Matthew P. Kraeuter, *Federal Rule of Evidence 502: Has It Lived Up To Its Potential?*, XVII RICH. J.L. & TECH. 8 (2011), *available at* http://jolt.richmond.edu/v17i3/article8.pdf.

argued that TAR might be used to exclude from review documents that have been agreed to as clearly privileged based on sender/recipient/date/content criteria.[131] It is also possible to use TAR to generate categorical logs which include more detail regarding what and why documents are withheld, as well as a log of the documents that were not personally reviewed but fall under the category. On this front, the development, use, and acceptance of TAR engines are in their formative stages. It is too early to tell whether and to what extent these newer technologies can be used effectively in privilege review.

131. Maura R. Grossman & Gordon V. Cormack, *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review*, XVII RICH. J.L. & TECH. 11 (2011), *available at* http://jolt.richmond.edu/v17i3/article11.pdf.

APPENDIX A: RULE 502 & EXPLANATORY NOTE ON EVIDENCE RULE 502

Prepared by the Judicial Conference Advisory Committee on Evidence Rules (Revised 11/28/2007)

Rule 502. Attorney-Client Privilege and Work Product; Limitations on Waiver

The following provisions apply, in the circumstances set out, to disclosure of a communication or information covered by the attorney-client privilege or work-product protection.

(a) Disclosure Made in a Federal Proceeding or to a Federal Office or Agency; Scope of a Waiver. When the disclosure is made in a federal proceeding or to a federal office or agency and waives the attorney-client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a federal or state proceeding only if:

(1) the waiver is intentional;

(2) the disclosed and undisclosed communications or information concern the same subject matter; and

(3) they ought in fairness to be considered together.

(b) Inadvertent Disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if:

(1) the disclosure is inadvertent;

(2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and

(3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).

(c) Disclosure Made in a State Proceeding. When the disclosure is made in a state proceeding and is not the subject of

a state-court order concerning waiver, the disclosure does not operate as a waiver in a federal proceeding if the disclosure:

(1) would not be a waiver under this rule if it had been made in a federal proceeding; or

(2) is not a waiver under the law of the state where the disclosure occurred.

(d) Controlling Effect of Court Orders. A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding.

(e) Controlling Effect of a Party Agreement. An agreement on the effect of disclosure in a federal proceeding is binding only on the parties to the agreement, unless it is incorporated into a court order.

(f) Controlling Effect of This Rule. Notwithstanding Rules 101 and 1101, this rule applies to state proceedings and to federal court-annexed and federal court-mandated arbitration proceedings, in the circumstances set out in the rule. And notwithstanding Rule 501, this rule applies even if state law provides the rule of decision.

(g) Definitions. In this rule:

(1) "attorney-client privilege" means the protection that applicable law provides for confidential attorney-client communications; and

(2) "work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial."

This new rule has two major purposes:

1) It resolves some longstanding disputes in the courts about the effect of certain disclosures of communications or information protected by the attorney-client privilege or as work product—specifically those disputes involving inadvertent disclosure and subject matter waiver.

2) It responds to the widespread complaint that litigation costs necessary to protect against waiver of attorney-client privilege or work product have become prohibitive due to the concern that any disclosure (however innocent or minimal) will operate as a subject matter waiver of all protected communications or information. This concern is especially troubling in cases involving electronic discovery. *See, e.g.*, *Hopson v. City of Baltimore*, 232 F.R.D. 228, 244 (D. MD. 2005) (Grimm, J.) (electronic discovery may encompass "millions of documents" and to insist upon "record-by-record pre-production privilege review, on pain of subject matter waiver, would impose upon parties costs of production that bear no proportionality to what is at stake in the litigation").

The rule seeks to provide a predictable, uniform set of standards under which parties can determine the consequences of a disclosure of a communication or information covered by the attorney-client privilege or work-product protection. Parties to litigation need to know, for example, that if they exchange privileged information pursuant to a confidentiality order, the court's order will be enforceable. Moreover, if a federal court's confidentiality order is not enforceable in a state court then the burdensome costs of privilege review and retention are unlikely to be reduced.

The rule makes no attempt to alter federal or state law on whether a communication or information is protected under the attorney-client privilege or work-product immunity as an initial matter. Moreover, while establishing some exceptions to

waiver, the rule does not purport to supplant applicable waiver doctrine generally.

The rule governs only certain waivers by disclosure. Other common-law waiver doctrines may result in a finding of waiver even where there is no disclosure of privileged information or work product. *See, e.g., Nguyen v. Excel Corp.*, 197 F.3d 200 (5th Cir. 1999) (reliance on an advice of counsel defense waives the privilege with respect to attorney-client communications pertinent to that defense); *Ryers v. Burleson*, 100 F.R.D. 436 (D. D.C. 1983) (allegation of lawyer malpractice constituted a waiver of confidential communications under the circumstances). The rule is not intended to displace or modify federal common law concerning waiver of privilege or work product where no disclosure has been made.

Subdivision (a). The rule provides that a voluntary disclosure in a federal proceeding or to a federal office or agency, if a waiver, generally results in a waiver only of the communication or information disclosed; a subject matter waiver (of either privilege or work product) is reserved for those unusual situations in which fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary. *See, e.g., In re United Mine Workers of America Employee Benefit Plans Litig.*, 159 F.R.D. 307, 312 (D. D.C. 1994) (waiver of work product limited to materials actually disclosed, because the party did not deliberately disclose documents in an attempt to gain a tactical advantage). Thus, subject matter waiver is limited to situations in which a party intentionally puts protected information into the litigation in a selective, misleading and unfair manner. It follows that an inadvertent disclosure of protected information can never result in a subject matter waiver. *See* Rule 502(b). The rule rejects the result in *In re Sealed Case*, 877 F.2d 976 (D.C. Cir. 1989), which held that inadvertent disclosure

of documents during discovery automatically constituted a subject matter waiver.

The language concerning subject matter waiver—"ought in fairness"—is taken from Rule 106, because the animating principle is the same. Under both Rules, a party that makes a selective, misleading presentation that is unfair to the adversary opens itself to a more complete and accurate presentation.

To assure protection and predictability, the rule provides that if a disclosure is made at the federal level, the federal rule on subject matter waiver governs subsequent state court determinations on the scope of the waiver by that disclosure.

Subdivision (b). Courts are in conflict over whether an inadvertent disclosure of a communication or information protected as privileged or work product constitutes a waiver. A few courts find that a disclosure must be intentional to be a waiver. Most courts find a waiver only if the disclosing party acted carelessly in disclosing the communication or information and failed to request its return in a timely manner. And a few courts hold that any inadvertent disclosure of a communication or information protected under the attorney-client privilege or as work product constitutes a waiver without regard to the protections taken to avoid such a disclosure. *See generally Hopson v. City of Baltimore*, 232 F.R.D. 228 (D. Md. 2005), for a discussion of this case law.

The rule opts for the middle ground: inadvertent disclosure of protected communications or information in connection with a federal proceeding or to a federal office or agency does not constitute a waiver if the holder took reasonable steps to prevent disclosure and also promptly took reasonable steps to rectify the error. This position is in accord with the majority view on whether inadvertent disclosure is a waiver.

Cases such as *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985) and *Hartford Fire Ins.*

Co. v. Garvey, 109 F.R.D. 323, 332 (N.D. Cal. 1985), set out a multifactor test for determining whether inadvertent disclosure is a waiver. The stated factors (none of which is dispositive) are the reasonableness of precautions taken, the time taken to rectify the error, the scope of discovery, the extent of disclosure and the overriding issue of fairness. The rule does not explicitly codify that test, because it is really a set of non-determinative guidelines that vary from case to case. The rule is flexible enough to accommodate any of those listed factors. Other considerations bearing on the reasonableness of a producing party's efforts include the number of documents to be reviewed and the time constraints for production. Depending on the circumstances, a party that uses advanced analytical software applications and linguistic tools in screening for privilege and work product may be found to have taken "reasonable steps" to prevent inadvertent disclosure. The implementation of an efficient system of records management before litigation may also be relevant.

The rule does not require the producing party to engage in a post-production review to determine whether any protected communication or information has been produced by mistake. But the rule does require the producing party to follow up on any obvious indications that a protected communication or information has been produced inadvertently.

The rule applies to inadvertent disclosures made to a federal office or agency, including but not limited to an office or agency that is acting in the course of its regulatory, investigative or enforcement authority. The consequences of waiver, and the concomitant costs of pre-production privilege review, can be as great with respect to disclosures to offices and agencies as they are in litigation.

Subdivision (c). Difficult questions can arise when 1) a disclosure of a communication or information protected by the at-

torney-client privilege or as work product is made in a state proceeding, 2) the communication or information is offered in a subsequent federal proceeding on the ground that the disclosure waived the privilege or protection, and 3) the state and federal laws are in conflict on the question of waiver. The Committee determined that the proper solution for the federal court is to apply the law that is most protective of privilege and work product. If the state law is more protective (such as where the state law is that an inadvertent disclosure can never be a waiver), the holder of the privilege or protection may well have relied on that law when making the disclosure in the state proceeding. Moreover, applying a more restrictive federal law of waiver could impair the state objective of preserving the privilege or work-product protection for disclosures made in state proceedings. On the other hand, if the federal law is more protective, applying the state law of waiver to determine admissibility in federal court is likely to undermine the federal objective of limiting the costs of production.

The rule does not address the enforceability of a state court confidentiality order in a federal proceeding, as that question is covered both by statutory law and principles of federalism and comity. *See* 28 U.S.C. § 1738 (providing that state judicial proceedings "shall have the same full faith and credit in every court within the United States . . . as they have by law or usage in the courts of such State . . . from which they are taken"). *See also Tucker v. Ohtsu Tire & Rubber Co.*, 191 F.R.D. 495, 499 (D. Md. 2000) (noting that a federal court considering the enforceability of a state confidentiality order is "constrained by principles of comity, courtesy, and . . . federalism"). Thus, a state court order finding no waiver in connection with a disclosure made in a state court proceeding is enforceable under existing law in subsequent federal proceedings.

Subdivision (d). Confidentiality orders are becoming increasingly important in limiting the costs of privilege review

and retention, especially in cases involving electronic discovery. But the utility of a confidentiality order in reducing discovery costs is substantially diminished if it provides no protection outside the particular litigation in which the order is entered. Parties are unlikely to be able to reduce the costs of pre-production review for privilege and work product if the consequence of disclosure is that the communications or information could be used by non-parties to the litigation.

There is some dispute on whether a confidentiality order entered in one case is enforceable in other proceedings. *See generally Hopson v. City of Baltimore*, 232 F.R.D. 228 (D. Md. 2005), for a discussion of this case law. The rule provides that when a confidentiality order governing the consequences of disclosure in that case is entered in a federal proceeding, its terms are enforceable against non-parties in any federal or state proceeding. For example, the court order may provide for return of documents without waiver irrespective of the care taken by the disclosing party; the rule contemplates enforcement of "claw-back" and "quick peek" arrangements as a way to avoid the excessive costs of pre-production review for privilege and work product. *See Zubulake v. UBS Warburg* LLC, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (noting that parties may enter into "so-called 'claw-back' agreements that allow the parties to forego privilege review altogether in favor of an agreement to return inadvertently produced privileged documents"). The rule provides a party with a predictable protection from a court order—predictability that is needed to allow the party to plan in advance to limit the prohibitive costs of privilege and work-product review and retention.

Under the rule, a confidentiality order is enforceable whether or not it memorializes an agreement among the parties to the litigation. Party agreement should not be a condition of enforceability of a federal court's order.

Under subdivision (d), a federal court may order that disclosure of privileged or protected information "in connection with" a federal proceeding does not result in waiver. But subdivision (d) does not allow the federal court to enter an order determining the waiver effects of a separate disclosure of the same information in other proceedings, state or federal. If a disclosure has been made in a state proceeding (and is not the subject of a state-court order on waiver), then subdivision (d) is inapplicable. Subdivision (c) would govern the federal court's determination whether the state-court disclosure waived the privilege or protection in the federal proceeding.

Subdivision (e). Subdivision (e) codifies the well-established proposition that parties can enter an agreement to limit the effect of waiver by disclosure between or among them. Of course such an agreement can bind only the parties to the agreement. The rule makes clear that if parties want protection against non-parties from a finding of waiver by disclosure, the agreement must be made part of a court order.

Subdivision (f). The protections against waiver provided by Rule 502 must be applicable when protected communications or information disclosed in federal proceedings are subsequently offered in state proceedings. Otherwise the holders of protected communications and information, and their lawyers, could not rely on the protections provided by the rule, and the goal of limiting costs in discovery would be substantially undermined. Rule 502(f) is intended to resolve any potential tension between the provisions of Rule 502 that apply to state proceedings and the possible limitations on the applicability of the Federal Rules of Evidence otherwise provided by Rules 101 and 1101.

The rule is intended to apply in all federal court proceedings, including court-annexed and court-ordered arbitrations, without regard to any possible limitations of Rules 101 and

1101. This provision is not intended to raise an inference about the applicability of any other rule of evidence in arbitration proceedings more generally.

The costs of discovery can be equally high for state and federal causes of action, and the rule seeks to limit those costs in all federal proceedings, regardless of whether the claim arises under state or federal law. Accordingly, the rule applies to state law causes of action brought in federal court.

Subdivision (g). The rule's coverage is limited to attorney-client privilege and work product. The operation of waiver by disclosure, as applied to other evidentiary privileges, remains a question of federal common law. Nor does the rule purport to apply to the Fifth Amendment privilege against compelled self-incrimination. The definition of work-product "materials" is intended to include both tangible and intangible information. *See In re Cendant Corp. Sec. Litig*., 343 F.3d 658, 662 (3d Cir. 2003) ("work product protection extends to both tangible and intangible work product").

APPENDIX B: RULES RELATING TO THE CLAIM OF PRIVILEGE

A. Federal Rules of Civil Procedure Rule 26(b)(5) – Language of the Rule

The 2006 Amendments added a procedure for claiming privilege and work product after inadvertent production during discovery. The rule did not resolve the issue of whether the production constituted a waiver.[132]

B. Rule 26 of The Federal Rules of Civil Procedure: General Provisions Regarding Discovery; Duty of Disclosure

1. Discovery Scope and Limits

Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

2. Claims of Privilege or Protection of Trial Preparation Materials

When a party withholds information otherwise discoverable under these rules by claiming that it is privileged or subject to protection as trial preparation material, the party shall make the claim expressly and shall describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection.

3. Summary of Advisory Committee Notes

Subdivision (b)(2). The [2006] amendment to Rule 26(b)(2) is designed to address issues raised by difficulties in lo-

132. 12 OKLA. ST. § 3226(B)(5)(b) (2010) ("[t]his mechanism" does not alter the standards governing whether the information is privileged or subject to protection as trial preparation material or whether such privilege or protection has been waived).

cating, retrieving, and providing discovery of some electronically stored information. Electronic storage systems often make it easier to locate and retrieve information. These advantages are properly taken into account in determining the reasonable scope of discovery in a particular case. But some sources of electronically stored information can be accessed only with substantial burden and cost. In a particular case, these burdens and costs may make the information on such sources not reasonably accessible.

It is not possible to define in a rule the different types of technological features that may affect the burdens and costs of accessing electronically stored information. Information systems are designed to provide ready access to information used in regular ongoing activities. They also may be designed so as to provide ready access to information that is not regularly used. But a system may retain information on sources that are accessible only by incurring substantial burdens or costs. Subparagraph (B) is added to regulate discovery from such sources.

Under this rule, a responding party should produce electronically stored information that is relevant, not privileged, and reasonably accessible, subject to the (b)(2)(C) limitations that apply to all discovery. The responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.

A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence. Whether a responding party is required to preserve unsearched sources of potentially responsive information that it

believes are not reasonably accessible depends on the circumstances of each case. It is often useful for the parties to discuss this issue early in discovery.

The volume of—and the ability to search—much electronically stored information means that in many cases the responding party will be able to produce information from reasonably accessible sources that will fully satisfy the parties' discovery needs. In many circumstances the requesting party should obtain and evaluate the information from such sources before insisting that the responding party search and produce information contained on sources that are not reasonably accessible. If the requesting party continues to seek discovery of information from sources identified as not reasonably accessible, the parties should discuss the burdens and costs of accessing and retrieving the information, the needs that may establish good cause for requiring all or part of the requested discovery even if the information sought is not reasonably accessible, and conditions on obtaining and producing the information that may be appropriate.

If the parties cannot agree whether, or on what terms, sources identified as not reasonably accessible should be searched and discoverable information produced, the issue may be raised either by a motion to compel discovery or by a motion for a protective order. The parties must confer before bringing either motion. If the parties do not resolve the issue and the court must decide, the responding party must show that the identified sources of information are not reasonably accessible because of undue burden or cost. The requesting party may need discovery to test this assertion. Such discovery might take the form of requiring the responding party to conduct a sampling of information contained on the sources identified as not reasonably accessible; allowing some form of inspection of such sources; or taking depositions of witnesses knowledgeable about the responding party's information systems.

Once it is shown that a source of electronically stored information is not reasonably accessible, the requesting party may still obtain discovery by showing good cause, considering the limitations of Rule 26(b)(2)(C) that balance the costs and potential benefits of discovery. The decision whether to require a responding party to search for and produce information that is not reasonably accessible depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified in the circumstances of the case. Appropriate considerations may include: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

The responding party has the burden as to one aspect of the inquiry—whether the identified sources are not reasonably accessible in light of the burdens and costs required to search for, retrieve, and produce whatever responsive information may be found. The requesting party has the burden of showing that its need for the discovery outweighs the burdens and costs of locating, retrieving, and producing the information. In some cases, the court will be able to determine whether the identified sources are not reasonably accessible and whether the requesting party has shown good cause for some or all of the discovery, consistent with the limitations of Rule 26(b)(2)(C), through a single proceeding or presentation. The good-cause determination, however, may be complicated because the court and parties may know little about what information the sources identified

as not reasonably accessible might contain, whether it is relevant, or how valuable it may be to the litigation. In such cases, the parties may need some focused discovery, which may include sampling of the sources, to learn more about what burdens and costs are involved in accessing the information, what the information consists of, and how valuable it is for the litigation in light of information that can be obtained by exhausting other opportunities for discovery.

The good-cause inquiry and consideration of the Rule 26(b)(2)(C) limitations are coupled with the authority to set conditions for discovery. The conditions may take the form of limits on the amount, type, or sources of information required to be accessed and produced. The conditions may also include payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible. A requesting party's willingness to share or bear the access costs may be weighed by the court in determining whether there is good cause. But the producing party's burdens in reviewing the information for relevance and privilege may weigh against permitting the requested discovery.

C. Federal Rule of Evidence 502 – Rulemaking and Legislative History of the Rule[133]

1. Advisory Committee on the Federal Rules of Evidence

On April 24, 2006, The United States Judicial Advisory Committee on the Federal Rules of Evidence held a mini-conference inviting a broad-based coalition of judges, academics, and

133. Patrick L. Oot, *The Protective Order Toolkit: Protective Privilege with Federal Rule of Evidence 502*, 10 SEDONA CONF. J. 237 (2009).

practitioners to discuss the state of privilege protection in litigation and the need for rules reform.[134] After the hearings, the committee approved the proposed new Rule 502 for publication to the general public and scheduled two hearing dates where the committee would consider public testimony.

On January 29, 2007, there were 24 speakers in courtroom 24A at 500 Pearl Street in New York to testify before The Advisory Committee about the benefits of Proposed Federal Rule of Evidence 502. The participants sought to persuade the Advisory Committee to approve the expansion of privilege protection for all parties in litigation and regulatory filings by providing hard data about the true cost of protecting privilege for a single matter.

Described in part of the testimony was the laborious and tedious process of multi-tier document review that litigants wade-through in an effort to locate relevant documents and to prevent privileged information from disclosure. It was further described that plaintiffs and defendants used this expensive and time-consuming process in hopes to avoid the (pre-Rule 502) perils that occur when a party inadvertently produces a privileged document. One participant revealed to the Advisory Committee the cost of responding to document requests and protecting privilege for a single real-life matter. His corporate employer spent over $13.5 million reviewing and logging documents for relevancy and privilege in a single matter.[135] The testimony also focused on the issues associated with manual review in terms of time, cost, accuracy, and consistency.

---

134. The materials for the April 24, 2006, meeting can be found at http://www.uscourts.gov/rules-policies/archives/agenda-books/advisory-committee-rules-evidence-april-2006. The Sedona Conference Advisory Board was represented at the meeting by several members and observers.

135. *See* Gartner RAS Core Research Note G00148170, *Cost of eDiscovery Threatens to Skew Justice System*, ID Number: G00148170, KNOWLEDGE

The testimony discussed alternate, less-expensive techniques to protect privilege that would be possible if Rule 502 was enacted. For example, it was explained how a litigant could "bucket" or "set-aside" documents that contain law-firm domain names and documents which advanced search engines can flag as potentially privileged.[136] If a producing party had a multi-jurisdictionally enforceable Protective Order under Rule 502 with a claw-back, that party could feel more comfortable rapidly producing or even providing an initial quick-peek to the remaining corpus of data. The parties could also exchange electronically exported logs of the "potentially privileged" withheld bucket. Subsequently, the requesting party could develop better targeted search methods and requests for the set-aside data sets. Allowing litigants to conduct a real initial investigation furthers both a better understanding of the case and the goals of Federal Civil Procedure Rule 1.[137]

2. Advisory Committee Report

After the public hearings, on May 15, 2007, the Advisory Committee issued a Report of the Advisory Committee of Evidence Rules, modifying the previously published proposed

---

STRATEGY SOLUTIONS (April 20, 2007), *available at* http://www.knowledgestrategysolutions.com/wp-content/uploads/cost_of_ediscovery_threatens_148170-2.pdf. Coincidentally, this 2005 statistic is often cited as one of the few data-points available regarding the cost of document review in complex litigation and regulatory filings in the United States. *See also* Adreas Kluth, *The Big Data Dump*, THE ECONOMIST (August 28, 2008), http://www.economist.com/node/12010377. *See also*, Daniel Fisher, *The Data Explosion*, FORBES (October 1, 2007), http://www.forbes.com/forbes/2007/1001/072.html.

136. *See* Report of the Advisory Committee on Rules of Evidence (May 15, 2007), *available at* http://www.uscourts.gov/rules-policies/archives/committee-reports/advisory-committee-rules-evidence-may-2007.

137. FED. R. CIV. P. 1.

Rule.[138] The report dropped the selective waiver provision, stretched the jurisdiction of the rule (and Protective Orders) to state forums (for disclosures made in federal court) and productions to federal agencies, almost eliminated subject-matter waiver, and instituted principles of reasonableness to avoid waiver for inadvertent disclosure.[139]

The report cited precedent that "set out multi-factor tests for determining whether the inadvertent disclosure is a waiver."[140] Although the report did not codify the inquiry, it included a pentad test drawn from the case law. In determining whether waiver applies for inadvertent disclosures, courts should consider:

(1) the reasonableness of the precautions taken;
(2) the time taken to rectify the error;
(3) the scope of discovery;
(4) the extent of discovery; and
(5) the over-ridding issue of fairness.[141]

The Advisory Committee also provided guidance to courts with additional considerations when interpreting the *reasonableness of the precautions taken*. Interestingly, the additional considerations refresh twenty-year-old waiver tests with elements contemplating the massive data volumes litigants face when managing discovery. The reasonableness considerations include:

---

138. *See* Report of the Advisory Committee on Evidence Rules, *available at* http://www.uscourts.gov/rules-policies/archives/committee-reports/advisory-committee-rules-evidence-may-2007.

139. *Id*.

140. *Id.* (citing Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co., 104 F.R.D. 103, 105 (S.D.N.Y. 1985) and Hartford Fire Ins. Co. v. Garvey, 109 F.R.D. 323, 332 (N.D. Cal. 1985)).

141. *Id*.

(1) the number of documents to be reviewed;
(2) the time constraints for production;
(3) the use of software applications and linguistic tools in screening for privilege; and
(4) the implementation of an efficient records management system before litigation.[142]

Finally, the committee expressly stated that Rule 502 does not require a post production review, but litigants should follow up on any obivous indications of inadvertent production.[143]

3. Legislative Enactment

Both The Committee on Rules of Practice and Procedure and The Judicial Conference approved the proposed Rule for transmittal to Congress.[144] On September 26, 2007, Hon. Lee Rosenthal, Chair of The United States Judicial Conference transmitted the resulting proposed Rule 502; developed from over 70 public comments, the testimony of over 20 witnesses, the views of the Subcommitte on Style, and the Advisory Committe's own judgement.[145] The transmittal letter also included a proposed Committee Note that the Judicial

142. *Id*.

143. *Id*.

144. Because the draft Rule involved an evidentiary privilege, congressional action was required before the Rule could be adopted. *See* 28 U.S.C. § 2074(b) ("Any such rule creating, abolishing, or modifying an evidentiary privilege shall have no force or effect unless approved by Act of Congress.").

145. Letter from Hon. Lee H. Rosenthal to Hon. Patrick Leahy, Hon. Arlen Specter, Hon. John Conyers, Jr., and Hon. Lamar Smith, transmitting Proposed New Federal Rule of Evidence 502 to Judiciary Committee (September 26, 2007), *available at* http://federalevidence.com/pdf/2008/06-June/Hill_Letter_EV_502on9-26-07.pdf.

Conference sought to include in the legislative history of Rule 502.[146]

Senator Leahy introduced the proposed rule in the Senate on December 11, 2007. On January 31, 2008, the Senate Judiciary Committee approved the bill unanimously without amendment and published its findings to the full Senate with a written report.[147] After incorporating the Advisory Committee Notes, the bill passed in the Senate on February 27, 2008, and The House of Representatives on September 8, 2008. The bill was enacted as Public Law 110-322 on September 18, 2008, to amend the Federal Rules of Evidence to address the waiver of the attorney-client privilege and the work-product doctrine.[148]

---

146. *Id*.

147. S. REP. NO. 110–264 (February 25, 2008) ("The rule proposed by the Standing Committee is aimed at adapting to the new realities that a accompany today's modes of communication, and reducing the burdens associated with the conduct of diligent electronic discovery.").

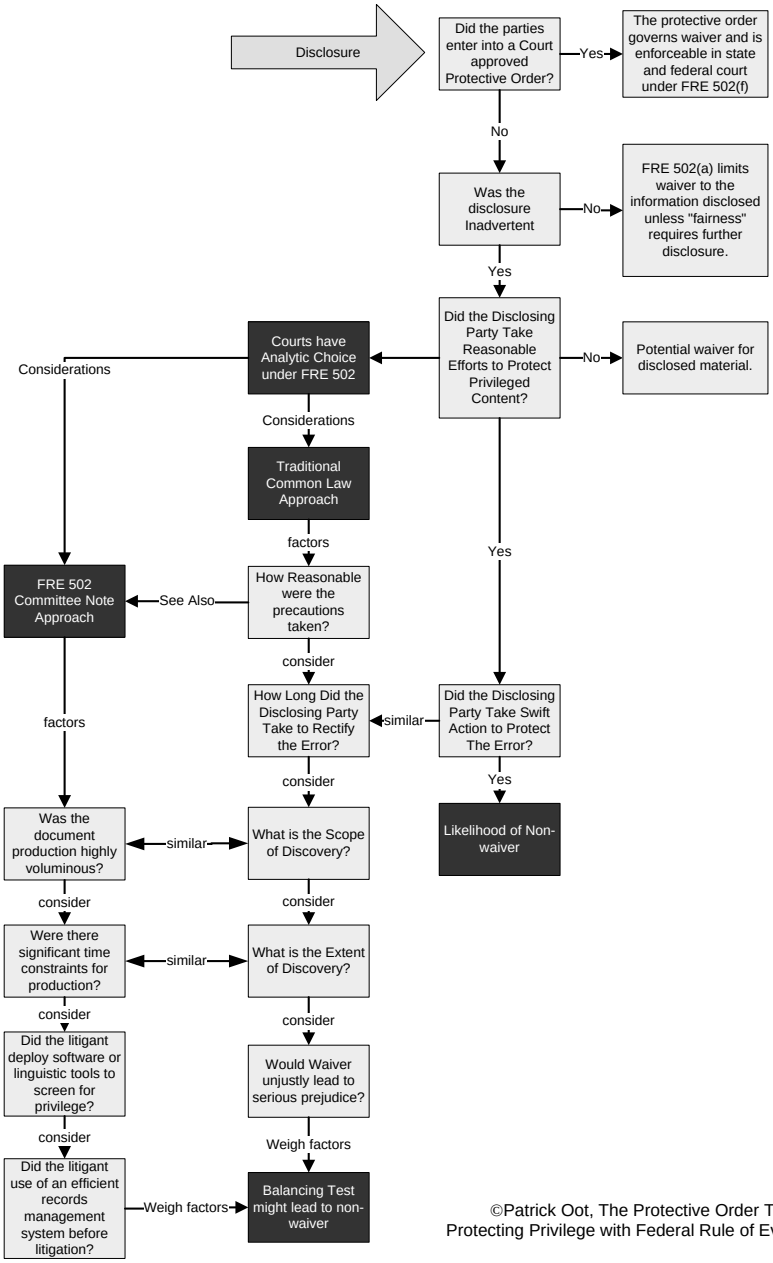
148. *See* 154 CONG. REC. S1317 (Feb. 27, 2008) (remarks of Sen. Leahy) ("I ask unanimous consent to have printed in the Record the Judicial Conference's Committee Note to illuminate the purpose of the new Federal Rule of Evidence and how it should be applied."); 154 CONG. REC. H7818 (Sept. 8, 2008) (remarks of Rep. Jackson Lee) ("In order to more fully explain how the new rule is to be interpreted and applied, the Advisory Committee also prepared an explanatory note, as is customary, for publication alongside the text of the rule. The text of the explanatory note appears in the Record in the Senate debate."). Administration of George W. Bush, Acts Approved by the President, 1234 (2008).

4. Language of Federal Rule of Evidence 502

Rule 502(a)	Disclosure Made in a Federal Proceeding or to a Federal Office or Agency; Scope of a Waiver: Rule 502(a) limits waiver of the privilege normally to the communication or materials disclosed, and not to the entire subject matter of the communication. The scope of any waiver is therefore confined to the information disclosed unless "fairness" requires further disclosure.
Rule 502(b)	Inadvertent Disclosure: Rule 502(b) clarifies that inadvertent disclosure does not result in waiver when the holder of the privilege "took reasonable steps to prevent disclosure" and "promptly took reasonable steps to rectify the error."
Rule 502(c)	Disclosure Made in a State Proceeding: Rule 502(c) addresses circumstances where disclosure was first made in a state proceeding and is later considered in a federal proceeding. The provision applies the federal or state law that furnishes the greatest protection to the privilege and work product.
Rule 502(d)	Controlling Effect of a Court Order: Rule 502(d) recognizes that a federal court may enter a confidentiality order providing "that the privilege or protection is not waived by disclosure connected with the litigation pending before the court."
Rule 502(e)	Controlling Effect of a Party Agreement: Rule 502(e) allows parties to enter into an agreement to limit the effect of any disclosure. The agreement is only binding on the parties unless the agreement is included in a court order.
Rule 502(f)	Controlling Effect of This Rule: Rule 502(f) notes that the rule "applies to state proceedings and to federal court-annexed and federal court-mandated arbitration proceedings" and "even if state law provides the rule of decision."
Rule 502(g)	Definitions: Rule 502(g) includes definitions for "attorney-client privilege" and "work-product protection."

APPENDIX C: NAVIGATING FRE 502 IN FEDERAL COURT

Navigating FRE 502 in Federal Court



©Patrick Oot, The Protective Order Toolkit:
Protecting Privilege with Federal Rule of Evidence 502

APPENDIX D: MODEL RULE 502(d) ORDER

[COURT NAME]
[DISTRICT OR COUNTY]

Plaintiffs,	Case No. _____
vs.	
Defendants.	

[PROPOSED] STIPULATED ORDER REGARDING THE DISCLOSURE OF PRIVILEGED INFORMATION

The [insert name of parties], by and through their respective counsel, have jointly stipulated to the terms of Stipulated Order Governing the Disclosure of Privileged Information, and with the Court being fully advised as to the same, it is hereby ORDERED:

I. APPLICABILITY

1. This Order shall be applicable to and govern all deposition transcripts and/or videotapes, and documents produced in response to requests for production of documents, answers to interrogatories, responses to requests for admissions, affidavits, declarations and all other information or material produced, made available for inspection, or otherwise submitted by any of the parties in this litigation as well as testimony adduced at trial or during any hearing (collectively "Information").

II. PRODUCTION OF DISCOVERY MATERIALS CONTAINING POTENTIALLY PRIVILEGED INFORMATION

1. The production of any privileged or otherwise protected or exempted Information, as well as the production of Infor-

mation without an appropriate designation of confidentiality, shall not be deemed a waiver or impairment of any claim of privilege or protection, including, but not limited to, the attorney-client privilege, the protection afforded to work-product materials, or the subject matter thereof, or the confidential nature of any such Information, as to the produced Information, or any other Information.

2. The production of privileged or work-product protected documents, electronically stored information ("ESI") or Information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d).
3. The producing party must notify the receiving party promptly, in writing, upon discovery that a document has been produced. Upon receiving written notice from the producing party that privileged and/or work-product material has been produced, all such Information, and all copies thereof, shall be returned to the producing party within ten (10) business days of receipt of such notice and the receiving party shall not use such information for any purpose, except as provided in paragraph 5, until further Order of the Court. The receiving party shall also attempt, in good faith, to retrieve and return or destroy all copies of the documents in electronic format.
4. The receiving party may contest the privilege or work-product designation by the producing party, shall give the producing party written notice of the reason for said disagreement. However, the receiving party may not challenge the privilege or immunity claim by arguing that the disclosure itself is a waiver of any applicable privilege. In that instance, the receiving party shall, within fifteen (15) business days

from the initial notice by the producing party, seek an Order from the Court compelling the production of the material.

5. Any analyses, memoranda or notes which were internally generated based upon such produced Information shall immediately be placed in sealed envelopes, and shall be destroyed in the event that (a) the receiving party does not contest that the Information is privileged, or (b) the Court rules that the Information is privileged. Such analyses, memoranda or notes may only be removed from the sealed envelopes and returned to its intended purpose in the event that (a) the producing party agrees in writing that the Information is not privileged, or (b) the Court rules that the Information is not privileged.
6. Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or Information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected Information before production.

STIPULATED AND AGREED TO on _____.

[INSERT NAME OF PLAINTIFF]

By: _____

[INSERT NAME OF DEFENDANT]

By: _____

IT IS SO ORDERED: _____

[Insert name.]

United States District Court Judge

DATED:

Dated: _____

APPENDIX E: MODEL RULE 502(d) ORDER POSTED BY HON. ANDREW J. PECK (S.D.N.Y.)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- -	x	
	:	RULE 502(d) ORDER
	:	
	:	
	:	
	:	
- -	x	

ANDREW J. PECK, United States Magistrate Judge:

1. The production of privileged or work-product protected documents, electronically stored information ("ESI") or information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d).

2. Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.

SO ORDERED.

Dated: New York, New York

[DATE]

_____
Andrew J. Peck
United States Magistrate Judge

Copies by ECF to: All Counsel

Judge _____

APPENDIX F: FEDERAL RULE 502—STATE LAW ANALOGUES

Federal Rule 502 applies to disclosures in federal proceedings and to federal offices and agencies. The rule addresses waiver in connection with such disclosures in the initial federal proceeding and in subsequent federal and state proceedings. Rule 502 also contains a provision concerning waiver in a federal court with respect to a production in a prior state proceeding.

However, the applicable state's privilege, work product, and waiver law govern disclosures made solely in a state proceeding and may govern disclosures made initially in a state proceeding, if the applicable state law affords more protection than federal law. Traditionally, different states have employed different tests to determine whether the attorney-client privilege or the work-product doctrine has been waived.

Since Federal Rule 502 was enacted in September 2008, a number of states have adopted versions of Federal Rule 502. For example, Arizona, Alabama, Delaware, Illinois, Indiana, Iowa, Kansas, Vermont, Virginia, Washington, and West Virginia have enacted rules or statutes that contain most of the provisions of Federal Rule 502, namely 502(a), (b), (d), (e), and (g).[149]

---

149. ARIZ. R. EVID. 502 (contains analogues to Fed. R. Evid. 502(a), (b), (d), (e), and (g) with respect to disclosures in an Arizona proceeding, and subsection (c) of the Arizona rule addresses disclosures in federal proceedings and another state's proceedings);

ALA. R. EVID. 510 (contains analogues to Fed. R. Evid. 502(a), (b), (c), (d), (e), and (g) with respect to disclosures in an Alabama proceeding);

DRE 510 (Delaware Uniform Rule of Evidence 510 contains analogues to Fed. R. Evid. 502(a) – (e) with respect to disclosures made to law enforcement agencies and in state proceedings);

ILL. R. EVID. 502 (contains analogues to Fed. R. Evid. 502(a), (b), (d), (e), and (g) with respect to disclosures in an Illinois proceeding or to an Illinois office

The Alabama, Arizona, Illinois, Kansas, Vermont, Washington, and West Virginia enactments also contain provisions concerning disclosures made in federal proceedings or another state's proceedings, which are analogues to Federal Rule 502(c).[150] Wisconsin's statute contains analogues to Rule 502(a) and (b).[151]

---

or agency, and subsection (c) of the Illinois rule addresses disclosures in federal proceedings and another state's proceedings, and disclosures to federal, or another state's, offices or agencies);

IND. R. EVID. 502 (contains analogues to Fed. R. Evid. 502(a), (b), (d), and (e) with respect to disclosures in court proceedings);

IOWA R. EVID. 5.502 (contains analogues to Fed. R. Evid. 502(a), (b), (d), (e), and (g) with respect to disclosures in court or agency proceedings);

KAN. STAT. ANN. § 60-426a (West 2012) (contains analogues to Fed. R. Evid. 502(a), (b), (d), (e), and (g) with respect to disclosures in court or agency proceedings, and subsection (c) of the Kansas rule addresses non-Kansas proceedings);

VT. R. EVID. 510(b)(1-6) (contains analogues to Fed. R. Evid. 502(a), (b), (d), (e), and (g) with respect to disclosures in Vermont proceedings or to a Vermont office or agency, and subsection (3) of the Vermont rule addresses non-Vermont proceedings);

VA. CODE ANN. § 8.01-420.7 (West 2012) (contains analogues to Fed. R. Evid. 502(a), (b), (d), and (e) with respect to disclosures in a proceeding or to any public body);

WASH. R. EVID. 502 (contains analogues to Fed. R. Evid. 502(a), (b), (d), (e), and (g) with respect to disclosures in Washington proceedings or to Washington offices or agencies, and subsection (c) of the Washington rule addresses non-Washington proceedings);

W. VA. R. EVID. 502 (contains analogues to Fed. R. Evid. 502(a), (b), (c), (d), (e), and (g) with respect to disclosures in a West Virginia court or agency).

150. ALA. R. EVID. 510; ARIZ. R. EVID. 502(c); ILL. R. EVID. 502(c); KAN. STAT. ANN. § 60-426a(c) (West 2012); VT. R. EVID. 510(b)(3); WASH. R. EVID. 502(c); W. VA. R. EVID. 502(c).

151. WIS. STAT. § 905.03(5)(a) and (b) (2013) (contain analogues to Fed. R. Evid. 502(a) and (b), although the Wisconsin statute uses the term "inadvertent" instead of "intentional" in its Rule 502(a) counterpart).

Maryland's rule predated Federal Rule 502 but has provisions that are analogous to Rule 502(b), (d), and (e).[152]

The rules of several states only contain Rule 502(b) equivalents.[153] Most of those rules provide, in substance, that an inadvertent disclosure does not operate as a waiver if the privilege holder took reasonable steps to prevent the inadvertent disclosure and promptly took reasonable steps to rectify the inadvertent disclosure after it was discovered.

It is also worth noting that the Louisiana rule requires the receiving party to return or promptly safeguard the inadvertently produced privileged material—without notification from the producing party—if it is clear that the material received is privileged.[154] That provision is more akin to the ethical requirements of certain jurisdictions under those circumstances.

---

152. MD. CODE ANN., MD. RULES § 2-402(e)(3) and (4) (West 2012) (contains analogues to Fed. R. Evid. 502(b), (d), and (e)).

153. TENN. R. EVID. 502 (generally similar to Fed. R. Evid. 502(b));

LA. CODE CIV. PROC. ANN. art. 1:1424(D) (2012) (generally similar to Fed. R. Evid. 502(b) in that an inadvertent disclosure made in connection with litigation or administrative proceedings "does not operate as a waiver if [the privilege holder] took reasonably prompt measures" after learning of "the disclosure, to notify the receiving party of the inadvertence of the disclosure and the privilege asserted." After receiving such notice, "the receiving party shall either return or promptly safeguard the [inadvertently disclosed] material," but may assert waiver.);

OKLA. STAT. tit. 12, § 2502(E) and (F) (2012) (Subsection E is similar to Fed. R. Evid. 502(b). Subsection F addresses waiver in connection with productions to a "governmental office, agency or political subdivision in the exercise of its regulatory, investigative, or enforcement authority.").

154. LA. CODE CIV. PROC. ANN. art. 1:1424(D) (2012) (Without receiving notice from the producing party, "if it is clear that the material received is privileged and inadvertently produced, the receiving party shall either return or promptly safeguard the material, and shall notify the sending party . . . with the option of asserting a waiver.").

Some states, such as Arkansas, Florida, Massachusetts, New Hampshire, and Texas, have rules that address waiver in connection with inadvertent productions.[155] Those statutes do not, however, mirror the language of Federal Rule 502(b) and do not contain other subsections of Rule 502.

---

155. ARK. R. EVID. 502(e) and (f) (Under subsection (e) of the Arkansas rule, an "[i]nadvertent disclosure does not operate as a waiver if the disclosing party follows the procedure specified in" the Arkansas analogue to Fed. R. Civ. P. 26(b)(5) and, if challenged, "the circuit court finds in accordance with [the Arkansas analogue to Fed. R. Civ. P. 26(b)(5)(D)] that there was no waiver." Subsection (f) of the Arkansas rule provides that a disclosure "to a governmental office or agency in the exercise of its regulatory, investigative, or enforcement authority does not operate as a waiver of the privilege or protection in favor of non-governmental persons or entities.");

FLA. R. CIV. P. Rule 1.285(a) and (c) (2011) (Under subsection (a) "[a]ny party, person, or entity, after inadvertent disclosure of any materials pursuant to these rules, may thereafter assert any privilege recognized by law as to those materials. This right exists without regard to whether the disclosure was made pursuant to formal demand or informal request." Subsection (c) of the Florida rule allows any party receiving notice of inadvertent disclosure to challenge the assertion of privilege on the grounds that, *inter alia*, "[t]he circumstances surrounding the production or disclosure of the materials warrant a finding that the disclosing party, person, or entity has waived its assertion that the material is protected by a privilege. . . . ");

MASS. GUIDE EVID. § 523(c)(2) (2012) ("disclosure does not waive the privilege if . . . (2) there is an unintentional disclosure of a privileged communication and reasonable precautions were taken to prevent the disclosure.");

N.H. R. EVID. 511 ("A claim of privilege is not defeated by . . . a disclosure that was made inadvertently during the course of discovery.");

TEX. R. CIV. PROC. § 193.3(d) (West 2012) ("Privilege Not Waived by Production. A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these Rules of Evidence if—within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made—the producing party amends the response, identifying the material or information produced and stating the privilege asserted.").

During the initial stages of the rulemaking process, proposed Federal Rule 502 contained a provision addressing non-waiver for the production of privileged or protected materials to a governmental entity in connection with its investigation, regardless of whether the production was inadvertent. That provision proved to be controversial and was not included in the final version of Rule 502 that was submitted to Congress. Nevertheless, the Arkansas rule extends non-waiver protection to disclosures made to government entities, regardless of whether the disclosure was inadvertent.[156] In that respect, Arkansas' rule is broader than Federal Rule 502. The Oklahoma rule similarly provides that a production to a governmental entity will not result in a waiver to non-governmental entities or persons but further provides for the possible waiver of undisclosed communications on the same subject matter.[157]

States that have not adopted versions of Federal Rule 502 may nevertheless have rules similar to Federal Rule of Civil Procedure 26 or otherwise permit parties to include non-waiver or clawback provisions in protective orders. Accordingly, clawback orders may still be a valuable tool in states that have not

156. ARK. R. EVID. 502(f) (a disclosure "to a governmental office or agency in the exercise of its regulatory, investigative, or enforcement authority does not operate as a waiver of the privilege or protection in favor of non-governmental persons or entities.").

157. OKLA. STAT. tit. 12, § 2502(F) (2012) (Under subsection F, the disclosure of attorney-client privileged or work-product information "to a governmental office, agency or political subdivision in the exercise of its regulatory, investigative, or enforcement authority does not operate as a waiver . . . in favor of nongovernmental persons or entities." Further, "[d]isclosure of such information does not waive the privilege or protection of undisclosed communications on the same subject matter unless: 1. The waiver is intentional; 2. The disclosed and undisclosed communications or information concern the same subject matter; and 3. Due to principles of fairness, the disclosed and undisclosed communications or information should be considered together.").

adopted a Rule 502 analogue, even if those orders do not provide all of the protections afforded by a Federal Rule 502(d) order.

THE SEDONA CANADA PRINCIPLES ADDRESSING ELECTRONIC DISCOVERY, SECOND EDITION*

A Project of The Sedona Conference Working Group on Sedona Canada (WG7)

Author: The Sedona Conference

Editor-in-Chief: Susan Nickle

Managing Editor: Jim W. Ko

Contributing Editors:

Anne Glover
Crystal O'Donnell
David N. Sharpe

Contributors:

Hon. Colin L. Campbell Q.C.
Roger B. Campbell
Robert J.C. Deane
Karen B. Groulx
David Outerbridge
James T. Swanson
Susan Wortzman

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 7. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Sustaining and 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.

*****

PREFACE

Welcome to the Second Edition of *The Sedona Canada Principles Addressing Electronic Discovery*, a project of The Sedona Conference Working Group on E-Discovery Issues in Canada ("Sedona Canada" or "WG7"). This is one of a series of working group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute that exists to allow leading jurists, lawyers, experts, academics, and others, at the cutting edge of issues in the areas of antitrust law, complex litigation, and intellectual property rights, in conferences and mini-think tanks called Working Groups, to engage in true dialogue, not debate, in an effort to move the law forward in a reasoned and just way.

WG7 was formed in 2006 with the mission "to create forward-looking principles and best practice recommendations for lawyers, courts, businesses, and others who regularly confront e-discovery issues in Canada." The first edition of these *Sedona Canada Principles* was released in early 2008 (in both English and French) and was immediately recognized by federal and provincial courts as an authoritative source of guidance for Canadian practitioners. It was explicitly referenced in the Ontario *Rules of Civil Procedure* and practice directives that went into effect in January 2010.

The Second Edition represents the collective efforts of many individual contributors. The drafting process for the Second Edition was initiated in October 2012 by a large group of Canadian practitioners, and was both developed and brought to consensus by the drafting team over an extensive process including countless conference calls. The draft was also the focus of dialogue at The Sedona Conference WG7 Meeting in Toronto, in August 2014. The Public Comment Version of the Second Edition was published in February 2015, and the editors have reviewed the comments received through the public comment process.

On behalf of The Sedona Conference, I thank all drafting team members for their time and attention during the drafting and editing process, including Susan Nickle, Anne Glover, Crystal O'Donnell, Da-

vid N. Sharpe, Hon. Colin L. Campbell Q.C., Roger B. Campbell, Robert J.C. Deane, Karen B. Groulx, David Outerbridge, James Swanson, and Susan Wortzman. I also thank volunteer Nadia Sayed. I further thank Luc Bélanger, Justice David M. Brown, Ronald Davis, Martin Felsky, Kelly Friedman, Heidi Lazar-Meyn, Kathryn Manning, Lynne Vicars, and, in particular, William E. Hoffman, and everyone else involved in this extensive project, for their assistance and contributions to this effort.

I also thank the original WG7 Editorial and Steering Committee members who brought to publication the First Edition of the *Sedona Canada Principles* in January 2008, including Hon. Colon L. Campbell Q.C., Robert J.C. Deane, Peg Duncan, David Gray, Dominic Jaar, Justice J.E. Scanlan, Glenn Smith, and Susan Wortzman, as well as the Technology Advisor, John H. Jessen.

Working Group Series output is first published in draft form and widely distributed for review, critique, and comment, including in-depth analysis at Sedona-sponsored conferences. Following this period of peer review, the draft publication is reviewed and revised by the Working Group and members of the Working Group Steering Committee, taking into consideration what is learned during the public comment period. Please send comments to info@sedonaconference.org, or fax them to 602-258-2499. 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 W. Weinlein
Executive Director
The Sedona Conference
November 2015

FOREWORD

The *Sedona Canada Principles* (the "*Principles*") were originally published in January 2008.[1] Since that time, the Canadian electronic discovery ("e-discovery") environment has matured significantly.

In 2008, the writers of the *Principles* necessarily advocated for cultural change in the legal profession to address the impact of e-discovery on the litigation process. Over the past seven years, we have seen notable changes: rules have been amended to accommodate e-discovery, a robust body of Canadian e-discovery case law has developed, the test for relevance has been narrowed in some jurisdictions to reflect a new, high volume, "e-reality," and across the country, the concept of proportionality has become firmly entrenched in the new discovery vernacular.

Now in 2015, further changes in legal culture are still required. Central to this shift is early and meaningful cooperation between counsel, as well as the acknowledgement that basic e-discovery principles apply to cases of every size and subject matter. The amended *Principles* presented below reflect these important ideals, as well as other important developments in Canadian law. In an effort to make the *Principles* as accessible to

1. The *Sedona Canada Principles* are the work of The Sedona Canada Working Group, which is Working Group 7 (WG7 or the "Working Group") of the Sedona Conference. The Sedona Conference was formed in 1997 in Sedona, Arizona, and is currently based in Phoenix, Arizona. The Sedona Conference, its *Principles* and its numerous publications and initiatives have been instrumental throughout the world in the development and promulgation of standards and best practices in the use of electronic information in litigation and other forms of investigation.

as wide an audience as possible, the Working Group has distilled the following updated *Principles* and associated Commentary into the following core statements:

The *Sedona Canada Principles* are focused on the discovery process. Issues related to the management of electronic records and other electronically stored information (ESI) are increasingly important from a business and legal point of view. Under the various Evidence Acts in Canada, the admissibility of electronic records as evidence often requires having regard to the integrity of the operation and functions of information systems and of the records they house and manage. There are current and emerging standards related to electronic records management systems and policies which are helpful and valuable in the general management of the life cycle of ESI, including authenticating and proving electronic records as evidence. However, records and information governance policies and practices, the integrity and operation of information systems and software, and the substantive law related to the admissibility of electronic records are in large part all beyond the scope of these *Principles*. Instead, the *Principles* focus on best practices related to the discovery process in the circumstances in which parties to litigation find themselves, and not the ways parties could have managed their systems and records before litigation arises, in order to improve their ability to deal with litigation and discovery obligations.

The *Sedona Canada Principles* are at the centre of the discovery process in Canada. The *Principles* provide an outline of best practices with respect to the management of ESI that are or may be relevant to every case. First published in January 2008, they have been the basis of formal rule amendments in at least two Provinces. They provide for the cooperative management of the discovery phase, which, due to the proliferation of

ESI, has an increasingly central role in the conduct of a civil action.

The *Sedona Canada Principles* provide practical guidelines. The *Principles* are flexible enough that practitioners and judges can use them when dealing with ESI in different case types; when assessing the effects of different sources, formats and volumes of ESI; and when determining the relative costs and benefits of adopting different forms of documentary production.

ESI is ubiquitous. Lawyers at all levels should be comfortable with managing ESI. Electronic communication now reaches into almost all aspects of our lives. The vast majority of information produced in the world today is electronic and will never be printed. ESI is present in virtually every case, meaning that all lawyers must have a basic knowledge of how to manage it.

Parties have an obligation to preserve potentially relevant ESI in the context of litigation, regulatory matters and audits. The duty to preserve potentially relevant information, when triggered, extends to ESI.

ESI behaves completely differently than paper documents. There are thousands of electronic file formats. Computer systems now replicate and distribute ESI without active human involvement. Duplicates and near-duplicates proliferate on the user's computer and elsewhere. As systems change, ESI can become less accessible and therefore harder to preserve and collect. The methods of searching, retrieving, converting and producing ESI are completely different from those relating to paper and are constantly evolving.

1. ESI can be mishandled in ways that are unknown in the world of paper. Electronic information can be overwritten, hidden, altered and even completely deleted

through inadvertent, incompetent, negligent or illicit handling without these effects being known until later. It is therefore important to identify potentially relevant ESI and to preserve it as soon as possible in a manner that protects the integrity of the information. Understanding the basics of how ESI should be handled will help to minimize these risks while providing counsel with the knowledge to hold other parties to account. Counsel have a professional responsibility to advise clients of appropriate practices and the risks of not employing them.

2. Preservation of ESI is crucial. The special characteristics of ESI and the constant evolution of technology mean that it is critical, when meeting discovery obligations, to take prompt and active measures to preserve potentially relevant ESI in a defensible manner that protects the integrity of the information.
3. Large organizations and individual parties can equally threaten the loss of relevant ESI. Each entity or person may handle ESI differently and each can lose or alter potentially relevant ESI unless steps are taken to preserve it. Corporations may purge some ESI every day, but they have backup systems. Individuals may only purge ESI less frequently; but, when they do, it may likely be lost forever.
4. ESI raises special challenges with respect to authentication. Only proper methods for preserving, collecting, processing, reviewing and producing ESI will defensibly protect data integrity and maintain chain of custody. Copying and moving ESI without using proper methods will almost always change some of its metadata.

For all the above reasons, it is important for counsel to learn about efficient and defensible methods for handling ESI—

whether with respect to initial preservation, subsequent collection, processing, review or production.

ESI can be relevant in even the smallest cases. ESI is not confined to large, complex or high-profile cases. It is relevant in almost every civil litigation matter, including personal injury and family law litigation. It can be important even in very small or simple cases—for example, where the case turns on the information contained on a cell phone or in e-mail.

Small cases may give rise to their own procedures and expectations. Rules and practices that make sense for large entities may not make sense for individual litigants. A large corporation would be expected to have a document retention policy; an individual would not. To expect a large multinational corporation to put a hold on all its physical computer devices would be disproportionate in almost all cases; to expect an individual plaintiff to preserve his or her cell phone and all its social media content may not be.

All e-discovery should be conducted with a view to what is proportionate in the circumstances. Proportionality is the barometer applied to the question of how much time, effort and expense a party should reasonably have to expend with respect to ESI in light of all relevant factors. Every jurisdiction that has adopted ESI-related rules of procedure that impose affirmative obligations has adopted a proportionality principle. All ESI is potentially discoverable and parties have a duty to preserve, search and then produce what meets the relevant test for disclosure. But no party is required to preserve, search and produce all (or particularly problematic sets of) ESI where to do so would impose costs and burdens disproportionate to the value of the case or the probative value of the evidence in question, taking into account the availability of the same information from other sources and other factors. (*See* Principle 2).

Core principles and best practices apply everywhere, regardless of the size of the case. Early discussions between opposing counsel and cooperation regarding the management of all aspects of ESI are important in all cases. Even if the scope, volume and methods differ, the key elements of cooperation and the development of a discovery plan remain the same: what is at issue, who are the key individuals, what are the sources of information, what should be preserved, in what order should information be collected and processed, in what formats will the parties review and produce, and so on. Of these types of issues, search methods can be the most important. In smaller cases there may be no access to sophisticated tools. In such cases, the proper handling of ESI may be of *greater* immediate concern than it is in larger cases.

Parties should confer as early as possible to work out reasonable ways of meeting their discovery obligations. The *Principles* call for meaningful and ongoing cooperation between parties throughout discovery. Parties are called upon: to confer as soon as practicable and on an ongoing basis to facilitate cooperative resolution of all discovery issues (*see* Principle 4); to agree as early as possible on production formats and the contents of various listings (*see* Principle 8); and to agree or seek direction on how to protect privileges, privacy, trade secrets and other confidential information (*see* Principle 9).

Ongoing cooperation and conferring between parties can minimize burdens, mitigate risks and lead to the speedier resolution of disputes. By engaging in early and ongoing discussions regarding the identification, preservation, collection, processing, review and production phases, and by sharing, as appropriate, information about relevant subsets of ESI (data preserved, data collected, search results, etc.), parties can gain tremendous efficiencies by reducing, at the outset, and thereafter at each subsequent stage, the volume of information they

have to collect, process, search, review and produce. This approach can replace the traditional practice whereby each party prepares a listing of relevant documents, and in some cases may even proceed to produce the entirety of what it believes to be relevant documents, without consultation with the other parties.

Early, ongoing and meaningful cooperation between the parties can minimize costs, reduce delay, avoid the kinds of mistakes and confusion that arise from failures to communicate and avoid costly and time-consuming motions to deal with otherwise manageable discovery disputes.

Lawyers should accept document production in electronic form and understand the e-discovery components in each of their cases. The most important evidence in a case might be electronic; indeed, when the vast majority of communications are never printed, it almost certainly will be.

Managing information electronically allows for highly efficient organization, searching, review, analysis and production—far faster than what is possible with paper or scanned documents. It is faster, more efficient and cheaper to exchange electronic information and documents in electronic form than printing the electronic documents to paper and then reconverting the paper printouts to electronic form. This is true even in small cases. Modern tools allow for efficient collaborative discovery whereby all parties have access to relevant information, at lower cost per party, while enjoying all the benefits of electronic management and while maintaining all necessary partitions between datasets. Further, lawyers who avoid best practices for dealing with ESI may expose themselves to professional liability.

This Second Edition of the *Principles* continues to aim to assist in the resolution of what can be difficult and complex discovery disputes and, thus, to assist in reaching effective, timely, cost-efficient and defensible solutions to problems of document disclosure.

*****

The Sedona Canada Working Group has revised the original 2008 version of the *Principles* in a number of key areas. In several cases, the language of the Principles themselves has been modified. The Commentary under each of the Principles has been comprehensively updated, along with applicable case law where appropriate. The most significant amendments are summarized below as follows:

Principle 1

The Commentary for Principle 1 has been amended to add a reference to social media.

Principle 2

Principle 2 has been modified to create a five-part test for proportionality.

A new opening Commentary paragraph emphasizes the importance of the proportionality principle. A section dealing with the applicability of the proportionality principle to procedure and procedural motions has also been included.

The Commentary also now includes a reference to the E-Discovery Implementation Committee (EIC) of the Ontario Bar Association and its development of model documents.

Principle 3

The Commentary has been amended to emphasize the value and importance of information governance as a way of preparing for litigation and, in particular, for e-discovery.

Principle 4

Principle 4 has been amended to emphasize the concept of "cooperation" (versus "meet-and-confer") in developing a joint discovery plan.

There are important new sections and an overall shift in emphasis throughout the Commentary for this Principle. First, there is new emphasis on the importance and value of discovery planning. This section proposes that the term "meet-and-confer" be replaced with "discovery planning," "consultation" or any similar term that does not suggest that in-person meetings are required. Emphasis is placed on the good-faith sharing of information aimed at reaching agreement on a discovery plan.

Principle 5

The Commentary discussion in this Principle on data being "not reasonably accessible" and therefore being excluded from the set of ESI that needs to be dealt with has been removed. The fact that information has been deleted does not, on its own, mean that the data is not accessible or that a party has no obligation to obtain it.

Principle 6

Principle 6 now makes clear that "[a] party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual ESI that has been deleted in the ordinary course of business or within the framework of a reasonable information governance structure." While a party may not simply delete information to thwart discovery obligations, defensible information governance principles will be considered.

The Commentary has been updated to include new Canadian case law supporting the proposition that the deletion of

documents is permissible in the normal course of business or pursuant to a reasonable document retention policy.

Principle 7

Principle 7 has been amended to clarify that this Principle applies not only to electronic records, but to records in any format.

In the Commentary, given the advancements in technology and the pace at which technology is developing and changing, references to any specific techniques or tools have been removed. Further, the discussion on tools that can be used by a party to satisfy its document discovery obligations has been expanded.

Lastly, a section on the importance of sampling and validating any method adopted to fulfill a party's discovery obligations has been added.

Principle 8

Principle 8 has been amended to remove the reference to "lists of documents" given the fact that many parties no longer exchange lists of documents. The proposed new Principle is simplified to read as follows: "Parties should agree as early as possible in the litigation process on the format, content and organization of information to be exchanged between the parties."

Additional information has been included in the section on "Agreeing on a Format for Production" given the change in the practice over the years to productions being made in native format where possible.

The section on "Document Lists – Format and Organization" has been renamed "Affidavits and the Format and Organization of Record Lists." This section has also been expanded to discuss the fact that the manual coding of documents is often no

longer required given the movement to producing native files (and collecting native files from clients).[2] A comment has also been included on the issues that have arisen in this new electronic age with the wording in certain Affidavits of Documents required by the applicable rules of court in certain provinces.

Principle 9

In the Commentary, there has been an expansion of the discussion on privilege and inadvertent disclosure. Further, a new section regarding the information on coded documents in a document list has been added.

A number of new sections regarding privacy in different contexts have been added, including privacy and social media, employee privacy on employer-issued devices and criminal investigations.

Lastly, a brief section on data security and chain-of-custody issues has been added.

Principle 10

The Principle has been changed to reflect different geographic jurisdictions and forums.

The Commentary has been substantially expanded to address areas of difference in cross-border litigation that counsel should consider, and it includes a brief discussion of issues that arise in cross-forum litigation, such as criminal and regulatory proceedings.

A section on the use of electronic evidence in arbitrations has also been added.

---

2. For a discussion of coding, see *infra*, Introduction, section F.8 (Advanced Technology Can Help to Organize, Search and Make Sense of ESI) and note 27.

Principle 11

The Principle has been amended to confirm that sanctions may be considered for a party's failure to meet any obligation with respect to any phase of discovery. A previous reference to a defaulting party avoiding sanctions if it demonstrates the failure was not intentional or reckless has been removed.

The Commentary describing the American experience has been removed and replaced with a discussion of the growing body of Canadian case law regarding spoliation and sanctions for nondisclosure.

The previous Commentary section on reasonable records management has been renamed and expanded to more broadly discuss information governance principles and rebutting the presumption of spoliation.

Principle 12

The Principle has been amended to confirm that the party producing ESI will generally bear its own costs of all phases of discovery.

The case law in the Commentary has been updated and a direct reference to proper information governance as a significant factor in reducing costs associated with e-discovery has been included.

Susan Nickle
Editor-in-Chief

Anne Glover
Crystal O'Donnell
David N. Sharpe
Contributing Editors

Hon. Colin L. Campbell Q.C.
James Swanson
Co-Chairs, Working Group 7 Steering Committee

TABLE OF CONTENTS

THE SEDONA CANADA PRINCIPLES ADDRESSING ELECTRONIC DISCOVERY—AT A GLANCE

Principle 1. Electronically stored information is discoverable.

Principle 2. In any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account: (i) the nature and scope of the litigation; (ii) the importance and complexity of the issues and interests at stake and the amounts in controversy; (iii) the relevance of the available electronically stored information; (iv) the importance of the electronically stored information to the Court's adjudication in a given case; and (v) the costs, burden and delay that the discovery of the electronically stored information may impose on the parties.

Principle 3. As soon as litigation is reasonably anticipated, the parties must consider their obligation to take reasonable and good-faith steps to preserve potentially relevant electronically stored information.

Principle 4. Counsel and parties should cooperate in developing a joint discovery plan to address all aspects of discovery and should continue to cooperate throughout the discovery process, including the identification, preservation, collection, processing, review and production of electronically stored information.

Principle 5. The parties should be prepared to produce relevant electronically stored information that is

reasonably accessible in terms of cost and burden.

Principle 6. A party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual electronically stored information that has been deleted in the ordinary course of business or within the framework of a reasonable information governance structure.

Principle 7. A party may use electronic tools and processes to satisfy its documentary discovery obligations.

Principle 8. The parties should agree as early as possible in the litigation process on the format, content and organization of information to be exchanged.

Principle 9. During the discovery process, the parties should agree to or seek judicial direction as necessary on measures to protect privileges, privacy, trade secrets and other confidential information relating to the production of electronically stored information.

Principle 10. During the discovery process, the parties should anticipate and respect the rules of the forum or jurisdiction in which the litigation takes place, while appreciating the impact any decisions may have in related proceedings in other forums or jurisdictions.

Principle 11. Sanctions should be considered by the Court where a party will be materially prejudiced by

another party's failure to meet its discovery obligations with respect to electronically stored information.

Principle 12. The reasonable costs of all phases of discovery of electronically stored information should generally be borne by the party producing it. In limited circumstances, it may be appropriate for the parties to arrive at a different allocation of costs on an interim basis, by either agreement or court order.

I. INTRODUCTION TO THE SECOND EDITION: DISCOVERY IN TODAY'S WORLD OF ELECTRONICALLY STORED INFORMATION

The rapid transformation of information and technology continues to present challenges to the legal profession. In the first decade of this century, the courts and the legal profession began to meet this challenge in earnest. A few milestones of note:

1. Following the release in the United States of the first public comment draft of *The Sedona Principles* in 2003, a set of changes in late 2006 to the U.S. Federal Rules of Civil Procedure relating to electronically stored information (ESI)[3] and several well-publicized U.S. federal court decisions, the Sedona Canada Working Group 7 (WG7 or the "Working Group") was formed in 2006.
2. The first edition of these *Sedona Canada Principles Addressing Electronic Discovery* (the "*Sedona Canada Principles*" or the "*Principles*") was released in January 2008.[4]
3. Nova Scotia became the first Canadian province to amend its *Rules of Civil Procedure* to address electronic discovery by the insertion of a new Rule 16[5] in 2008; these amendments were based on the *Principles*.[6]

---

3. Federal Rules of Civil Procedure: Title V. Disclosure and Discovery: Rule 26 at "Committee Notes on Rules - 2006 Amendment," online: Legal Information Institute <http://www.law.cornell.edu/rules/frcp/rule_26>.

4. The Sedona Conference, *The Sedona Canada Principles Addressing Electronic Discovery* (January 2008), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/71>.

5. *Nova Scotia Civil Procedure Rules*, Royal Gazette Nov 19, 2008, at r 16.

6. Nova Scotia Barristers' Society, Table of Concordance: (from CPR 2008 to CPR 1972) at 4, online: Nova Scotia Barristers' Society <http://nslaw.nsbs.org/nslaw/concordance.do>.

4. On January 1, 2010, Ontario amended its *Rules of Civil Procedure* to include two new rules: Rule 29.1 (Discovery Plan) and Rule 29.2. (Proportionality in Discovery).[7] Rule 29.1 imposes an affirmative obligation on the parties to agree to a discovery plan and requires that "[i]n preparing the discovery plan, the parties shall consult and have regard to the document titled *The Sedona Canada Principles Addressing Electronic Discovery* developed by and available from The Sedona Conference®."
5. On September 5, 2014, the Ontario Superior Court of Justice released its decision in *Palmerston Grain v. Royal Bank of Canada*.[8] In a strongly worded decision, the Court held that parties are required to comply with the *Sedona Canada Principles* and failing to do so is a breach of the *Rules of Civil Procedure*, effectively making the Principles mandatory for Ontario cases dealing with electronic information.

As the *Sedona Canada Principles* have come to play a prominent role in Canadian civil procedure, it is important to remember that they are not a set of national rules; they are a set of guidelines and best practices that can assist parties and judges in deciding how best to manage ESI during discovery, in a range of circumstances.

A. What is Electronic Discovery?

Electronic discovery ("e-discovery") refers to the discovery of ESI. Information is "electronic" if it exists in a medium that can be, or needs to be, read using computers or other digital

7. The enacting regulation affecting this amendment was O Reg. 438/08, ss. 25–26.

8. [2014] O.J. No. 4132.

devices. Electronic media include magnetic disks, optical disks, magnetic tape and solid state drives. Electronic information can come in the form of e-mails, word-processing files, spreadsheets, web pages, databases, video recordings, sound recordings and thousands of other formats.

Electronic discovery differs from traditional paper discovery in a number of ways, which are discussed in more detail below. One fundamental difference is that electronic data requires the use of electronic devices and software and, therefore, the direct or indirect support and involvement of software developers, computer technicians and other specialists.

B. To Whom are these *Principles* Addressed?

These *Principles* and their associated Commentary are addressed to anyone who works with electronic evidence for legal or other investigative purposes. At a minimum, all such people need to understand certain basic technical facts regarding how ESI is created, stored, manipulated and used for evidentiary purposes.[9] They also must be familiar with the guidance, recommendations and best practices provided in these *Principles*. It is now impossible to understand the scope of, and to perform one's obligations concerning, the handling of evidence without extending those obligations and understanding to electronic information.

The Working Group continues to encourage a broader understanding and acceptance of these *Principles* in the Canadian legal and investigative community. It is not merely litiga-

9. For a convenient reference to technical terms relevant to electronic discovery, see The Sedona Conference, *Glossary For E-Discovery and Digital Information Management* (April 2014), online: The Sedona Conference <https://thesedonaconference.org/download-pub/3757>.

tors involved in large cases who should develop their understanding in this area. All persons involved in the legal community will benefit from greater familiarity with and adoption of these *Principles*.

C. What Rules Govern Electronic Document Production in Canada?

In Canada, the rules for documentary production are governed by each province's rules of civil procedure or rules of court. Each court in Canada, whether provincially or federally instituted, has a rule requiring the production of documents relevant to matters in issue in the action, along with a definition of "document" that includes electronic records or data. Each province, territory and federal jurisdiction has a well-developed set of rules regulating the production, inspection, and listing of

documents that are relevant to the proceedings at hand.[10] [11] While the approach varies from jurisdiction to jurisdiction, the Rules of most Provinces and Territories are similar.

D. Why Do Courts and Litigants Need Standards Tailored to Electronic Discovery?

Prior to the first publication of these *Principles* in 2008 it could be said that e-discovery was uncommon. Most counsel were unfamiliar with ESI and its special requirements. In most jurisdictions, neither the courts nor other litigating parties had

---

10. The general rules requiring documentary production are found at the following sections in the relevant province's rules: Ontario *Rules of Civil Procedure,* RRO 1990, O Reg 194, r 30.02 [*Ontario Rules*]; Alberta *Rules of Court*, Alta Reg 124/2010, Part 5 [*Alberta Rules*]; British Columbia *Supreme Court Civil Rules*, BC Reg 168/2009, r 7-1 [*BC Rules*]; Manitoba *Court of Queen's Bench Rules*, Man Reg 553/88, r 30.02 [*Manitoba Rules*]; New Brunswick *Rules of Court*, NB Reg 82-73, r 31.02 [*NB Rules]*; Newfoundland and Labrador *Rules of the Supreme Court*, SNL 1986 c 42, Sch. D, r 32.01 and 32.04; Northwest Territories *Rules of the Supreme Court*, NWT Reg 010-96, r 219, 225 and 229 [*NWT Rules*]; Nunavut *Rules of the Supreme Court*, NWT Reg 010-96 (Nu) r 219, 225 and 229 [*Nu Rules*]; *Nova Scotia Rules*, *supra* note 5; Prince Edward Island, *Supreme Court Rules of Civil Procedure* [*PEI Rules*] , r 30.02; Saskatchewan *The Queen's Bench Rules*, S Gaz, December 27, 2013, 2684, Part 5 [*Saskatchewan Rules*]; Quebec *Code of Civil Procedure*, CQLR c C-25, s 401-403 [*Quebec Code*]; Yukon *Rules of Court*, YOIC 2009/65, r 25 [*Yukon Rules*]; *Tax Court of Canada Rules (General Procedure)*, SOR/90-688a, r 78 and 80 [*Tax Court Rules*]; and *Federal Courts Rules* (SOR/98-106), r 222 and 223 [*Federal Court Rules*].

11. Definitions of "document" are found at the following sections in the respective province's rules: *Ontario Rules*, *supra* note 10, r 30.01; *BC Rules*, *supra* note 10, r 1; *Manitoba Rules, supra* note 10, r. 30.01; NB Rules, *supra* note 10, r 31.01; *NWT Rules*, *supra* note 10, r 218; *Nu Rules*, *supra* note 10, r 218; *Yukon Rules*, *supra* note 10, r 1 (8); *PEI Rules*, *supra* note 10, r 30.01; *Saskatchewan Rules,* Part 17; Quebec, *An Act to establish a legal framework for information technology*, RSQ c C-1.1 [*Quebec Information Technology Act*], s 3; *Tax Court Rules*, *supra* note 10, r 78; *Federal Courts Rules*, *supra* note 10, r 222(1).

demanded rigorous adherence to best practices in the handling of electronic evidence. At the same time, some litigants found the discovery of ESI to be costly and burdensome. A precursor to these *Principles* was the document titled *Guidelines for the Discovery of Electronic Documents in Ontario* (the "Ontario E-Discovery Guidelines").[12] The introduction to that document noted that the "rules and the case law to date provide little clear guidance to parties and their counsel on how to fulfill that [e-discovery] requirement." This situation was not limited to Canada.[13]

In brief, attempts to apply the then existing discovery principles from the former paper-based age to the world of electronic information proved to be problematic. The new issues that have arisen in the world of electronic information have required a new approach. This demand was met by the publication of these *Principles* in 2008, which courts across Canada have since adopted as a standard.[14]

---

12. Discovery Task Force, *The Supplemental Discovery Task Force Report* (October 2005), online: Ontario Bar Association <http://www.oba.org/en/pdf_newsletter/DTFFinalReport.pdf>. The Supplemental Report includes Guidelines for the Discovery of Electronic Documents in Ontario, prepared by the e-discovery sub-committee.

13. See *Williams v. Sprint/United Management Co.,* 230 FRD 640 at 651, 2005 US Dist. LEXIS 21966 (WL): "[T]he Court finds insufficient guidance in either the federal rules or case law, and thus relies primarily on the Sedona Principles and comments for guidance on the emerging standards of electronic document production. . . ."

14. See e.g. Newfoundland and Labrador: *GRI Simulations Inc. v. Oceaneering International Inc.*, 2010 NLTD 85 (CanLII); Nova Scotia: *Velsoft Training Materials Inc. v. Global Courseware Inc*., 2012 NSSC 295 (CanLII), [*Velsoft*]; British Columbia: *Liquor Barn Income Fund v. Mather*, 2011 BCSC 618 (CanLII); Alberta: *Innovative Health Group Inc. v. Calgary Health Region*, 2008 ABCA 219 (CanLII); New Brunswick: *Saint John (City) Conseil des fiduciaires du régime de retraite des employés c Ferguson*, 2009 NBBR 74 (CanLII); Manitoba:

E. The Overarching Principles: Proportionality and Cooperation between the Parties

To anyone approaching ESI for the first time—perhaps someone more familiar with traditional information sources and methods of disclosure—the world of ESI will present two immediate and significant challenges: volume and complexity. To address these challenges, there are two principles at the heart of the Working Group's e-discovery best practices as articulated in these *Principles*: proportionality (*see* Principle 2) and cooperation between parties (*see* Principle 4).

Proportionality. In order to cope with the problems associated with the ever growing volume and complexity of electronic documentation, most jurisdictions have incorporated a principle of proportionality into their rules of court. Proportionality relates to the question of how much time and effort a party should reasonably have to expend, in light of all relevant factors, to perform e-discovery. Every jurisdiction that has adopted ESI-related rules of procedure that impose affirmative obligations has adopted a proportionality principle. While all ESI is discoverable and parties have a duty to preserve, search and then produce what meets the relevant test for disclosure, no party should be expected to preserve, search and produce all, or specific problematic sets of, ESI where to do so would impose costs and burdens disproportionate to the value of the case or the probative value of the evidence in question, taking into account the availability of the same information from other sources.

Commonwealth Marketing Group Ltd. et al v. The Manitoba Securities Commission et al., 2008 MBQB 319 (CanLII).

For example, Ontario Rule 29.1.03 requires the parties to agree to a discovery plan that takes into account "[the] relevance, costs and the importance and complexity of the issues in the particular action."[15] The discovery plan shall also include "any other information intended to result in the expeditious and cost-effective completion of the discovery process *in a manner that is proportionate to the importance and complexity of the action*."[16] Ontario Rule 29.1 also requires that, "[i]n preparing the discovery plan, the parties *shall* consult and have regard to the document titled 'The Sedona Canada Principles Addressing Electronic Discovery' developed by and available from The Sedona Conference."[17]

Cooperation between the Parties. While the original *Principles* primarily discussed the "meet-and-confer" process, the Canadian experience has developed more significantly around the principle of ongoing cooperation and the development of a discovery plan. The idea of cooperation between counsel and parties extends well beyond the confines of a meeting, or series of meetings, to the transparent sharing of information in an effort to keep discovery costs proportionate and timelines reasonable. At The Sedona Conference Working Group 7 August 2014 Meeting in Toronto, there was a universal consensus that the "meet and confer" language in these *Principles* be replaced with "cooperation" and "collaboration."

The Ontario Rules are illustrative of this principle of cooperation. The same provisions that emphasize proportionality also require consultation and agreement between the parties at

15. *Ontario Rules*, *supra* note 10, r 29.1.03(3)(a).

16. *Ontario Rules*, *supra* note 10, r 29.1.03(3)(e) [emphasis added].

17. *Ontario Rules*, *supra* note 10, r 29.1.03(4) [emphasis added].

the outset of the litigation.[18] The purpose of such consultation and cooperation in jointly developing a discovery plan is to minimize the scope, complexity and attendant difficulties of e-discovery for the parties and the entire judicial system. The Ontario Rules relating to e-discovery illustrate the importance of proportionality and of ongoing consultation between the parties in the e-discovery process.

F. How are Electronic Documents Different from Paper Documents?

Exploring and understanding the differences between paper and electronic documents can reveal important factors that determine how ESI should be handled. It can allow courts and parties to break from past practice where appropriate, while still achieving the fundamental objective of securing the "just, most expeditious and least expensive" resolution of each dispute.[19]

1. Large Volume and Ease of Duplication

ESI is created at much greater rates than paper documents. As such, there are vastly more electronic documents than paper documents.

Electronic documents are more easily duplicated than paper documents. For example, e-mail users frequently send the same e-mail to many recipients. Recipients often forward messages. E-mail systems automatically create copies as messages are sent. Other software applications periodically and automatically make copies of data.

---

18. See e.g. *Ontario Rules*, *supra* note 10, r 29.1.03(2).

19. See e.g. *Tax Rules*, *supra* note 10, s 4(1).

2. Persistence—ESI is Hard to Destroy

Electronic documents are more difficult to dispose of than paper documents. A simple command to "delete" an electronic document still generally leaves the file on a storage device until it is overwritten. Until it is overwritten, the data still exists and may be recovered using forensic methods. If the original electronic storage device is handed over by the producing party to the receiving party, the receiving party may find and be permitted to use that "deleted" data. *In Prism Hospital Software Inc. v. The Hospital Records Institute,*[20] the defendants produced magnetic media on which the plaintiff was able to locate a series of files that, although "deleted," continued to exist. The persistence of ESI means that it accumulates without a custodian knowing that it is still available.

It may be easier and less expensive to recover destroyed electronic documents than destroyed paper documents. At times, computer forensic techniques may allow parties to recover or reconstruct deleted documents, even, in some cases, documents that appear to have been permanently deleted. However, this does not mean that parties responding to document requests will always be required to produce deleted data or data fragments. Generally, the expense and disruption caused by such techniques cannot be justified. Here, an analogy to paper is useful. A producing party is not required to produce papers that it threw away a year ago. In *Rowe Entm't Inc. v. The William Morris Agency Inc.*,[21] (a U.S. case) the Court held, "just as a party would not be required to sort through its trash to resurrect discarded paper documents, so it should not be obligated

20. *Prism Hospital Software Inc. v. The Hospital Medical Records Institute*, 1991 BCJ No 3732 (1991) 62 BCLR (2d) 393 (WL) (SC).

21. 205 FRD 421 at 431 (WL) (SDNY 2002).

to pay the cost of retrieving deleted e-mails." However, if established that material evidence has been destroyed or lost, requiring parties to bear the costs of recovering destroyed documents may be justified. (*See* Principle 6).

3. Dispersion of ESI

While paper documents will usually be found in a limited number of locations, ESI can reside in numerous locations: desktop hard drives, laptops, network servers, smart phones, tablets, CDs, backup tapes and even floppy disks. These sources will likely contain not only exact digital duplicates; they will also likely contain "near-duplicates" ("near-dupes")—for example, multiple drafts of a report or contract.

4. Dynamic, Changeable Nature of Much ESI

In the world of paper discovery, a document preservation order requiring that a corporate party freeze all of its documents is a manageable burden. Paper documents can be left in their files or copied if they need to be marked up. Personnel can suspend their practice of throwing away old files. With paper, inaction is usually enough to preserve the document.

In contrast, in the electronic context, freezing all electronic information could be catastrophic to a business. It is virtually impossible to "freeze" a company's entire set of ESI without effectively shutting down its entire computer system. Normal business operations involve the constant alteration of certain classes of data. Instead, a well-organized litigation hold is required. There are now reliable methods of implementing and maintaining a hold on potentially relevant information without disrupting the entire enterprise.

Managing the dynamic nature of ESI is an ongoing challenge throughout any e-discovery project. Unlike paper documents, some kinds of electronic information have dynamic features that change over time, often without the user even being aware of the changes taking place. Collaborative tools also allow file contents and metadata to change without any particular user being aware of the change.

Databases present a particular challenge in e-discovery, as most large enterprises run databases that are constantly being updated, whether through direct user input or automatically. For example, a chain store with multiple locations may have the accounting system at each location update a main system with daily sales information, and a warehouse inventory database is typically updated every time shipments of product are received or sent. The information in business operations databases can change by the minute. Deciding which version of the database is the appropriate one to preserve for discovery may be problematic. Pre-preservation interviews with the client's information technology department (IT) and business unit leaders can address many of these issues.

More common file types like word-processing files and spreadsheets also have dynamic features. Date and time metadata can change when a user opens, moves or copies a file. Files that have other files linked with them or embedded within them may change whenever the related file changes. To prevent these changes from occurring, data can be forensically preserved, collected, or both. It can then be processed so as to preserve a particular version, including its metadata, while making the file viewable in a review tool.[22]

22. Modern processing and review tools allow reviewers to view either an image of the file or a native version of the file. However, in both cases,

5. Metadata

Nearly all electronic documents contain information known as metadata, which presents unique issues for the preservation and production of documents in litigation. Metadata is electronic information stored within or linked to an electronic file that is not normally seen by the creator or viewer of the file. Typical and common metadata fields are DateCreated, DateSent, Author and FileLocation (i.e. the location of the document on the user's computer or device, on the server or in the user's mailbox). Metadata is generated by the operating system or the application. Some metadata is not accessible without special tools.

In most cases, metadata will have no material evidentiary value; it does not usually matter when a document was printed or who typed the revisions. There are situations where metadata may be necessary for authenticating a document or establishing facts material to a dispute, such as when a file was accessed in a suit involving theft of trade secrets. These cases, however, are rare in practice.

Metadata can be used to objectively code documents or to properly interpret the meaning of other data.[23] There is, however, a real danger that some metadata recorded by the computer may be inaccurate. This risk is most present with loose electronic files. For example, word-processing documents do not come with metadata accurately identifying many important

---

the original, unaltered metadata will have been extracted, preserved and loaded into the review tool alongside the native file and/or image.

23. E.g. spreadsheet formulas can be used to properly interpret a spreadsheet; "track changes" functionality in Microsoft Word can be used to observe changes made to a document during the drafting process. For a full discussion, see *infra*, Introduction, section F.8 (Advanced Technology Can Help to Organize, Search and Make Sense of ESI) and see *infra* note 27.

attributes or contents of the document (e.g. the signatory of the letter, the sender of a memorandum and the people receiving carbon copies (CC) of the letter). When a new employee uses a word-processing program to create a memorandum by using a memorandum template created by a former employee, the metadata for the new memorandum may incorrectly identify the former employee as the author. To capture the true date, author, recipient, subject line, etc., of a set of documents, the parties cannot rely on such metadata alone—this information often must be derived from the text of the electronic document itself.

E-mail metadata, on the other hand, is often accurate and extremely useful for litigation purposes. Unlike the metadata associated with loose electronic files, e-mail metadata (if collected properly) does accurately identify the e-mail's signatory ("From"), the recipients ("To" and "CC"), and the precise date and time sent ("DateTime").[24] These fields can be extracted and loaded into a review platform for efficient searching and review.

In their discovery planning, counsel should consider whether to exchange metadata. As the profession has come to understand more about what metadata is and how it can be of use, too many practitioners still improperly refuse to consider the possibility of exchanging it as part of a production.[25] It is important to consider both (a) whether the metadata will have any

24. DateTime information in e-mails, however, can present challenges as time zone information, though embedded in the e-mail metadata, is often not correctly processed or displayed. For example, when a collection of documents involves custodians from various time zones, the DateTime information may not be correct depending on the time zone selected when processing the documents.

25. Discussions between the parties to exclude "metadata" from production often focus on ensuring that "hidden data," such as track changes in

dispositive evidentiary value in the proceedings and (b) whether the metadata will be useful for organizing and making sense of a body of ESI. While the metadata itself may not be used at trial, it is certainly useful for the litigation process when deciding what to review and in what order.

In advance of production, parties should agree on which metadata fields they will provide to each other along with the documents. If questions are raised about authenticity or chain of custody, additional metadata can be provided.

6. Structured Data

Today's information technologies have yielded not just electronic files that look and function more or less like letters and memoranda; they include databases and other kinds of "structured data" files. Information in databases is not necessarily organized in a body that can be read in rows starting in the top left and ending in the bottom right. The information is broken up into constituent elements, which are stored in multiple tables, each with records and fields. A sales database, for example, will contain multiple variables (e.g. Organizations, People, Transactions and Invoices), and someone interested in what happened on a particular day can only learn this if multiple rows and columns from all of these tables are pulled together in the proper way.

Parties possessing or demanding access to databases should agree in advance whether to produce native database files or provide, for example, specific reports from the database

---

word documents and formula in spreadsheets, is not produced. When such documents are produced in printed or scanned form, this information is lost to the receiving party. Strictly speaking, however, this kind of information is part of the substantive content of the document and should be preserved and, if appropriate, produced.

routinely produced, based on particular queries that contain specified records and fields.

7. Obsolescence of Hardware and Software

Electronic data, unlike paper data, may be incomprehensible when separated from the software within which it is created and used. Organizations upgrade their systems, sometimes rendering older files unreadable. People who know how to use the old system leave the organization and cannot be located. Software companies stop offering support for earlier versions of their software. In these situations, only reasonably accessible data need be produced, with "reasonably" being interpreted in light of all of the factors that affect proportionality. (*See* Principle 5).

8. Advanced Technology Can Help to Organize, Search and Make Sense of ESI

Working with ESI, while the volumes may far exceed those in the world of paper, is far more efficient than working with paper could ever be. Modern digital technologies, especially search and text classification tools, are extremely powerful, making it possible to organize, search and make sense of vast amounts of information in manageable amounts of time.

When reviewing paper documents before production, lawyers and paralegals commonly review each page of a document to see if the document mentions a person or event relevant to the issues in the pleadings. This practice need not be adopted with electronic files. In fact, it is inadvisable to print out electronic files to do a page-by-page review, as this entails the loss

of valuable information, including metadata, which could otherwise be used to organize, sort, search and make sense of the original "native" file.[26]

It is now possible to search ESI *in situ*, without the need for collection and removal to another location. On-site identification and culling prior to collection can be an effective means of reducing data volumes, with benefits at all later stages. Advance discussions with clients and cooperation with other parties is strongly encouraged. Proper forensic methods should be employed and soliciting the advice or involvement of experienced e-discovery professionals is strongly advised.

De-duplication technology can now eliminate significant volumes of ESI early in the process. With paper (and scanned images of paper), it was almost impossible to know that several reviewers were encountering copies of the same document. With ESI, de-duplication is easily accomplished, obviating the need for redundant review and, even worse, the risk of inconsistent review decisions. Near-duplicate detection allows similar documents to be grouped for more efficient review. E-mail threading organizes e-mails into conversations and identifies e-

26. "Native" is the term used to describe an electronic file in its original state, capable of being opened and viewed in the application that created it, with all the features it first possessed in that format. Thus, a Word document remains in its native format until it is printed or converted, for example to TIF or PDF format. A PDF is almost always a derivative of another (native) format, since most PDFs are generated from a preexisting e-mail, word-processing, spreadsheet, presentation, or other formats. But the fact that a file looks like a native file (if it has a .docx extension, for example) is not in itself proof that this is the original native file: someone can take a richly-formatted Word document, save it to plain-text format and then open it again in Word. It is no longer in its native format, even though it is now (again) in Word. It has lost much of its original content. Only the first Word file, with all its content and formatting, is the true native file.

mails whose content is wholly contained in other e-mails (and which can thus be suppressed from review), making review far more efficient.

It is now possible, using Technology Assisted Review (TAR), for lawyers to perform basic responsiveness coding and even issue-coding on a far greater body of documents than they could have reviewed manually.[27] This is accomplished having

27. The term "coding" is important in both paper-based and electronic discovery. It always refers to the assignment to a document of either (a) a piece of information that captures a property of the document or (b) a designation that reflects a judgment about the document. Coding is not applied to the face of the document; instead, it is stored as values in a database field linked to the document record. These fields are searchable, allowing users to find documents by specifying coding values—e.g. <Document Date falls after 1/1/2012>; <Author contains "Smith">; or <Attorney coding is "Relevant">. There are two mutually-exclusive kinds of coding: objective and subjective.

1. Objective Coding. Also known as bibliographic, or "bib", coding, objective coding comprises any factual information about the document that is not subject to interpretation or debate, such as DateSent, Author, Recipient and Title. Much of this objective information will be on the face of the document (DateReceived, Author, Subject), but often it is not (it is a letter; it is a fax cover page; it has four attachments). To perform objective coding is to determine which facts about a document are pertinent for the review and to populate database fields with the appropriate values so that the document record now contains that additional information. The term "objective coding" refers to both the act of coding and the body of searchable information created by the coding exercise. With paper or scanned documents, all objective coding must be created manually. With electronic documents, much of the objective *information* is found in metadata (E-mail Sender, DateSent, E-mail Subject), i.e. it is embedded in the electronic document. But with electronic files, much relevant information is not stored in metadata; objective coding may be necessary or desired, such as for word-processing documents in which the Author of a letter or the Subject of a Memorandum is not available in metadata. This helps to explain why metadata is not generally included in

one or a handful of subject-matter experts (SMEs—usually partners or senior associates who know the case extremely well) review subsets of documents, code them and then use this coding to "teach" the software what kinds of documents are wanted and not wanted. The software codes the rest of the documents, and then the team takes a sample of these results and checks to see if the system properly coded those documents. The SME decisions confirming or overturning the software's decisions are then fed back into the system. After a few iterations (SME coding, processing, sampling, SME coding. . .), a final result is achieved on the entire collection with a degree of statistical accuracy greater than could be hoped for in a traditional linear review by human coders. This technology has now met with judicial approval in the U.S.[28] While not yet widely adopted in

---

the concept "coding": "coding" connotes the act of capturing what is not already there and entering it into a database where it is searchable.

2. Subjective coding. This is the assigning to a document (traditionally, using Post-Its, but now by adding values to the document record in a review database) a reviewer's assessment of the significance of that document. Subjective coding captures a subjective judgment. Common subjective coding fields are Relevance, Issues and Privilege. While it is common for parties to exchange at least some objective fields (whether derived from metadata or created through manual coding), it is uncommon for them to exchange subjective coding. The latter will often constitute work product that could reveal the thoughts and impressions of counsel and which therefore enjoys protection from disclosure. See *infra*, Principle 9.

3. Predictive coding. The word "coding" now has a new connotation derived from recent machine learning applications. "Predictive coding" involves computers processing the text of large numbers of documents and, based on algorithms, assigning a score or a binary value to each document in an attempt to imitate or predict human subjective judgment. For a discussion of predictive coding, see *infra*, Comment 7.c.iv.

28. See e.g. *Da Silva Moore v. Publicis Groupe*, 287 FRD 182 (WL) at 192 (SDNY 2012), aff'd sub nom. *Moore v. Publicis Groupe SA*, 2012 US Dist. LEXIS 58742 (SDNY 2012) (Carter, J).

Canada, this illustrates the power and the potential of modern technology as a tool for efficiently and effectively managing ESI in litigation.

9. The Risk of Inadvertent Disclosure of Sensitive Documents

In the world of paper, the generally smaller document volumes coupled with an inability to perform searches make a linear "eyes-on" review of all documents eligible for production the appropriate means of guarding against the disclosure of sensitive information.[29] With ESI, the much larger volumes make linear review all but impossible (and cost-prohibitive in many cases), while modern electronic search technologies offer an alternative: searches that can find many if not most of the sensitive documents. But clients and counsel need to understand the inherent limitations of any kind of search technology and be alert to the risks of inadvertent disclosure that persist, and can even be accentuated, through the use of electronic search methods.

First, it is all but impossible to craft a set of search terms that will find, in a targeted and efficient way, all of the sensitive documents being sought.[30] Such a search will (a) return documents that are not in fact sensitive despite containing one or

29. The term "sensitive" is meant to encompass all reasons for either withholding entirely or redacting a document, including: all forms of privilege, the work product doctrine, commercially sensitive information, personal health information, personally identifiable information, and so on.

30. A common practice in the search for documents that might warrant a claim of solicitor-client privilege is to search the presumptive production population for the names of lawyers and law firms. Such a search will guarantee that any documents that are privileged and that contain one or more of these names will be pulled back, but it will also (1) pull back large numbers of documents that are not privileged despite containing these

more terms ("false positives") and (b) fail to identify documents that are or might be sensitive despite the lack of any of these terms ("false negatives"). The goal of any information retrieval exercise is to reduce the rate of false negatives (i.e. to find as many of the desired documents as possible) without also returning too many false positives. This remains a challenge for all forms of information retrieval but it is particularly acute in the world of legal search because of the risks involved.[31]

Second, it is essential when using automated search techniques against ESI to understand what is and is not being searched. The most important distinction here is between the "body" of a document and its metadata. The body of a document and its metadata are commonly separated from each other during processing and loaded into separate database fields in a review tool. At the same time, most review tools will build a standard "extracted text" index that only includes the body of

---

names and also (2) fail to pull back documents that might be privileged but do not contain any of these names. The first problem (low precision) results in increased review time; the second (low recall) represents the risk of inadvertent disclosure. To reduce this second risk (generally felt to be more acute), review teams will often include in their searches additional terms thought to be strong indicators of potential privilege, such as: law, lawyer*, legal, lawsuit*, privilege*, confidential*, damages, plaintiff, etc. But each of these terms will pull in false positives, particularly the terms privilege* and confidential*, which will find all e-mails that contain a standard automated disclaimer containing one or both of these terms.

31. It is always possible to reduce the risk of inadvertent disclosure by simply reviewing more documents. But searches that include more terms, or more permissive terms (e.g. using wildcards, stemming and fuzzy searching) to get closer to finding all potentially sensitive documents will almost always bring back larger and larger numbers of false positives. Reducing false negatives will increase "recall," thereby lowering the risk of inadvertent disclosure, but almost always at the cost of reduced "precision," which means increased review costs.

each document. A simple keyword search will thus, most likely, search only the body of e-mail messages and the visible content of non-e-mail files. It will not search the "e-mail header fields"[32] or any other metadata fields, such as Filename or the Folder Path from which a file was collected. As a result, unless indexes or the searches themselves are designed to avoid this risk, searches will most likely not return documents that the review team needs to see. Conversely, if these sorts of metadata fields are included in searches, results may be over-inclusive—such as when a search for a person's name returns all of that person's e-mails or when a search for a company name returns all the contents collected from a folder structure on the server. All of these factors should be kept in mind when performing searches to identify potentially sensitive information.

Clients and counsel need to understand both the benefits and the limitations of automated search methods, and seek advice where appropriate.

32. This term is generally used to refer to the From, To, Cc, Bcc and Subject fields.

II. PRINCIPLES AND COMMENTARY

Principle 1: Electronically stored information is discoverable.

Comment 1.a. Definition of Electronically Stored Information

While the rules of court in Canadian jurisdictions provide varying definitions of what constitutes a "record" or "document" for the purposes of production in discovery, they all provide that ESI must be produced as part of the discovery process. Typical forms of ESI include, but are not limited to, Word, PowerPoint, and Excel documents, e-mail, instant messages, databases, information on social media, and information posted on the internet.

The *Personal Information Protection and Electronic Documents Act*,[33] defines "electronic document" as "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print-out or other output of that data." The *Canada Evidence Act*[34] defines an electronic record or document as "data that is recorded or stored on any medium in or by a computer system or other similar device."

Quebec passed *An Act to Establish a Legal Framework For Information Technology*,[35] which includes the following definition:

33. SC 2000, c 5. [*PIPEDA*].

34. RSC 1985, c C-5, s 31.8. [*Canada Evidence Act*].

35. *Quebec Information Technology Act*, *supra* note 11.

> "Document": Information inscribed on a medium constitutes a document. The information is delimited and structured, according to the medium used, by tangible or logical features, and is intelligible in the form of words, sounds or images. The information may be rendered using any type of writing, including a system of symbols that may be transcribed into words, sounds or images or another system of symbols.

Comment 1.b. Relevancy

Canadian courts have repeatedly held that ESI is producible and compellable in discovery.[36] Rules of court make relevancy a prerequisite to production, regardless of the form of record. For example, Part Five, Rule 5.2(1) of the *Alberta Rules of Court*[37] provides that producible records be both relevant and material. The Ontario *Rules of Civil Procedure*[38] provide that every document relevant to any matter in question in the action shall be produced. The British Columbia rules were amended in

---

36. See *Cholakis v. Cholakis*, [2000] MJ No 6 at para 30, 44 CPC (4th) 162 (CanLII) (Man QB): "The plaintiff has satisfied me that the electronic information requested falls within the definition of a document under the Rules and contains relevant information that should be produced. If the defendants. . .wish to provide the information in a format that does not reveal irrelevant information, then it is incumbent upon them to develop a mechanism by which that can be done. The interests of broad disclosure in a modern context require, in my view, the production of the information in the electronic format when it is available."

37. *Alberta Rules, supra* note 10.

38. *Ontario Rules, supra* note 10, r 30.02 (1): Every document relevant to any matter in issue in an action that is or has been in the possession, control or power of a party to the action shall be disclosed as provided in rules 30.03 to 30.10, whether or not privilege is claimed in respect of the document.

2009 to introduce concepts of proportionality and narrow the scope of documentary discovery.[39]

Courts have ordered the production of actual media in particular cases, such as in *Reichmann v. Toronto Life Publishing Co.*,[40] where a party was ordered to produce not only a printed copy of a manuscript stored on a disk and already produced, but the disk itself. The Court found that the disk fell within the common law definition of a "document" and therefore had to be produced.

In *Northwest Mettech Corp. v. Metcon Service Ltd.*,[41] however, the Court declined to order production by the defendants of an entire hard drive, and ordered production of only the relevant data stored on the drive. The Court found that the drive was simply a storage medium or electronic filing cabinet containing electronic documents, and that the defendants were not required to list the entire contents or produce the entire electronic filing cabinet any more than they would be with respect to a filing cabinet containing paper. The Court did order the defendants to produce an affidavit verifying all of the files on the hard drive related to the matter in issue. In appropriate circumstances, with proper safeguards for privilege and confidentiality, a court may be willing to grant access to a hard drive or other medium, and/or to allow inspection.[42] This suggests that access for forensic purposes such as recovering deleted information may be permitted.

39. See *BC Rules, supra* note 10.

40. 66 OR (2d) 65 (HCJ), 1988 CanLII 4644 (ON SC).

41. 1996 CanLII 1056 at para 10 (BCSC).

42. See *Nicolardi v. Daley*, [2002] OJ No 595 at para 5 (ONSC) (QL).

Comment 1.c. E-Commerce Legislation and Amendments to the Evidence Acts

Most provinces have passed legislation that provides guidance for the use of electronic means for creating and managing records, and for electronic commerce transactions.[43] These statutes provide that information shall not be denied legal effect or enforceability solely by reason that it is in electronic form.

The statutes do not require individuals to use or accept information in electronic form, but the consent of a person to do so may be inferred from the person's conduct. Requirements that information be in writing are generally satisfied if the information is accessible so as to be useable for subsequent reference.

Currently, legislation across Canada provides a means to facilitate the admissibility of ESI in the courts, including the establishment of evidentiary presumptions related to integrity of electronic information and procedures for introducing such evidence and challenging its admissibility, accuracy and integrity. The legislation generally does not modify any common law or statutory rule related to the admissibility of records, except the rules relating to authentication and best evidence.[44]

---

43. The Yukon, Prince Edward Island, Ontario, Newfoundland, Nova Scotia and Nunavut have respectively passed: *Electronic Commerce Act*, RSY 2002, c 66; RSPEI 1988, c E-4.1; SO 2000, c 17; SNL 2001, c.E-5.2; SNS 2000, c 26; and SNu 2004, c 7. Alberta, New Brunswick, British Columbia and the North West Territories have similar legislation under the title of the *Electronic Transactions Act*, found respectively at: SA 2001, c E-5.5; RSNB 2011, c 145, SBC 2001, c 10, and SNWT 2011, c 13. Manitoba's legislation is titled: *Electronic Commerce and Information Act*, CCSM 2000 c E55. Saskatchewan's legislation is entitled: *Electronic Information and Documents Act*, SS 2000, c E-7.22. Quebec's legislation is: *Quebec Information Technology Act*, *supra* note 11.

44. See e.g. *Evidence Act*, RSO 1990 c E.23, s 34.1 [*Ontario Evidence Act*]; *Quebec Information Technology Act*, *supra* note 11, s 5, 6 and 7.

Principle 2: In any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account: (i) the nature and scope of the litigation; (ii) the importance and complexity of the issues and interests at stake and the amounts in controversy; (iii) the relevance of the available electronically stored information; (iv) the importance of the electronically stored information to the Court's adjudication in a given case; and (v) the costs, burden and delay that the discovery of the electronically stored information may impose on the parties.

Comment 2.a. The Role of Proportionality

Proportionality is the "reasonableness" principle applied to the question of how much time and effort a party should have to expend with respect to ESI in light of all relevant factors. Courts across the country, including the Supreme Court of Canada, have confirmed that the principle of proportionality is to play a significant role in case management.[45] Every jurisdiction in Canada that has adopted ESI-related rules of procedure that impose affirmative obligations (e.g. ESI is discoverable, parties have a duty to preserve it, search it and produce what meets the threshold for disclosure) has adopted a proportionality principle.

The principle of proportionality is a reaction to delays and costs impeding access to justice, and while it requires a shift in legal culture, the intent of the principle is to create a new

45. See e.g. *Marcotte v. Longueuil (City)*, 2009 SCC 43 (CanLII); *Total Vision Enterprises Inc. v. 689720 BC Ltd*, 2006 BCSC 639 (CanLII) at para 36; *Abrams v. Abrams*, 2010 ONSC 2703 (CanLII).

norm. Master Short's decision in *Siemens Canada Limited v. Sapient Canada Inc.*,[46] provides an important analysis of proportionality and expectations of counsel to comply with this new principle.[47] This decision is referenced throughout these *Principles* and provides guidance for discovery planning and the transparency required by counsel in meeting their obligations.[48]

ESI is discoverable, and parties have a duty to preserve, search and then produce what ESI meets the relevant test for disclosure. But no party is required to preserve, search and produce all (or particularly problematic sets of) ESI where to do so would impose costs and burdens disproportionate to the value of the case or the probative value of the evidence in question, taking into account the availability of the same information from other sources and other factors. Proportionality principles are often used by a party seeking to reduce disclosure obligations, sometimes appropriately and sometimes inappropriately.

---

46. *Siemens Canada Limited v. Sapient Canada Inc.*, 2014 ONSC 2314 (CanLII) at para 51 [*Siemens*]. In *Siemens*, the parties did not establish a discovery plan but proceeded to produce documents without communicating with each other. When Siemens produced 120,043 documents, and Sapient only produced 23,356 documents, Siemens challenged Sapient's document production as deficient. While Siemens was partially successful on its motion, the Ontario Superior Court of Justice denied it any costs, noting that the parties were "the authors of their own misfortune" for proceeding without a discovery plan.

47. See also detailed analyses in: *Warman v. National Post Co* 2010 ONSC 3670 (Master Short) [Warman]; Kaladjian v. Jose, 2012 BCSC 357 (Davies, J) [Kaladjian]; The Sedona Conference, *The Sedona Canada Commentary on Proportionality in Electronic Disclosure & Discovery* (Oct. 2010 public comment version) and its Appendix 1, online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/468>.

48. *Siemens*, *supra* note 46. See also <http://www.felsky.com/blog/ontario-master-proportionality-requires-transparency> for a discussion on the key points of the decision.

The widespread use of computers and the internet has created vast amounts of ESI, making the cost and burden of discovery exponentially greater than it was in the "paper" world. Even a case involving small dollar amounts and straightforward legal issues can give rise to significant volumes of ESI. Litigants should take a practical and efficient approach to electronic discovery, and should ensure that the burden of discovery remains proportionate to the issues, interests and money at stake. Without a measured approach, overwhelming electronic discovery costs may prevent the fair resolution of litigation disputes. "The new *Rules* recognize that application of a 19th century test to the vast quantity of paper and electronic documents produced and stored by 21st century technology had made document discovery an unduly onerous and costly task in many cases. Some reasonable limitations had become necessary and Rule 7-1 (1) is intended to provide them."[49]

The case law underscores that "proportionality is a parsimonious principle."[50] That is, the proportionality principle should generally lead to a narrowing, not an expansion, of the volume of discovery. That being said, parties should not use the proportionality principle as a shield to avoid their legitimate discovery obligations. Parties should plan for the e-discovery process from the outset with a view to analyzing the potential costs of e-discovery, the means of controlling such costs and what process might best achieve proportionality.[51] As stated by

---

49. *Kaladjian, supra* note 47 at para 60, citing N. Smith J in *More Marine Ltd. v. Shearwater Marine Ltd.*, 2011 BCSC 166.

50. *Ontario v. Rothmans Inc.*, 2011 ONSC 2504 (CanLII) at para 160.

51. See e.g. *L'Abbé v. Allen-Vanguard*, 2011 ONSC 7575 (CanLII) at para 24: "efficiency and cost effectiveness in production and discovery should be a mutual goal. Questions of relevance and privilege must be answered of course but it is necessary to apply those filters in a practical manner . . . .

the Court in *Siemens*: "[n]ow as we approach the fifth anniversary of the Rule changes, a case such as this presents an opportunity to demonstrate the consequences of postponing the development of a practical discovery plan and to stress the obligation of the parties and counsel to define the basis upon which both parties will establish their productions in complex cases such as this."[52]

Costs extend beyond recovering electronic documents or making them available in a readable form, searching documents to separate the relevant material from the irrelevant material, reviewing the documents for privilege and producing the documents to the other party. Non-monetary costs and other factors include possible invasion of individual privacy as well as the risks to confidences and legal privileges. Electronic discovery can overburden information-technology personnel and organizational resources.

Courts frequently balance the costs of discovery with the objective of securing a just, speedy and inexpensive resolution of the dispute on the merits.[53] In the discovery context, Canadian courts have begun to emphasize their mandate to meet that objective.[54] Courts have not ordered production of documents where the parties have demonstrated that the costs of producing documents or the adverse effect upon other interests, such as

---

Equally or more important is the need for collaborative and creative goal oriented problem solving by the parties and their respective counsel."

52. *Siemens, supra* note 46 at para 51.

53. The rules of court in every jurisdiction in Canada contain a provision emphasizing the overriding importance of maintaining proportionality within legal proceedings.

54. See e.g. *L'Abbé, supra* note 51 at para 41.

privacy and confidentiality, outweigh the likely probative value of the documents.[55]

It has also been suggested that discovery disputes need to be proportionate and not themselves be an occasion for adversarial advocacy, and alternate forms of adjudication such as a reference under Ontario's Rule 54.03 may be appropriate.[56] At least one Justice of the Ontario Superior Court of Justice included proportionate electronic discovery and planning in his standard Case Management Directions.[57] Proportionality applies not only to the parties' use of their own resources, but also to their use of the Court's time.[58]

---

55. *Goldman, Sachs & Co. v. Sessions*, 2000 BCSC 67 (CanLII) (declining to order production where probative value outweighed by time and expense of production and the party's confidentiality interest); *Ireland v. Low*, 2006 BCSC 393 (CanLII) [*Low*] (declining to order production of hard drive where probative value outweighed by privacy interests); *Baldwin Janzen Insurance Services (2004) Ltd. v. Janzen*, 2006 BCSC 554, 53 BCLR(4th) 329 [*Janzen*] (CanLII) (declining to order production of hard drive in the particular circumstances of the case); *Desgagne v. Yuen*, 2006 BCSC 955, 56 BCLR(4th) 157 (CanLII) (declining to order production of a hard drive, metadata and internet browser history due, in part, to the intrusive nature of the requested order compared to the limited probative value of the information likely to be obtained.).

56. *Siemens, supra* note 46 at para 40; *Lecompte Electric Inc. v. Doran (Residential) Contractors Ltd.*, 2010 ONSC 6290 (CanLII) at para 15.

57. See e.g. *Yan v. Chen*, 2014 ONSC 3111 at Appendix A (CanLII) (Brown J).

58. *Sherman v. Gordon*, 2009 CanLII 71722 (ON SC) ("The concept of proportionality has to apply in the context of the litigants' use of court time as well as to the expenditure of their funds.").

Comment 2.b. The Proportionality Rule by Jurisdiction

As noted above, in the last few years, most Canadian jurisdictions have amended their respective rules of court to expressly include proportionality as a general rule for all litigation, and specifically in discovery procedures.

The Chief Justice of the Supreme Court of British Columbia promulgated a *Practice Direction Regarding Electronic Evidence* (effective July 1, 2006),[59] setting forth default standards for the use of technology in the preparation and management of civil litigation, including the discovery of documents in electronic form (whether originating in electronic form or not). Section 6.1 suggests that the scope of discovery may be modified to reflect the circumstances of the particular case. For example, it requires the parties to confer regarding limitations on the scope of electronic discovery where the ordinary rules would be "unduly burdensome, oppressive or expensive having regard to the importance or likely importance" of the electronic documents.[60]

In Nova Scotia, the requesting party must establish a *prima facie* case that something relevant will be uncovered. The Court has authority to limit discovery. For example, in *Nova Scotia (Attorney General) v. Royal & Sun Alliance Insurance Co. of Canada*,[61] the Court observed: "there is a discretion to limit discovery where it would be just to do so, such as where the burdens

59. Courts of British Columbia, *Practice Direction Re: Electronic Evidence* (2006), online: Courts of British Columbia <http://www.courts.gov.bc.ca/supreme_court/practice_and_procedure/practice_directions_and_notices/electronic_evidence_project/Electronic%20Evidence%20July%201%202006.pdf> [*BC Practice Direction*].

60. *Ibid.*

61. 2003 NSSC 227 at para 8, 218 NSR(2d) 288 (CanLII).

that would be placed upon the party making answer clearly outweigh the interests of the party questioning."

In Quebec, Section 4.2 of the *Code of Civil Procedure* (CCP) reads as follows: "In any proceeding, the parties must ensure that the proceedings they choose are proportionate, in terms of the costs and time required, to the nature and ultimate purpose of the action or application, and to the complexity of the dispute; the same applies to proceedings authorized or ordered by the judge."[62] Quebec courts have indicated that the proportionality rule must be interpreted in conjunction with section 4.1 CCP.[63] Section 4.1 reads as follows: "Subject to the rules of procedure and the time limits prescribed by this Code, the parties to a proceeding have control of their case and must refrain from acting with the intent of causing prejudice to another person or behaving in an excessive or unreasonable manner, contrary to the requirements of good faith." The rule of proportionality has been applied to the exchange of documents on CDs,[64] to the examination of a witness by videoconference[65] as well as to the control of an examination where an excessive volume of documents had been requested and an unreasonable number of questions had been asked.[66] Although "the Court sees to the orderly progress of the proceedings and intervenes to ensure proper manage-

62. RSQ c C-25, s 4.2.

63. *9103-3647 Québec Inc. c Couët*, 2003 IIJCan 14311 (CanLII) (QC CS).

64. *Citadelle, Cie d'assurance générale c Montréal (Ville)*, 2005 IIJCan 24709 (CanLII) (QC CS).

65. *Entreprises Robert Mazeroll Ltée c Expertech - Batisseur de réseaux Inc.*, 2005 IIJCan 131, 2005 CarswellQue 9122 (QC CQ).

66. *Ryan Parsons c Communimed Inc.* (2005), JE 2005-1042, 2005 CarswellQue 2058 (WL) (CQ).

ment of case" according to section 4.1 CCP para 2, the application of the proportionality rule relies on the parties, as stated by section 4.2 CCP.[67]

The proportionality principles in the Ontario *Rules of Civil Procedure* and the *Sedona Canada Principles* have also been adopted in interpreting procedural rules in other forums, including Ontario's Financial Services Tribunal.[68]

Comment 2.c. An Evidentiary Foundation for Proportionality

When a producing party wishes to reduce the scope of its production obligations by relying on the proportionality principle, or when a requesting party seeks to compel the responding party to expand its document disclosure, that party must lead evidence.[69]

In Ontario, the E-Discovery Implementation Committee has prepared a model chart to assist parties to argue production

---

67. Luc Chamberland, *La Règle de proportionnalité: à la recherche de l'équilibre entre les parties?* in La réforme du Code de procédure civile, trois ans plus tard (Cowansville, Que: Yvon Blais, 2006).

68. *BCE Inc. v. Ontario (Superintendent of Financial Services)*, 2012 ONFST 25 (CanLII) and *Rakosi v. State Farm Mutual Automobile Insurance Co.*, 2012 CarswellOnt 7066 (ONFSC Appeal decision).

69. See e.g. *Midland Resources Holding Limited v. Shtaif*, 2010 ONSC 3772 (CanLII) at para 15 ("at least some evidence"); *Dell Chemists (1975) Ltd. v. Luciani et al*, 2010 ONSC 7118 at para 5 (CanLII) ("cogent evidence"); *Saliba v. Swiss Reinsurance Co.* , 2013 ONSC 6138 (CanLII) (appeal from Master); *Velsoft*, *supra* note 14 at para 8; *Siemens*, *supra* note 46 at paras 142–144; *BCE*, *supra* note 68 at para 35; *Hudson v. ATC Aviation Technical Consultants*, 2014 CanLII 17167 (ON SC) [*ATC Aviation*] (appeal of Master's decision) at para 13; and *Kaladjian, supra* note 47 at paras 62–64. But see *Rothmans, supra* note 50 at para 164**.**

motions based on proportionality.[70] The case law supports the use of the chart to structure proportionality arguments.[71]

Comment 2.d. Proportionality in Procedure

While the focus of these *Principles* is to provide an outline of best practices with respect to the handling of ESI, it is important to note briefly the broader role proportionality has in civil litigation and the required shift in legal culture. In *Hryniak v. Mauldin*,[72] the Supreme Court of Canada discussed the role of proportionality in the Canadian civil justice system and the need for a shift in legal culture to maintain the goals of a fair and just process that results in a just adjudication of disputes.[73]

While the context of the decision was an appeal of a summary judgment motion, the Court discussed the developing consensus that extensive pretrial processes no longer reflect modern reality, and a new proper balance requires proportionate procedures for adjudication. As stated at paragraphs 28–29:

> The principal goal remains the same: a fair process that results in a just adjudication of disputes. . . . However, that process is illusory unless it is also accessible—proportionate, timely and affordable. The proportionality principle means that the best forum for resolving a dispute is not always that with the most painstaking procedure.

---

70. Ontario Bar Association, *Model E-Discovery and E-Trial Precedents* at "Materials for use by the Court-Model Document #10," online: Ontario Bar Association <http: //www.oba.org/en/publicaffairs_en/e-discovery/model_precedents.aspx>.

71. *Guestlogix v. Hayter*, 2010 ONSC 4384 (CanLII).

72. *Hryniak v. Mauldin,* 2014 SCC 7 (CanLII), [2014] 1 S.C.R. 87.

73. *Ibid* at paras 23–33.

> . . .
>
> If the process is disproportionate to the nature of the dispute and the interests involved, then it will not achieve a fair and just result.

Noting that the proportionality principle is reflected in many of the provinces' rules, the Court confirmed that proportionality can act as a touchstone for access to civil justice. Relying on a decision of the Newfoundland Court of Appeal,[74] the Court stated that even where the proportionality principle is not codified, rules of court that involve discretion include the underlying principle of proportionality, taking into account the appropriateness of the procedure, costs and impact on the litigation and its timeliness, given the nature and complexity of the litigation.

Most provinces have summary litigation procedures where the amount at issue is less than $100,000. For example, in British Columbia, Rule 68 of the Supreme Court Rules[75] modifies ordinary litigation procedures for certain actions to require the Court to consider what is reasonable where the amount at issue is less than $100,000. Rule 68 limits the times at which interlocutory applications may be brought and modifies the generally broad scope of discoverable documents. In particular, a party must list only those documents referred to in the party's pleading, the documents to which the party intends to refer to at trial, and all documents in the party's control that could be used to prove or disprove a material fact at trial. The Court has the discretion to require more extensive discovery, but will

74. *Szeto v. Dwyer*, 2010 NLCA 36, cited at *Hryniak*, *ibid* at para 31.

75. *BC Rules*, *supra* note 10; see also *Ontario Rules*, *supra* note 10, r 76, presenting a Simplified Procedure applicable to most civil actions involving less than $100,000.

"consider the difficulty or cost of finding and producing the documents."

Principle 3. As soon as litigation is reasonably anticipated, the parties must consider their obligation to take reasonable and good-faith steps to preserve potentially relevant electronically stored information.

Comment 3.a. Scope of Preservation Obligation

A party's obligation to preserve potentially relevant evidence will vary across jurisdictions and proceedings. Parties should understand their obligations with respect to the preservation/non-spoliation of evidence, including ESI.[76] For example, as set out below, in common law jurisdictions the obligation to preserve data arises as soon as litigation is contemplated or threatened, but when that point is reached is a fact-by-fact determination. If a company receives threats of litigation on a daily basis, having to preserve all data every time a letter is received would effectively mean that the company could never delete any documents. When this obligation arises is a legal question to be carefully considered in each case.

Due to volume, complexity, format, location and other factors, the possible relevance of collections of ESI or individual electronic files may be difficult to assess in the early stages of a dispute. Even where such an assessment is technically possible,

76. The obligations to preserve relevant evidence for use in litigation are distinct from any regulatory or statutory obligations to maintain records. For example, various federal and provincial business corporations' acts and insurance health statutes prescribe statutory requirements for record keeping. Records management and obligations to meet regulatory and statutory record keeping is outside the scope of *The Sedona Canada Principles Addressing Electronic Discovery*.

it may involve disproportionate cost and effort. In such circumstances, it may be more reasonable to expect a party to first make a good-faith assessment of where (in what locations; on what equipment) its relevant ESI is most likely to be found and then, with the benefit of this assessment, take appropriate steps to preserve those sources.

The general obligation to preserve evidence extends to ESI but must be balanced against the party's right to continue to manage its electronic information in an economically reasonable manner. This includes routinely overwriting electronic information in appropriate cases. It is unreasonable to expect organizations to take every conceivable step to preserve all ESI that may be potentially relevant.

Comment 3.b. Preparation for Electronic Discovery Reduces Cost and Risk: Information Governance and Litigation Readiness

The costs of discovery of ESI can be best controlled if steps are taken to prepare computer systems and users of these systems for the demands of litigation or investigation. Information governance is growing in importance, beyond just the realm of e-discovery, implicating virtually all operations of an organization. To reflect the importance of information governance and its "downstream" effects in an e-discovery engagement, the Electronic Discovery Reference Model (EDRM) incorporated Information Governance into its diagram in 2007[77] and has also developed an Information Governance Reference Model (IGRM).[78]

---

77. See EDRM, EDRM Diagram Elements, online: EDRM <http://www.edrm.net/resources/diagram-elements>.

78. The IGRM is more than an expansion of this one cell in the EDRM. See EDRM, Information Governance Reference Model (IGRM), online:

The possibility that a party will have to demonstrate that it used defensible methods in the handling of ESI and that it maintained proper chains of custody makes effective information governance practices all the more important. The integrity of electronic records begins with the integrity of the records management systems in which they were created and maintained.

With a view to litigation readiness, larger organizations should consider establishing an e-discovery response team, with representation from key stakeholders, including legal, business unit leaders, IT, records/information governance, human resources, corporate security and perhaps external e-discovery consultants / service providers.

The steps to be taken to ensure compliance with best practices and to control costs include defining orderly procedures and policies for preserving and producing potentially relevant ESI, and establishing processes to identify, locate, preserve, retrieve, assess, review and produce data. A records retention policy should provide guidelines for the routine retention and destruction of ESI as well as paper, and account for necessary modifications to those guidelines in the event of litigation.

EDRM <http://www.edrm.net/projects/igrm>. "The IGRM Project does NOT aim to solely build out the Information Management node of the EDRM framework. It will be extensible in numerous directions, such as records management, compliance and IT infrastructure." Principles and protocols about ESI and evidence have been published by various bodies across Canada, including the Canadian Judicial Council, the Canadian General Standards Board, the Competition Bureau <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03789.html>, and various provinces. The Sedona Canada Working Group favors continuing efforts to reach consensus on principles, protocols and best practices in information governance and e-discovery.

Having a records management system that provides a map of where all data is stored and how much data is in each location, and having an understanding of how difficult it is to access, process and search those documents will enable a party to present a more accurate picture of the cost and burden to the Court when refusing further discovery requests, or when applying for orders shifting costs to the receiving party in appropriate cases. It also mitigates the risk of failing to preserve or produce evidence from computer systems, thereby reducing the potential for sanctions. Costs can also be controlled through careful and cooperative discovery planning.

In *Siemens*, the defendant's corporate retention policy was considered inadequate and resulted in an order requiring further recovery attempts. The Court stated that "[o]bviously a company is entitled to establish whatever e-mail retention policies it wishes in order to minimize server use and cost. However, in a project such as this, which obviously carries over a lengthy period of time, such a policy can potentially create serious problems."[79]

Comment 3.c. Response Regarding Litigation Preservation

Parties should take reasonable and good-faith steps to meet their obligations to preserve information relevant to the issues in an action.[80] As noted above, in common law jurisdictions, the preservation obligation arises as soon as litigation is

79. *Siemens*, *supra* note 46 at paras 135–138.

80. *Doust v. Schatz*, 2002 SKCA 129 at para 27, 227 Sask. R 1 (CanLII): "The integrity of the administration of justice in both civil and criminal matters depends in a large part on the honesty of parties and witnesses. Spoliation of relevant documents is a serious matter. Our system of disclosure and

contemplated or threatened.[81] Owing to the dynamic nature of ESI, any delay increases the risk of relevant evidence being lost and subsequent claims of spoliation.[82] A proactive preservation plan will ensure a party can respond meaningfully and quickly to discovery requests or court orders.

---

production of documents in civil actions contemplates that relevant documents will be preserved and produced in accordance with the requirements of the law: see e.g. *Livesey v. Jenkins*, reflex, [1985] 1 All E.R. 106 (H.L.); *Ewing v. Ewing (No. 1)* (1987), 1987 CanLII 4889 (SK CA), 56 Sask. R. 260; *Ewing v. Ewing (No. 2)* (1987), 1987 CanLII 4865 (SK CA), 56 Sask. R. 263 (C.A.); *Vagi v. Peters*, reflex, [1990] 2 W.W.R. 170; *R. v. Foster and Walton-Ball* (1982), 1982 CanLII 2522 (SK CA), 17 Sask. R. 37 (C.A.); and *Rozen v. Rozen*, 2002 BCCA 537 (CanLII), [2002] B.C.J. No. 2192 (Q.L.). "A party is under a duty to preserve what he knows, or reasonably should know, is relevant in an action. The process of discovery of documents in a civil action is central to the conduct of a fair trial and the destruction of relevant documents undermines the prospect of a fair trial."

81. See *Culligan Canada Ltd. v. Fettes*, 2009 SKQB 343 (reversed on other grounds): "As soon as litigation was threatened in this dispute, all parties became obligated to take reasonable and good faith steps to preserve and disclose relevant electronically stored documents." In *Johnstone v. Vincor International Inc.*, 2011 ONSC 6005, a defendant was on notice that a legal action had been started, but chose to rely on a technicality regarding service and failed to follow its own policies in place to deal with situations of this nature when it knew that it had record retention policies in place that would possibly lead to the loss of important and relevant documents. The Court noted that as retention policies and preservation plans serve two different purposes, organizations may need to act promptly at the outset of possible litigation to suspend automatic electronic file destruction policies in order to preserve evidence.

82. On the issue of intentional spoliation of evidence as a separate tort, see *North American Road Ltd. v. Hitachi Construction*, 2005 ABQB 847 at paras 16–17, [2006] AWLD 1144; *Spasic Estate v. Imperial Tobacco Ltd., et al.* (2000), 49 OR (3d) 699 (CA), 2000 CanLII 17170. On the issue of the appropriate relief in connection with negligent spoliation, see *McDougall v. Black & Decker Canada Inc.*, 2008 ABCA 353 (CanLII).

In Nova Scotia, Rule 16 of the *Civil Procedure Rules* specifically outlines preservation requirements and refers to the obligations established by law to preserve evidence before or after a proceeding is started.[83]

The scope of what is to be preserved and the steps considered reasonable may vary widely depending upon the nature of the claims and information at issue.[84] The courts have ordered

---

83. *Nova Scotia Civil Procedure Rules*, Royal Gazette Nov 19, 2008, Part 5;

16.01:

> (1) This Rule prescribes duties for preservation of relevant electronic information, which may be expanded or limited by agreement or order.
>
> (2) This Rule also prescribes duties of disclosure of relevant electronic information and provides for fulfilling those duties . . .

16.02:

> (1) This Rule 16.02 provides for preservation of relevant electronic information after a proceeding is started, and it supplements the obligations established by law to preserve evidence before or after a proceeding is started.

16.14:

> (1) A judge may give directions for disclosure of relevant electronic information, and the directions prevail over other provisions in this Rule 16.
>
> (2) The default Rules are not a guide for directions.
>
> (3) A judge may limit preservation or disclosure in an action only to the extent the presumption in Rule 14.08, of Rule 14 — Disclosure and Discovery in General, is rebutted.

84. In contrast to the extensive case law and commentary in the United States, the law regarding preservation of electronic documents in Canada is still developing. Not surprisingly, several Canadian courts have looked to the U.S. for guidance in defining the scope of the duty to preserve, though

more targeted preservation.[85] That said, parties that repeatedly have to deal with preservation issues should consider what steps they can take to avoid having to repeat steps in the future.

Comment 3.d. Notice to Affected Persons in Common Law Jurisdictions—Legal Holds

Upon determining that a preservation obligation has been triggered,[86] the party should communicate to affected persons the need to preserve relevant information in both paper and electronic form. This notice is referred to as a "legal hold." The style, content and distribution of the legal hold will vary widely depending upon the circumstances, but the language used should be plain and clear and provide clear instructions to recipients. The legal hold should set out in detail the kinds of information that must be preserved so the affected custodians

---

U.S. law is more demanding than in Canada in notable respects. The decisions from the Southern District of New York in *Zubulake v. UBS Warburg LLC*, 220 FRD 212 at 217 (SDNY 2003) (WL) and *Pension Committee of the University of Montreal Pension Plan v. Banc of America Secs., LLC, et al.*, No 05 Civ 9016 (SAS), 2010 WL 184312 (SDNY 2010), provide guidance regarding the scope of the duty to preserve electronic documents and the consequences of a failure to preserve documents that fall within that duty. At paragraph 7 of the former, the Court commented as follows on the scope of the duty to preserve: "Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no.' Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation. As a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation."

85. *Drywall Acoustic, Lathing and Insulation, Local 675 Pension Fund (Trustees) v SNC Lavalin Group Inc.*, 2014 ONSC 660 at paras 111–112 [*Drywall Acoustic*].

86. The Crown and police in criminal proceedings also have a duty to preserve evidence. See *R v. Sharma,* 2014 ABPC 131 (CanLII) at para 92.

can segregate and preserve it. Legal holds should not typically require the suspension of all routine records management policies and procedures. The legal hold should also advise the custodians that relevant documents can exist in multiple locations (i.e. networks, workstations, laptop, home computers, phones, tablets, voicemail, paper, etc.).

As noted above, the legal hold only needs to be sent to "affected" persons, i.e. those reasonably likely to maintain documents relevant to the litigation. Often custodian interviews will help to identify which people actually hold relevant documents. The legal hold should also be sent to the person(s) responsible for maintaining and operating the computer systems that house the documents subject to the legal hold. This is often the organization's IT department. A meeting should also be held with the IT people to ensure everyone understands what information must be preserved by the legal hold. The legal hold may, in certain cases, also be sent to non-parties who have in their possession, control or power information relating to matters at issue in the action.

The legal hold should mention the volatility of ESI and make it clear that particular care must be taken not to alter, delete or destroy it.[87] Once a legal hold is issued, this step is not over. It is advisable to resend the legal hold to the custodians at least every 6 months, and to ensure it is sent to any new employees to whom it may apply. While we have not seen any case law on this point yet in Canada, there is case law in the U.S. that requires legal holds to be resent on a regular basis. Custodians should also be advised when a legal hold is lifted. When legal

87. Ontario Bar Association, *Model E-Discovery and E-Trial Precedents* at "Materials for use by the Court-Model Document #5-6," online: Ontario Bar Association <http: //www.oba.org/en/publicaffairs_en/e-discovery/model_precedents.aspx>.

holds apply to documents and data spanning a significant or continuing period, organizations should determine how to deal with systems, hardware or media containing unique relevant material that might be retired as part of technology upgrades. Database information should also be considered.

> *Illustration i:* A company receives a statement of claim alleging that it has posted false or misleading information about its products on its website. It uses an outsourcer to manage its e-mail and its website. As part of its contract for services, the company requires the outsourcer to make weekly backups of the website and to keep the backup tapes for 6 months, after which it would keep the last copy of the month. The company issues a legal hold to the outsourcer asking it to suspend the rotation of the backup tapes until it can determine which tapes would contain the version of the website corresponding to the time period mentioned in the claim.
>
> *Illustration ii:* A former employee is suspected of having stolen client contact information and copies of design diagrams when he resigned to start a competing company. The relevant systems can generate electronic reports that can be sent by e-mail to a recipient. A legal hold should be sent to the company's IT department asking that it preserve the log of the former employee's activities as well as any e-mails sent, received or deleted from the former employee's account. The legal hold should also instruct the company's IT department

> from "wiping" the former employee's workstation and reassigning it to another member of the company.

The best evidence for the case in this illustration, however, may be with the former employee. See below discussion on Anton Piller orders in Comment 3.g. (Preservation Orders).

Comment 3.e. Preservation in the Province of Quebec

In the civil law jurisdiction of Quebec, the parties' obligations in the context of litigation differ from that in common law jurisdictions. For instance, the obligation to disclose documents to the opposing party ("communication of documents") is, at the first stage of litigation, limited to those documents that the disclosing party intends to refer to as exhibits at the hearing. The receiving party can also request specific documents in the context of discovery.

Although there is no specific obligation to preserve electronic documents in advance of litigation,[88] the Superior Court has recognized the existence of an implicit obligation to preserve evidence based on the general obligation of parties to refrain from acting with the intent of causing prejudice to another person or behaving in an excessive or unreasonable manner, which would be contrary to the requirements of good faith as prescribed by the *Code of Civil Procedure*.[89]

Before litigation has started, a party who has reason to fear that relevant evidence will become lost or more difficult to use can apply to the Court for an order to allow a person of their

88. *Jacques c Ultramar ltée*, 2011 QCCS 6020 (CanLII).

89. *Quebec Code*, *supra* note 10 at s 4.1.

choice to examine the evidence in question if its condition may affect the outcome of the expected legal proceeding.[90]

In Quebec, in view of the absence of an express preservation obligation, a party seeking a preservation order would need to present a motion for injunction or safeguard order in accordance with the criteria governing such proceedings.[91] In all circumstances, parties should send a legal hold letter to the other parties to ensure that the other parties are aware of the ESI that will be requested.

Comment 3.f. Extreme Preservation Measures Are Not Necessarily Required

The basic principle which defines the scope of the obligation to preserve relevant information can be found in the common law.[92] A reasonable inquiry based on good faith to identify and preserve active and archival data should be sufficient. In instances where relevant ESI can only be obtained from backup tapes or other non-readily accessible sources and the effort required to preserve them is not disproportionate given the issues and interests at stake, they should be preserved.[93]

In situations where deleted, fragmented or overwritten information can only be recovered at significant cost, a party may not be required, absent agreement or a court order based

---

90. *Ibid*, s 438.

91. *Ultramar, supra* note 88 at para 26.

92. The Ontario E-Discovery guidelines provide a useful resource: Discovery Task Force, *Guidelines for the Discovery of Electronic Documents* (2005) at Principle 3 and Principle 4, online: Ontario Bar Association <http://www.oba.org/en/pdf_newsletter/E-discoveryguidelines.pdf> [*Discovery Task Force Guidelines*].

93. *Mansfield v. Ottawa*, 2012 ONSC 5208 at para 43 (CanLII).

on demonstrated need and relevance, to recover and preserve such information. (See Principle 6).

Comment 3.g. Preservation Orders

In some cases it may be appropriate to seek the intervention of the Court to ensure that ESI is preserved. For example, Anton Piller orders,[94] which allow one party to copy or take custody of evidence in the possession of another party, have been widely used in most Canadian jurisdictions when one party is concerned that the opposing party will destroy relevant ESI. Anton Piller orders are exceptional remedies, granted without notice and awarded in very limited circumstances, for instance "when it is essential that the plaintiff should have inspection so that justice can be done between the parties. . . [and]. . .there is a grave danger that vital evidence will be destroyed." The Supreme Court of Canada provided guidelines for the granting and execution of Anton Piller orders in *Celanese Canada Inc. v. Murray Demolition Corp*.[95]

To avoid having a Court make a determination as to whether a sufficiently strong case has been presented for the granting of an Anton Piller order, the parties may choose to deal "cooperatively and in a common sense manner with the points of concern," as the parties did with respect to the motion brought by the plaintiffs for Anton Piller relief in *CIBC World Markets Inc. v. Genuity Capital Markets*.[96] The defendants voluntarily undertook to preserve the electronic evidence and retained a forensic consultant to execute the preservation. The

94. The order is named after the English case of *Anton Piller KG v Manufacturing Processes Ltd & Ors*, [1975] EWCA Civ 12, [1976] 1 All ER 779.

95. 2006 SCC 36 (CanLII).

96. 2005 CanLII 3944 (ON SC).

Court provided in its Order that the forensic consultant was to have access to the defendants' systems and devices so that it could image and store the contents of computers, Blackberries and other similar electronic devices the defendants had in their possession, power, ownership, use and control, both direct and indirect. The Court Order also provided that the forensic consultant was to have access to such devices wherever located, including at any office or home (but not restricted to such locations), regardless of whether the devices were owned or used by others.

In instances where intentional destruction of evidence is not an issue, the risk of inadvertent deletion can be addressed by a demand to preserve evidence.[97] An Anton Piller order obtained *ex parte* was set aside where the plaintiff did not establish a real possibility that evidence may be destroyed.[98]

In *Portus Alternative Asset Management Inc. (Re)*,[99] the Ontario Securities Commission successfully applied for an order appointing a receiver of all assets, undertakings and properties of an asset management company. The Court granted the receiver unfettered access to all electronic records for the purpose of allowing the receiver to recover and copy all electronic information, and specifically ordered the debtors not to alter, erase or destroy any records without the receiver's consent. The debtors were ordered to assist the receiver in gaining immediate ac-

97. *Nac Air, LP v. Wasaya Airways Limited*, 2007 CanLII 51168 (ON SC) at para 26.

98. In the decision *Velsoft Training Materials Inc. v Global Courseware Inc.*, 2011 NSSC 274, the Anton Piller order was set aside on the grounds that the discovery that one employee had his computer erased was not sufficient basis to find grave risk that the defendants would destroy evidence.

99. (2005), 28 OSC Bull 2670.

cess to the records, to instruct the receiver on the use of the computer systems and to provide the receiver with any and all access codes, account names and account numbers. In addition, all internet service providers were required to deliver to the receiver all documents, including server files, archived files, recorded messages and e-mail correspondence.

Comment 3.h. All Data Does Not Need to be "Frozen"

Even though it may be technically possible to capture vast amounts of data during preservation efforts, this usually can be done only with significant disruption to IT operations. If a party's established and reasonable practice results in a loss or deletion of some ESI, it should be permitted to continue such practice after the commencement of litigation, as long as such practice does not result in the overwriting of ESI relevant to the case that is not preserved elsewhere.

Imposing an absolute requirement to preserve all ESI could require shutting down computer systems and making copies of data on each fixed disk drive, as well as other media that are normally used by the system—a procedure which could paralyze the party's ability to conduct ongoing business. A party's preservation obligation should therefore not require freezing of all ESI, but rather the appropriate subset of ESI that is relevant to the issues in the action.[100]

Comment 3.i. Disaster Recovery Backup Media

Some organizations have short-term disaster recovery backup media that they create in the ordinary course of business. The purpose of this media is to have a backup of active computer files in case there is a system failure or a disaster such

100. See *Schatz*, *supra* note 80; and *Janzen*, *supra* note 55.

as a fire. Their contents are, by definition, duplicative of the contents of active computer systems at a specific point in time.

Generally, parties should not be required to preserve these short-term disaster backup media, provided that the appropriate contents of the active system are preserved. Further, because backup media generally are not retained for substantial periods, but are instead periodically overwritten when new backups are made, preserving backup media would require a party to purchase new backup media.

In some organizations, the concepts of "backup" and "archive" are not clearly separated, and backup media are retained for a relatively long period of time. Backup media may also be retained for long periods of time out of concern for compliance with record retention laws. Organizations that use backup media for archival purposes should be aware that this practice is likely to cause substantially higher costs for evidence preservation and production in connection with litigation.[101] Organizations seeking to preserve data for business purposes or litigation should, if possible, consider employing means other than traditional disaster recovery backup media.

---

101. See *Farris v. Staubach Ontario Inc.*, 2006 CanLII 19456 at para 19 (ONSC): "In his testimony before me Mr. Straw corrected one statement in the June 28, 2005 letter to the solicitors for the plaintiff. In that letter the solicitors for TSC reported that TSC did not have a separate archival copy of its electronic databases for the November-December 2003 time period. This is not strictly accurate. Sometime in 2004 and probably after June 28, 2004, Mr. Straw had a backup set of tapes made of all information on the TSC server. These tapes have been preserved. While they are not an archival copy of the TSC database for November–December 2003, some of the information on these tapes goes back to that time period. Mr. Straw did not know how many documents were on those preserved archival tapes. However he said they contain in excess of one terabyte of information."

If a party maintains archival data on tape or other offline media[102] not accessible to end users of computer systems, steps should be taken promptly after the duty to preserve arises to preserve those archival media that are reasonably likely to contain relevant information not present as active data on the party's systems.[103] These steps may include notifying persons responsible for managing archival systems to retain tapes or other media as appropriate.[104]

> *Illustration i.* Pursuant to an information technology management plan, once each day a company routinely copies all electronic information on its systems and retains, for a period of 5 days, the resulting backup tapes for the purpose of reconstruction in the event of an accidental erasure, disaster or system malfunction. A requesting party seeks an order requiring the company to preserve, and to cease reuse of, all existing backup tapes pending discovery in the case. Complying with the requested order would impose large expenses and burdens on the company, and no credible evidence is shown establishing the likelihood that, absent the requested order, the producing party will not produce all relevant information during

---

102. Offline data sources refer to those sources of data that are no longer active in the sense that they cannot be readily accessed by a user on the active computer system. Examples of offline data sources include backup tapes, floppy diskettes, CDs, DVDs, portable hard drives, ROM-drive devices, etc.

103. *Mansfield v. Ottawa*, 2012 ONSC 5208 (CanLII) at para 43.

104. Martin Felsky & Peg Duncan, *Making and Responding to Electronic Discovery Requests*, *LawPRO Magazine* (September 2005), online: <http://www.lawpro.ca/LawPRO/ElectronicDiscoveryRequests.pdf>.

> discovery.[105] The company should be permitted to continue the routine recycling of backup tapes in light of the expense, burden and potential complexity of restoration and search of the backup tapes.
>
> *Illustration ii.* An employee was dismissed for cause from a company. Three months later, the former employee sues for wrongful dismissal. During the search for information relevant to the matter, counsel learns that the IT department routinely deletes user inbox e-mails older than 30 days in an effort to control the volume of e-mail on their mail servers. The tape from the last backup of the month is kept for a year before being returned to the backup tape recycling pool. As part of the preservation plan, the backup tapes that are three months and older are retrieved and safeguarded; counsel reasons that tapes used in the daily pool need not be preserved since the evidence they are seeking is at least 90 days old. This is a reasonable position to take. The backup taken just after the employee left is restored and e-mails advancing the employer's case and damaging the plaintiff 's are found.

Finally, if it is unclear whether there are unique, relevant data contained on backup media, the parties or the Court may consider the use of sampling to better understand the data at

105. See *Apotex Inc. v. Merck & Co. Inc.*, 2004 FC 1038 (CanLII) at para 14: "It is clear that the burden of showing that Merck's production is inadequate lies on Apotex, who made that allegation. Apotex must show that documents exist, that they are in the possession or control of Merck and that the documents are relevant."

issue. Sampling will help establish the degree to which potentially relevant information exists on the tapes in question and the likely cost of the retrieval of such information. Consequently, sampling may lead to the informed retention of some, but not all, of the backup media.

> *Illustration iii.* In the course of a search for relevant e-mails belonging to a custodian who left the company's employ a number of years ago, the company discovers that IT has kept the last e-mail backup tape of the week for the past ten years. The backup tapes carry labels with the date of the backup and the server name; however, IT does not have a record of which accounts were stored on which servers. The events happened over a six-month period and the party determines that if there were e-mails, they should most likely appear in the middle of the period. Therefore, it would be reasonable for the company to sample the backup tapes that were labeled with the date in the middle of the range. If a backup of a particular server did not contain e-mails of the custodian, the backups for that particular server could be excluded from further searches.

Comment 3.j. Preservation of Shared Data

A party's networks or intranet may contain shared areas (such as public folders, discussion databases and shared network folders) that are not regarded as belonging to any specific

employee. Such areas should be identified promptly and appropriate steps taken to preserve shared data that is potentially relevant.[106]

> *Illustration i.* Responding to a litigation hold notice from in-house counsel, custodian X identifies the following sources of data relevant to an engineering dispute that she has in her possession or control: e-mail, word-processing and spreadsheet files on her workstation and on the engineering department's shared network drive, as well as a collection of CD-ROMs with relevant data and drawings. Following up on her response, counsel determines that custodian X also consults engineering department knowledge management databases, contributes to company wikis and discussion groups and is involved in online collaborative projects relevant to the dispute. Although custodian X does not consider herself to be in possession or control of these additional sources, counsel should work with the IT department to include these in the preservation process.

Principle 4. Counsel and parties should cooperate in developing a joint discovery plan to address all aspects of discovery and should continue to cooperate throughout the discovery process, including the identification, preservation, collection,

106. *Drywall Acoustic, supra* note 85 at paras 111–112.

processing, review and production of electronically stored information.

Comment 4.a. The Purpose of Discovery Planning

The purpose of discovery planning[107] is to identify and resolve discovery-related issues in a timely fashion and to make access to justice more feasible and affordable. The process is not intended to create side litigation.[108] Cooperation includes collaboration in developing and implementing a discovery plan to address the various steps in the discovery process. These will include some or all of the following steps: the identification,

107. It has been common to refer to the "meet-and-confer" process, or to say that the parties will "meet-and-confer" or attend a specific "meet-and-confer" session. While this Commentary will still use this term, the point is not that there must be one or more meetings; the emphasis should be on conferring with a view to reaching meaningful agreement on a discovery plan.

108. *Drywall Acoustic*, *supra* note 85 at paras 81–84.

preservation, collection and processing of documents;[109] the review and production of documents;[110] how privileged documents are to be handled or other grounds to withhold evidence; costs; and protocols.

While the original *Principles* primarily discussed the "meet-and-confer" process, the Canadian collaborative experience has developed more significantly around the principle of ongoing cooperation and the development of a discovery plan. The idea of cooperation between counsel and parties extends well beyond the confines of a meeting, or series of meetings, to transparent sharing of information in an effort to keep discovery costs proportionate and timelines reasonable. Accordingly, based on the universal consensus of the participants in The Sedona Conference Working Group 7 August 2014 Meeting in Toronto, the language in these *Principles* has moved towards "cooperation" and "collaboration" in lieu of the more restrictive "meet-and-confer" term.

---

109. "Processing" means "an automated computer workflow where native data is ingested by any number of software programs designed to extract text and selected metadata and then normalize the data for packaging into a format for the eventual loading into a review platform. [It] [m]ay also entail identification of duplicates/de-duplication." The Sedona Conference, *Glossary: E-Discovery & Digital Information Management* (April 2014), *supra* note 9. Processing can also involve steps to deal with documents that require special treatment, such as encrypted or password-protected files. Parties should avoid making processing decisions that have consequences for others without first discussing those decisions. An effective discovery plan will address issues such as the means of creating hash values, whether to separate attachments from e-mails and which time zone to use when standardizing DateTime values.

110. Parties may consider adopting a staged or phased approach to e-discovery where appropriate due to the volume of evidence. Parties should also agree as early as possible on production specifications.

A successful discovery plan will ensure that the parties emerge with a realistic understanding of what lies ahead in the discovery process. To address the increasing volumes of ESI and the high costs of litigation, these *Principles* strongly encourage a collaborative approach to e-discovery, reflecting recent judicial opinions and attitudes in Canada and other countries.[111] "Common sense and proportionality" have been described as the driving factors of discovery planning.[112]

In Ontario, the *Rules of Civil Procedure* were amended in 2010 to require the parties "to agree to a discovery plan in accordance with [Rule 29.1]."[113] The development of a meaningful

111. *Wilson v. Servier Canada Inc.*, 2002 CanLII 3615 (ON SC) [*Servier*] at paras 8–9: "The plaintiff's task in seeking meaningful production has been made particularly difficult by the defendants' general approach to the litigation. On the simple premise, as expressed by the defendants' lead counsel, that litigation is an adversarial process, the defendants have been generally uncooperative and have required the plaintiff to proceed by motion at virtually every stage of the proceeding to achieve any progress in moving the case forward. I take exception to this. In contrast with other features of the civil litigation process in Ontario, the discovery of documents operates through a unilateral obligation on the part of each party to disclose all relevant documents that are not subject to privilege. The avowed approach of the defendants' counsel is contrary to the very spirit of this important stage of the litigation process." See also *Sycor Technologies v. Kiaer,* 2005 CanLII 46736 (ON SC). In dispute was the form of production in a case where just the cost of printing e-mails was going to be $50,000 or so. The Court indicated that "procedural collaboration and a healthy dose of pragmatism and common sense" were required, and sent counsel back to work out an efficient method of production in accordance with the Ontario Guidelines.

112. *Drywall Acoustic*, *supra* note 85 at para 84.

113. *Rules of Civil Procedure*, RRO 1990, Reg 194, r 29.1.03(3) states that the plan shall include:

discovery plan requires meaningful and good-faith collaboration and information sharing between the parties that is proportionate and relevant to the nature of the individual action. Additionally, there is an ongoing duty to update the discovery plan as required.

In Quebec, the modifications to the *CCP* introduced the notion of cooperation by requiring the parties to agree on the conduct of the proceeding before the presentation of the introductory motion. A new chapter regarding case management was added to the *CCP* to ensure that parties take control of their case in accordance with the new section 4.1 *CCP*.[114]

To be effective, the discovery plan must be a "meeting of the minds" regarding the discovery process. The end result should be to reach agreement on a written discovery plan. This

---

> a) the intended scope of documentary discovery under rule 30.02, taking into account relevance, costs and the importance and complexity of the issues in the particular action;
>
> b) dates for the service of each party's affidavit of documents (Form 30A or 30B) under rule 30.03;
>
> c) information respecting the timing, costs and manner of the production of documents by the parties and any other persons;
>
> d) the names of persons intended to be produced for oral examination for discovery under rule 31 and information respecting the timing and length of the examinations; and
>
> e) any other information intended to result in the expeditious and cost-effective completion of the discovery process in a manner that is proportionate to the importance and complexity of the action.

114. CQLR c C-25, s 151.1–151.23.

is a best practice whether or not such a plan is prescribed by the rules of court of the applicable jurisdiction.[115]

The planning process may vary greatly, depending upon the scope and nature of the action. For example, a modest straightforward action may require a discovery plan that consists of a few paragraphs developed via telephone call or e-mail exchanges between counsel. A more complex case may require a series of in-person meetings and a more comprehensive plan.[116] Counsel should decide in each individual case what sort of meeting and discovery plan will be appropriate. Factors to be considered will include, but not be limited to: the amount at stake in the action, the volume and complexity of the electronic evidence to be exchanged, the location of counsel and other issues relevant to the discovery process.

An Ontario Court has held that "[t]he interplay between the *Rules of Civil Procedure*, Rules of Professional Conduct, Principles of Civility and Professionalism and the relatively new requirement for formal discovery planning is important."[117] The Courts have criticized counsel for failing to create a discovery plan, and have in some cases sanctioned counsel conduct using cost rules.[118]

---

115. For a sample discovery agreement and other model documents, see OBA, Model Precedents, *supra* note 70.

116. *Enbridge Pipelines Inc. v. BP Canada Energy Company*, 2010 ONSC 3796 at paras 3–4 (CanLII) (C. Campbell J.). The Court endorsed a discovery plan in a complex piece of litigation, but emphasized that not every case would require this level of detail.

117. *Kariouk v. Pombo*, 2012 ONSC 939 (CanLII) [*Kariouk*] at para 3, see also paras 55–56.

118. *Corbett v. Corbett*, 2011 ONSC 7161 (CanLII) [*Corbett*]; *Petrasovic Estate v. 1496348 Ontario Ltd.*, 2012 ONSC 4897 (CanLII) [*Petrasovic*]; *Siemens*,

Comment 4.b. Confer Early and Often

Parties should confer early in the litigation process and thereafter as appropriate. The first contact should take place as soon as possible after litigation has commenced and in any event prior to the collection stage. The parties should, at a minimum, confer as soon as the pleadings have closed to ensure the scope of the required collection is known.

While parties may have taken many, if not all, of the steps necessary to preserve potentially relevant information by the time they confer, there may be additional preservation issues for discussion. For example, if additional custodians are added to the list, or if timelines are agreed upon that are broader than originally anticipated by the parties, additional preservation steps will be required.

Meeting early is one of the keys to effective e-discovery. Decisions made about e-discovery from the earliest moment that litigation is contemplated will have serious impact on the conduct of the matter, not to mention the potential cost of discovery. Opening up discussion and debate on ESI early in the process avoids subsequent disputes, which may be costly and time consuming.

> *Illustration i*. A manufacturer defending a product liability claim issues a litigation hold to the operations division, captures the hard drives and server e-mail of twelve production managers and uses a long list of search terms drafted by in-house counsel to cull the data. Outside counsel spend six months reviewing the data before it is produced, almost a year after the litigation was launched.

---

supra note 46; 1414614 *Ontario Inc. v. International Clothiers Inc.*, 2013 ONSC 4821 (CanLII) [*International Clothiers*].

> The receiving party now argues that (a) all data from the marketing department relating to the defective product should also have been preserved; (b) there are eight additional managers, four of whom have since left the company, whose e-mails should have been preserved and reviewed; (c) the list of search terms is demonstrably too narrow according to its e-discovery expert; and (d) backup media containing highly probative evidence should have been restored because active end-user e-mail stores are purged every 90 days in accordance with the company's records management policy. If the parties had met at the beginning of the process many of these issues could have been addressed and dealt with in the discovery plan.

A single meeting will not be sufficient for the development of an appropriate discovery plan in some cases. Accordingly, Principle 4 envisions not just a single meeting but an ongoing series of discussions.[119] Those ongoing discussions assist counsel when they encounter unanticipated technical issues. In

119. See e.g. *L'Abbé, supra* note 51 at para 31, in which the Master held: "First and foremost, when dealing with vast numbers of documents, particularly electronically stored information, the parties ought to be devising methods for cost effectively isolating the key relevant documents and determining claims of privilege. To the extent that there is disagreement about the scope of relevance or privilege, it may be necessary to obtain rulings from the court but the onus is on counsel to jointly develop a workable discovery plan and to engage in ongoing dialogue." See also *Kaymar v. Champlain CCAC*, 2013 ONSC 1754 (CanLII) at para 37 (M. MacLeod) [*Kaymar*], in which the Master stated his view that discovery plans should be flexible. "In a perfect world, the discovery plan would be a living breathing process, modified, adapted and updated as necessary."

some situations, the volume of data to be collected and reviewed is underestimated, and search criteria used to cull the collection may need to be reviewed and adjusted if results are not sufficiently precise or relevant. These developments should be communicated to all parties. Absent such communication, any agreement reached through initial cooperation can easily evaporate.

As one Court has stated, "[t]he obligation to engage in discovery planning includes an obligation to confer at the outset and to continue to collaborate on an ongoing basis in order that the plan may be adjusted as necessary."[120] This obligation does not disappear because there is an order of the Court regarding discovery.[121]

Comment 4.c. Preparation for Planning

Counsel should participate in the planning process in good faith and come prepared to discuss several key issues in a substantive way. Those issues include identifying the sources of potentially relevant ESI, the steps to be taken for preservation and the methodology to be used to define and narrow the scope of the data to be reviewed and produced.

Depending on the nature of the discovery project and the scope of the litigation, preparation should also include collecting information from knowledgeable people within the client organization. These people may include a business manager or managers familiar with the operational or project areas involved in the litigation and the key players in the organization, someone familiar with the organization's document and records

120. *Kariouk, supra* note 117 at para 42.

121. *International Clothiers*, *supra* note 118 at para 20.

management protocols and the IT manager or managers familiar with the organization's network, e-mail, communication and backup systems. These individuals may also attend the discovery plan meeting(s) where appropriate. (See Comment 4.d. below).

Ideally, a written agenda should be prepared that sets out the key issues for discussion for the development of the discovery plan. Topics for the discovery plan meeting agenda will commonly include:

Comment 4.c.i. Identification

To prepare for the discovery plan meeting in a meaningful way, counsel should consult with IT staff, outside service providers, users and others to gain a thorough understanding of how ESI is created, used and maintained by or for the client, and to identify the likely sources of potentially relevant ESI.[122]

Comment 4.c.ii. Preservation

In developing the discovery plan, parties should discuss what ESI falls within the scope of the litigation and the appropriate steps required to preserve what is potentially relevant. If unable to reach a consensus the parties should apply on an ur-

122. See *Canada (Commissioner of Competition) v. Air Canada (TD)*, [2001] 1 FC 219 at para 27, 2000 CanLII 17157 (FCTD): "Counsel for the Commissioner noted that, at the time the Commissioner sought the section 11 order, he did not know what the record-keeping practices of Air Canada were. Counsel indicated that insofar as there were real difficulties in responding to the requests, as a result of the form in which they had been asked, this should be the subject of discussion between counsel, before the Court was asked to adjudicate further on it. That aspect of Air Canada's present motion was therefore set aside to allow for such discussion."

gent basis for court direction, or at the very latest after the delivery of pleadings, to ensure that relevant information is not destroyed.

While making copies of hard drives is useful in selective cases for the preservation phase, the processing of the contents of the hard drives should not be required unless the nature of the matter warrants the cost and burden.[123] Making forensic image backups of computers is often not required and should be discussed. Engaging in this process can divert litigation into side issues involving the interpretation of ambiguous forensic evidence. The key is for counsel to agree on reasonable, proportionate steps to ensure potentially relevant information is available for production.

Comment 4.c.iii. Collection and Processing

The parties should also discuss the steps they will take to narrow the potentially relevant information to a smaller set that is reasonable and proportionate in the context of the lawsuit. Typical selection criteria used to narrow the scope of the ESI include the names of key players, timelines, key data types, key systems (e.g. accounting), de-duplication and search terms. Every effort should be made to discuss and agree on these issues.

---

123. *Janzen*, *supra* note 55 at para 1: "This is an application to compel the defendant to produce a Supplemental List of Documents, listing his hard disk drives (HDD) and a mirror image copy of those hard disk drives as documents in its possession. The plaintiff wants the mirror-image HDD produced to its own computer expert for a computer forensic analysis;" and at para 36: "Without some indication that the application of the interesting technology might result in relevant and previously undisclosed documents, the privacy interests of the third parties and the avoidance of unnecessary and onerous expense militate against allowing such a search merely because it can be done."

Parties and counsel should agree on (1) the use of selection criteria as a means to extract targeted, high-value data; (2) the type(s) and form(s) of selection criteria to be used; (3) a process for applying the agreed-upon selection criteria; (4) specific search terms that will be used; and (5) a protocol for sharing and possibly adjusting the criteria. Absent such agreement, parties should be prepared to disclose the parameters of the search criteria that they have undertaken and to outline the scope of what they are producing and what sources or documents have not been searched.

Comment 4.c.iv. Review Process

Issues for discussion in connection with the review stage will include: the scope of the review; whether it will be conducted manually or with the assistance of electronic tools such as concept-clustering or predictive coding technologies; and the methods to be used to protect privileged, personal and confidential information and/or trade secrets. For more information, The Sedona Conference has published a Commentary on search and retrieval methods and technologies.[124]

Comment 4.c.v. Production

Counsel should discuss the form in which productions will be exchanged—for example, whether certain document types will be in native format (commonly used for PowerPoint presentations and Excel spreadsheets) or static images. Counsel would benefit from a detailed discussion even where source documents are in paper form, or where, as is commonly the

124. The Sedona Conference, *Best Practices Commentary on the Use of Search and Retrieval Methods in E-Discovery* (2013), 8 Sed. Conf. J. 189, online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/3669>.

case, source documents exist in both hard copy and digital format.[125] Early agreement on production specifications can save significant time and expense later in the process. Involving service providers in these discussions early in the process can help to avoid delays, mistakes and re-work.

Comment 4.c.vi. Timing

Counsel should discuss the schedule and timing for the processing, review and production of ESI and should also address the need for additional discussions throughout the matter and a resolution process for any issues that may arise.[126] [127]

125. *Logan v. Harper*, 2003 CanLII 15592 (ONSC) [*Logan*] at para 66: "Before indexing and scanning the documents, it would be useful for the parties to discuss how the documents are to be identified and organized and to agree upon the electronic format for the documents. If the parties can agree on a mutually acceptable system it may well save time, cost and confusion. It may be that Health Canada has an indexing and identification system that it would be appropriate to adopt."

126. See *Kaymar, supra* note 119 at paras 37–38 (M. MacLeod), in which the Master expressed his preference that discovery plans contain a "sophisticated non adversarial process" for dispute resolution. Although acknowledging the central role of courts in adjudicating disputes and supervising the discovery phase of cases, he stated: "A well-crafted plan should minimize the need for court intervention and utilize adversarial adjudication as a last resort. A contested motion with court inspection of disputed documents is inherently a cumbersome and expensive way to resolve discovery disputes."

127. In *2038724 Ontario Ltd. v. Quiznos Canada Restaurant Corp*., 2012 ONSC 6549 (CanLII) (Justice Perell) at paras 129-130 [*Quiznos*], the Court ordered a party to reproduce documents in Excel format despite the fact that the discovery plan had agreed that productions would be exchanged in TIFF. The Court found that there would be no hardship or difficulty in providing the documents in native format; and, that while important, discovery plans can be modified.

The preservation, collection, processing, review and production steps are considered in greater detail in Principles 3, 5, 6, 7 and 8.

Comment 4.d. Who Should Participate

In the e-discovery context, the development of a discovery plan is like any business planning meeting: if the right people are at the table, the agenda is set out in advance, the participants are prepared and the decisions are recorded and followed up upon, then the meeting will have a greater likelihood of success. Multi-party and class actions in particular need to have involvement from different points of view. Even if no in-person meetings take place, the same principles apply: clear objectives, good record-keeping, open communication and meaningful follow-up.

In many cases, each party involved in discovery planning may benefit from the participation of an e-discovery advisor with experience in the technical aspects of discovery, especially where complex technology, legacy systems or database information may be issues.

Principle 4 suggests that counsel and parties should both be involved, since matters to be addressed are not limited to legal issues alone. Although discovery planning should take place within the context of substantive and procedural law, important considerations may arise that are almost certain to be beyond the range of counsel's expertise. This is not a task to be delegated to junior lawyers. Given the nature and implications of a discovery plan, it is valuable to have senior counsel involved in these discussions.

In many cases, clients should also participate. The client will be able to state upfront what information is available, and in what format. Further, having the client involved increases the

openness of the process. The person who has best knowledge of the relevant data sources and systems should be present or at least consulted before the parties agree to a discovery plan.

In cases involving financial loss or evidence, the courts have suggested that the accountants participate in the planning process so that the disclosure could be targeted to what was actually needed by the parties to prove their case.[128]

Comment 4.e. Good-Faith Information Sharing to Facilitate Agreement

As stated above, an effective discovery planning process requires a meeting of the minds. The purpose is to facilitate proportionate discovery, not to create roadblocks. Open and good-faith sharing of relevant information is required for this purpose.

Discovery planning discussions are generally held on a "without prejudice" basis to facilitate the required level of openness. Once the discovery plan is signed, it becomes a "with prejudice" agreement.

The types of information properly exchanged during discovery planning are not privileged. These types of information include: search terms,[129] names of custodians, systems from which information will be retrieved and the e-discovery process developed by the parties for use in the case. Further, describing discovery processes does not disclose trial strategy or limit counsel from being strong advocates for their clients' interests. Instead, it ensures a defensible framework inside which the case can proceed. Once the discovery plan is agreed upon, counsel

128. *International Clothiers Inc., supra* note 118.

129. If search terms include terms that may be considered trade secrets, only then would they be excluded, on grounds of confidentiality.

can focus on the substantive aspects of and strategies for their case.

Accordingly, parties should describe the methodology they are employing for their case, including any steps they are taking to validate their results. If objections are raised to the validity or defensibility of the proposed process, the objections should be dealt with at the earliest possible stage. This level of openness ensures the discovery plan is meaningful and defensible at the earliest possible stage, potentially saving the clients the time, money and aggravation of having to re-do discovery processes at a much later date.

In cases where the parties (or a party) resist sharing relevant information or refuse to engage in the discovery planning process at all, counsel may consider sending a draft discovery plan to opposing counsel with a time line for agreement on its terms. If no response is received, the draft discovery plan may form the subject matter of a motion for court approval.[130]

Comment 4.f. Consequences of Failing to Cooperate

The courts have criticized counsel for failing to meet their obligations, referring to the "interplay between the Rules of Civil Procedure, Rules of Professional Conduct, Principles of Civility and Professionalism and the relatively new requirement for formal discovery planning."[131]

While the courts have confirmed a party may apply to the courts for a discovery plan when agreement cannot be reached, this is not intended to allow counsel to abdicate their

130. Courts have exercised their ability to impose discovery plans. See e.g. *Ravenda v. 1372708 Ontario Inc.,* 2010 ONSC 4559 (CanLII), and *TELUS Communications Company v. Sharp,* 2010 ONSC 2878 (CanLII).

131. *Kariouk, supra* note 117 at para 3.

responsibility to cooperate and draft a plan.[132] A risk all parties face when reliant on the courts for a discovery plan is that they lose control over the decision-making process and the courts may not be in a better position to determine the most appropriate plan.[133]

The parties continue to have an ongoing obligation to confer and make adjustments and disclosures where necessary.[134] Adverse cost consequences are a serious risk in discovery motions for parties who fail to act reasonably or fail to meet their obligations.[135] In Nova Scotia, the failure to come to an agreement on electronic disclosure results in the default provisions of Civil Procedure Rule 16, which include an obligation to perform all reasonable searches, including keyword searches, to find relevant electronic information.[136]

Principle 5. The parties should be prepared to produce relevant electronically stored information that is reasonably accessible in terms of cost and burden.

Comment 5.a. Scope of Search for Reasonably Accessible Electronically Stored Information

The primary sources of ESI in discovery should be those that are reasonably accessible. Typically this includes e-mails and electronic files (such as Word, PowerPoint and Excel documents) that can be accessed in the normal course of business.

132. See *Siemens, supra* note 46 at paras 79–84.

133. *Siemens, supra* note 46.

134. *International Clothiers Inc., supra* note 118; *Siemens, supra* note 46.

135. *Corbett, supra* note 118; *Petrasovic, supra* note 118; *Siemens, supra* note 46.

136. *Velsoft, supra* note 14.

Parties should be prepared to produce relevant ESI that is "reasonably accessible" in terms of cost and burden.

Whether ESI is "reasonably accessible" requires an assessment of the following issue: will the quantity, uniqueness or quality of data from any particular type or source of ESI justify the cost of the acquisition of that data? Essentially, it is a cost-benefit analysis. Certain forms of ESI—such as old backup tapes, data for which applications no longer exist, information that was available on old web pages and information in databases—are often assumed to be "not reasonably accessible" simply because they are more difficult to deal with than other data forms. This is not always the case.

To enable the Court to perform that cost-benefit analysis, counsel will be required to provide clear information on the types of media that will need to be searched (e.g. backup tapes, microfiche, etc.), the status of the media and its condition (e.g. media that is in a damaged state, media stored in boxes, etc.) and the likelihood of retrieving data from the media in a useable form. The Court may require expert evidence on all of the above points as well as the costs associated with the retrieval of the data and the time required for the data retrieval. It is not sufficient for the party resisting production to simply argue that it is expensive.

Recent cases show that Canadian courts have been aware of the need for this cost-benefit analysis. For example, in *Murphy et al v. Bank of Nova Scotia et al*,[137] the Court considered the plaintiff's request that additional e-mail information contained in backup tapes be produced by the defendant bank for a period of almost three years. The defendant argued this would cost be-

137. 2013 NBQB 316 (CanLII).

tween $1.2 million (for 13 employees) and $3 million (for 33 employees). The Court noted that ". . . the burden, cost, and delay of the production must be balanced against the probability of yielding unique information that is valuable to the determination of the issues. Counsel for the plaintiffs made reference to a possible 'smoking gun' that could exist in one of the many e-mails authored by [the bank's] employees. This is way too speculative." In the end, the Court ordered that the e-mails from only four employees be retrieved for a period of just over one month.

In *Hudson v. ATC Aviation Technical Consultants*,[138] the Master ordered the appellants—manufacturers of an airline engine identified as one of the causes of a fatal airline crash—to produce 39 years of documents concerning 15 parts and over 50 models, some of which were not even at issue in the lawsuit. The appellants appealed on the ground that the request was disproportionate and excessive. The Court held that the documents were relevant, not just to show that the defendants had a propensity to manufacture improperly, but to show that they knew of issues with similar systems that were probative of what it knew, did and said in relation to the engine and accident in this case. The appellants filed no evidence as to how accessible the data was. The Court held that absent evidence from the appellants demonstrating the hardship incurred in producing the records sufficient to counterbalance the relevancy and discretionary factors, the production order would stand.

Where the Court determines that the efforts to obtain the data do not justify the burden, it will exercise its discretion to

138. *ATC Aviation*, *supra* note 69.

refrain from ordering production of relevant documents. For example, in *Park v. Mullin*,[139] the Court noted that in the past it has "used its discretion to deny an application for the production of documents in the following circumstances: (1) where thousands of documents of only possible relevance are in question . . .; and (2) where the documents sought do not have significant probative value and the value of production is outweighed by competing interests, such as confidentiality and time and expense required for the party to produce the documents. . . ."

Owing to the volume and technical challenges associated with the discovery of ESI, the parties should engage in the above cost-benefit analysis in every case—weighing the cost of identifying and collecting the information from each potential source against the likelihood that the source will yield unique, necessary and relevant information. The more costly and burdensome the effort to access ESI from a particular source, the more certain the parties need to be that the source will yield relevant information. However, the fact that an organization does not proactively manage its information or has poor information governance practices should not itself operate in support of any argument that it should not be compelled to produce due to undue burden or cost in complying with its discovery obligations.[140]

A production request pertaining to an ESI source that is determined to be "not reasonably accessible" must be justified by showing that the need for that particular data outweighs the

139. 2005 BCSC 1813 (CanLII).

140. See e.g. Master Short's decision in *Siemens*, *supra* note 46 at paras 136–138, and 156, where he states that Sapient's e-mail retention policy which deletes e-mails after 30 days can cause serious problems, and ordered Sapient to restore and search backup tapes, despite counsel's argument that such an Order would be disproportionately costly.

costs involved.[141] Information that is otherwise relevant may be excluded on the grounds that recovery of that information involves an inordinate amount of time or resources which are not commensurate with the potential evidentiary value.[142]

Parties and courts should exercise judgment based on reasonable good-faith inquiry, taking into consideration the cost of recovery or preservation. If potentially marginally relevant documents are demanded from sources for which the information is difficult, time-consuming or expensive to retrieve, cost shifting may be appropriate.

In some jurisdictions, particularly where case management is available, a party may apply for directions regarding its discovery obligations. Seeking advance guidance may avoid a contentious after-the-fact dispute where the onus may lie on the producing party to demonstrate why it did not initially produce the requested information.

> *Illustration i.* In an employment case, the plaintiff employee claims to have received abusive e-mail from his supervisor as part of an ongoing pattern of harassment. The employee claims that the e-mail would have been sent 18 months ago. There are no backup tapes from the period and the plaintiff did not keep any copies. The employer company has imaged the workstation and conducted a thorough search of all e-mail folders, including

141. *Descartes v. Trademerit*, 2012 ONSC 5283 (CanLII); *GasTOPS Ltd. v. Forsyth*, [2009] OJ No 3969 (CanLII).

142. *R. v. Mohan*, [1994] 2 SCR 9, as quoted in *Gould Estate v. Edmonds Landscape & Construction Services Ltd.*, 1998 CanLII 5136 (NSSC), 166 NSR (2d) 334.

the deleted items folder, but the e-mail was not located. The plaintiff asks the Court to order a forensic examination of the computer to recover the deleted information. In the absence of any evidence from the plaintiff as to the existence of the abusive e-mail, the Court accepts the defendant's argument that the probability of finding traces of an e-mail that was deleted 18 months ago from a workstation that is in daily active use is negligible as the space on the disk would have been overwritten in the normal course of business.

Illustration ii. An unsuccessful bidder on a municipal government's request for proposals (RFPs) for a multi-million dollar construction contract alleges unfairness and impropriety. The final report of the evaluation committee was in printed format. The plaintiff alleges that the criteria used to compare the bids were changed during the evaluation. The plaintiff asks for the electronic version of the selection criteria that, according to the municipal government's RFP policy, must be determined before the RFP is released. The plaintiff explains that this document is material and necessary to its prosecution of the case. It has, however, been three years since the competitive tender, and due to staff turnover, the electronic version has been lost. However, a backup copy on the server used by the former contracts officer is available and can be recovered. Since the backup copy would be the only source for a piece of critical information in the suit, the Court orders the recovery of the electronic version from the server.

Comment 5.b. Outsourcing Vendors and Other Third-Party Custodians of Data

Many organizations outsource all or part of their information technology systems or share ESI with third parties for processing, transmitting or for other business purposes. Cloud storage is one example of this type of arrangement. In contracting for such services, organizations should consider how they will comply with their obligations to preserve and collect ESI for litigation. If such activities are not within the scope of contractual agreements, costs may escalate and necessary services may be unavailable when needed. Parties to actual or contemplated litigation may also need to consider whether preservation notices should be sent to non-parties, such as contractors or vendors.

Principle 6. A party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual electronically stored information that has been deleted in the ordinary course of business or within the framework of a reasonable information governance structure.

If ESI has been deleted in the ordinary course of business or within the framework of a reasonable, defensible information governance structure and is no longer easily accessible, then a party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual ESI. The need to identify, preserve and collect this type of data will be rare. While deleted or residual ESI may be required in any case, it is more likely to be relevant in criminal cases or those involving fraud.

As noted above, it is important to note that just because data has been deleted does not automatically mean that the data is difficult to access. Further investigations need to be made to validate that determination. For example, in some cases files that have been deleted remain readily retrievable from a party's computer system without any special expertise. In those cases, the courts are more likely to order production.[143]

Whether a court will order the production of deleted or residual ESI that is not easily accessible is a case-by-case determination. Courts will consider a number of factors including,

143. See *Low, supra* note 55 where the Court refused to order a forensic analysis of the plaintiff's hard drive for files that may have been deleted because of the significant costs and limited probative value of the files requested. The Court did, however, order that the plaintiff search for relevant files that had been deleted but which were still readily retrievable by using the computer's operating system.

but not limited to, the principle of proportionality, proof of intentional destruction of data and the scope of the search.

In *Holland v. Marshall*,[144] the plaintiff's hospital records had been destroyed. However, at the time the records were destroyed, the hospital had a policy in place to destroy adult records after the lapse of 11 years. The Court found that before the plaintiff's records were destroyed, litigation was not threatened nor reasonably apprehended by the hospital or any of the other defendants.

In *Patzer v. Hastings Entertainment Inc.*,[145] the plaintiff had deposited a number of betting slips into an automated gaming machine at the Hastings Park Racecourse in Vancouver. The plaintiff received from the machine a cash voucher in the amount of $6.5 million. The defendant refused to honour the voucher on the grounds that it was issued in error. The plaintiff sought production of a number of documents, including the betting slips. The standard practice at Hastings Park was that the betting slips were purged from each automatic machine on a weekly or bi-weekly basis and then sent out for recycling. When the documents were destroyed there was no evidence that the plaintiff was contemplating litigation. The Court held that the documents were destroyed in the ordinary course of business and there was no basis to apply the doctrine of spoliation.

> *Illustration i.* A plaintiff seeking production of relevant e-mails demands a search for e-mails deleted by the defendant during the normal course of business. The e-mails are not easily accessible. The plaintiff has not provided any justification or evidence that would suggest a particular need for

144. *Holland v. Marshall*, 2008 BCCA 468.

145. *Patzer v. Hastings Entertainment Inc.*, 2011 BCCA 60.

the deleted e-mails. The request would likely be denied by the Court as the production request is not proportionate; parties are not typically required to search the trash bin outside an office building after commencement of litigation.

Illustration ii. A defendant in a lawsuit has an existing information governance structure that set out that e-mails would be kept for 2 years. A lawsuit is brought, and the plaintiff requests e-mails going back 3 years. On a motion, the defendant explained the rationale for its 2 year e-mail retention policy and the costs involved in retrieving older e-mails from backup tapes. The Court holds that the defendant had a reasonable information governance structure and is not required to provide e-mails older than 2 years old.

Principle 7. A party may use electronic tools and processes to satisfy its documentary discovery obligations.

Comment 7.a. Greater Accuracy, Efficiency and Cost Control Through the Effective Use of Technology

Modern e-discovery tools have progressed to the point where virtually every phase of e-discovery can be made more accurate (in terms of the quality of the results), more defensible (in terms of the processes involved), more efficient (in terms of resources), more speedy and even more cost-effective than in the past.[146]

146. It is likely that not all of these benefits can be enjoyed at the same time; the normal trade-offs among speed, resource efficiency, overall cost and quality will still exist. However, there have been many reports of large

Parties who deploy appropriate technology at the right stages of the discovery lifecycle and as part of well-planned and well–managed processes, can in many cases achieve all three of "faster, better, cheaper." In many situations they can expect to spend less time and money than in the recent past while arriving at production sets that contain a higher proportion of the relevant documents that existed in the initial population (higher "recall") while also handing over fewer nonresponsive documents than were traditionally included in productions (higher "precision").[147] These tools also offer the significant benefit of bringing the most important documents to the fore much earlier in the project. The following sections discuss the most important uses of technology to achieve greater accuracy, efficiency and savings.

Comment 7.b. Appropriate Technology Within a Defensible Process

Tools must be chosen with a view to their reliability. Ultimately, the reliability of the entire production process is dependent on both the intelligent application of the appropriate tools and the process put into place. Put another way, it is imperative to develop and implement a defensible process. Any party that relies on technology to assist with the determination of relevance or privilege should ensure that the technology is

---

complex e-discovery projects in which the effective use of appropriate technology has made the process faster, better *and* cheaper than traditional linear review by teams of lawyers. What may seem like an added cost at the start of a project, e.g. for processing or analytics, can be the means of achieving better results and saving even greater amounts—and weeks or months of review time—later in the project.

147. For a full discussion of "recall" and "precision," see *infra*, Comment 7.d.

able to do what it says it can do, and can do so reliably. Parties may need to consult an expert on this issue if appropriate.

Where possible, parties should agree in advance on (1) the scope of data to be searched; (2) the use of de-duplication software to remove "true" duplicate documents; (3) the search tools to be used (e.g. search terms, concept searching, predictive coding); and (4) the method for validating the results. Absent such an agreement, parties should document for the Court the process and methodology used, including decisions to exclude certain types or sources of documents, in the event the approach taken is questioned.

Comment 7.c. Techniques to Reduce Volume

No matter how targeted and selective a party may be in identifying, preserving and collecting data, the majority of the ESI collected is likely to be irrelevant or only marginally relevant. It can therefore be impractical or prohibitively expensive to review all the information. Parties should therefore consider and discuss the use of appropriate technology throughout the discovery process.[148]

As new technologies emerge, parties should assess them and (and with the advice of experts, where appropriate) continue to embrace them. That being said, the most effective way to keep volumes of data as modest as possible is to maintain good, defensible information governance processes.[149]

---

148. Smaller volume collections may also benefit from the application of technology. Providing that the process is efficient and proportionate, there can be a significant return on investment for the use of technology instead of a completely manual review.

149. For discussion of Information Governance, see *supra*, Comment 3.b.

Comment 7.c.i. Data Metrics Report

When dealing with electronic records, a "data metrics" report can be created before data is collected and can be a useful tool to limit the collection of irrelevant documents. It can also be used after data collection (and is also useful for removing irrelevant documents at that point). A data metrics report provides information such as the types of file extensions in the data, the dates of the documents, custodians and file organization. This information can be used to eliminate categories of unnecessary data.

Collecting information and understanding the nature of the data as early as possible is a best practice. There are many new tools that provide highly sophisticated reports that will quickly allow counsel and their technical advisors to understand and assess a collection of information.

> *Illustration*. If photographs are not relevant to a case, the volume of digital photographs within a collection can be ascertained immediately, and a decision can be made to automatically identify and remove these records prior to processing or review.

Comment 7.c.ii. Duplicate Documents

Sources of ESI often include multiple copies of the exact same, or nearly the same, document or e-mail. There are electronic tools available to limit the volume of these types of documents.

a) De-Duplication

De-duplication or "de-duping" refers to a process of identifying exact duplicate[150] e-mails or other computer files and setting aside the copies. Depending on the case, de-duplication can save considerable amounts of time and money. In most cases, it will be appropriate to eliminate exact duplicates.

> *Illustration.* A company with hundreds of employees will have hundreds of copies of a relevant company policy that was e-mailed to each employee. It is not necessary to review hundreds of copies of the same policy, which would greatly increase the cost of the related review. Consider also the situation where a copy of a contract is saved by all employees in the department to their individual hard drives. It is only necessary to review one copy of this contract.

De-duplication can be performed within each custodian's data set or, more commonly, "across" all files ("case-wide de-dupe"). Where it is important to know whether a particular document existed in the files of a particular person, a party would perform custodian-level de-dupe, which ensures that the party will see each document that a person possessed, even if the same document exists in the files of other custodians. If it is

---

150. De-duplication should be limited to those documents or data items that are exactly alike (typically confirmed by comparing the documents' "hash" values). It should be noted that specific elements from a document or data item, such as author, creation date and time, size, full text and the like, can be used alone or in combination to develop targeted de-duplication algorithms. A "hash" is a mathematical algorithm that represents a unique value for a given set of data, similar to a digital fingerprint. Common hash algorithms include MD5 and SHA1. The Sedona Conference, *Glossary: E-Discovery & Digital Information Management* (April 2014), *supra* note 9.

not important to know whether a document existed in each person's files, the review team only needs to see it once in the whole case; here, in such cases, a case-wide de-dupe will be used. Understanding the implications of de-duplication technologies and choices is an important part of discovery planning.

b) Near Duplicates

A process called near-duplicate identification identifies documents that are substantially the same, although they may contain minor differences. For example, if a party has a business report generated on a weekly basis, these records will be similar but not identical to each other.

By grouping highly similar documents together, near-duplicate identification helps to expedite the review. This efficiency will save considerable time and cost and increase the quality and accuracy of the review.

c) E-mail Threading

E-mail threading software groups together an entire chain of an e-mail, identifies the e-mails whose content is wholly contained in later e-mails, and thus allows reviewers to review only (a) the last-best e-mail in a chain and (b) any other e-mails that add something new that is not found in any other e-mail. This technology saves time, increases the consistency of coding, permits better identification of privileged information and speeds up the pace of the review, allowing reviewers to "bulk code" groups of records where appropriate.

Comment 7.c.iii. Keyword Searching

Keyword searching involves searching the documents for words or phrases that are common and distinct to a claim or defence, such as product names and components in a product liability case. Note that, due to the casual nature of many e-mails, potentially relevant e-mails may not contain the words or

phrases selected, as the correspondents are familiar with the context and the exchange is part of a larger conversation. Care should be taken when selecting keywords, and the results of keyword searches should always be validated through sampling both the responsive and nonresponsive populations.

Comment 7.c.iv. Predictive Coding/Machine Learning Systems/Technology Assisted Review

Predictive coding, machine learning or technology assisted review is a combination of technology and workflow that assists in prioritizing records in a data set for review. The basic premise is that a person (ideally, a senior lawyer) familiar with the key issues in a case will "train" the computer to identify relevant records through a basic relevant/not relevant triage phase. Workflows and technology may vary in that the initial records may be a random sample, or the computer may be fed relevant records in a "seed set."

Once the computer confirms it has sufficient information to code the records the same way that the trainer would code the records, it ranks the remaining un-coded records by likelihood of being relevant. This permits the lawyers to prioritize the balance of the records for review, concentrating on the records most likely to be relevant first. In some cases, it may be reasonable and defensible to not review some of the remaining data set, given the low probability that it contains any relevant records.

While this is still an evolving field, with significant efforts being made to assess the capabilities of these still-evolving analytics technologies (including predictive coding and other forms of auto-classification), it is fair to say that these tools, when used by skilled practitioners as part of a process managed by experts, have repeatedly yielded more accurate results than

traditional eyes-on linear review by humans and have done so more quickly and at lower overall cost.

It must be emphasized that the workflow and validation processes are critical when utilizing predictive coding to ensure defensibility, since the algorithms are based on probability and statistical analysis. Predictive coding technology on its own is not a substitute for the legal judgment of review lawyers. It is merely a tool that may be effectively applied in large-volume cases where keywords and other technologies are not as effective.

All of the above tools can significantly increase, not just the efficiency of a document review project, but also its accuracy, and at the same time reduce the overall cost. It can also assist in preventing inadvertent production of privileged or confidential information. As valuable as these tools are, ultimately counsel must ensure that legal judgment and a carefully documented methodology are adopted and that the results of using any tools are validated.[151]

Comment 7.d. Sampling and Validating Results

All discovery processes should be subject to accepted methods of validation as appropriate for the particular circumstances.

One approach used to validate results is sampling. Sampling is the process of examining a subset of a document population and making a determination about the entire population based on that examination. Sampling can be carried out on a tar-

151. *Air Canada v. West Jet*, [2006] 81 OR (3d) 48, 2006 CanLII 14966 (ONSC) [*West Jet*].

geted basis ("purposive" sampling) or systematically ("statistical" sampling). The most appropriate method will depend on the circumstances of each case.

Under Principle 7, sampling—whether purposive or statistical—is an appropriate tool both to limit the initial scope and cost of a discovery project, and to validate the results of a technology assisted review.

For example:

- Where a party possesses a series of backup tapes, it may be appropriate to inspect the contents of a few of the tapes, as a sample, to determine whether the inspection of the remaining tapes is required. In this case, determining what tapes to sample could be a matter of common sense, informed by the client's special understanding of where relevant ESI would be most likely to reside. This situation might therefore call for purposive sampling.[152]
- The above example could also apply to a room full of boxes. Inspecting or sampling a set number of documents from each box may help in determining which boxes may require further review.
- Running search terms on files within a network group share and then sampling the results may help determine that a very low percentage of files within that network group share contain evidence that is relevant. This high cost/low return ratio (or low marginal utility ratio) may

152. See e.g. *McPeek v. Ashcroft*, 212 F.R.D. 33, 37 (D.D.C. 2003).

weigh against the need to search that source further or it may be a factor in a cost-shifting analysis if one party insists that very expensive and time consuming searches be employed. See *Consorcio Minero Horizonte S.A. et al. v. Klohn-Crippen Consultants Limited et al*[153] for an application for the concept of cost shifting in an analogous situation.

- During a review, the legal team identifies a pattern of records that are consistently irrelevant. Using keyword searching, a large subset of the records is identified as being potentially irrelevant. A statistically valid sample of this subset is reviewed, and no relevant records are identified. Based on this process, it is decided that the subset can be considered irrelevant with no further manual review.

There are two statistical measurements that are typically used to measure the results of a sample analysis: recall and precision.

i. **Recall.** The percentage of relevant records that are identified out of all relevant records in the population.

- If a collection has 100 relevant records and the analysis found 50 of them, the recall would be 0.5 or 50%.
- Recall measures how completely a process has captured the target set. High recall means that there were very few relevant documents that

153. 2005 BCSC 500 (CanLII).

were not found (false negatives); low recall indicates a higher proportion of false negatives.

- Higher recall supports the position that a party has met its production obligations.

ii. **Precision.** The percentage of documents retrieved that are in fact relevant.

- If 50 records are identified as relevant, but 5 of them turn out to be non-relevant, the precision is 0.9 or 90%.
- Precision measures how well a process has avoided including irrelevant records. High precision means there are very few documents in the result set that are not relevant (false positives); low precision indicates a higher proportion of false positives.
- A higher precision rate helps avoid reviewing too many irrelevant records.

The goal is to achieve both high recall and high precision.

Regardless of the technology used, or whether the documents are in paper or electronic format, a consistent method for selecting a sample and analyzing the results must be developed. This "consistent" method need only be consistent within a given set of records—each matter will have a set of documents with its own characteristics. As such, a method suitable for one matter may not be applicable to a different, albeit similar matter.

Principle 8. The parties should agree as early as possible in the litigation process on the format, content and organization of information to be exchanged.

Comment 8.a. Electronically Stored Information Should Be Produced in Electronic Format (Not Paper)

When at all possible, the production of ESI should be made in searchable electronic format,[154] unless the recipient is somehow disadvantaged and cannot effectively make use of a computer.[155] Examples of searchable electronic formats include native files (such as Microsoft Word, Microsoft Excel and Microsoft Outlook files) and imaged representations of the native files converted to a format (such as TIFF[156] or PDF[157]) in a searchable format.

---

154. *Discovery Task Force Guidelines*, *supra* note 92: "Production of voluminous documentation in a form that does not provide meaningful access should be avoided." See also *Cholakis, supra* note 36 at para 30, 44 CPC (4th) 162 (MBQB): "The interests of broad disclosure in a modern context require, in my view, the production of the information in the electronic format when it is available."

155. In a criminal case, in circumstances where the accused was in prison and had insufficient access to computers, the Crown was ordered to disclose in paper form. See *R v. Cheung*, 2000 ABPC 86 (CanLII) at para 99, 267 AR I79: "[W]hile electronic or soft copy disclosure may now in the 21st Century be considered a usual form also, in the circumstances of this case, it is not accessible to the accused."

156. TIFF stands for "Tagged Image File Format." It is a computer file format for exchanging raster graphic (bitmap) images between application programs. A TIFF file can be identified as a file with a ".tiff" or ".tif" file name suffix.

157. PDF stands for "Portable Document Format." It is a file format used to present documents in a manner independent of application software, hardware and operating systems. A PDF file can be identified with a ".pdf" file name suffix.

The practice of producing ESI in static format such as paper should be discouraged in most circumstances for several reasons:

- Depending on the nature of the electronic record, paper may not be an authentic substitute for the contents and properties of the original record.
- Paper cannot retain potentially critical metadata (such as who the author was, the date the document was created, the date the document was last modified), which, if relevant, is producible.
- Paper records are harder to search and are harder to logically organize using litigation support software tools. This means that a paper production set is usually less meaningful than a set of documents produced in a searchable electronic format.[158]
- Reviewing a large collection of paper records is more time-consuming and expensive than re-

158. See *Servier, supra* note 111 at para 10: "Following this contrary approach, the defendants took the position in the first instance that the CD-ROMs and electronic database (used in conjunction with the *Summation* legal data processing system) defendants' counsel had prepared at significant expense for themselves in respect of their own documents (so as to organize meaningfully the documents they disclosed in their affidavits) were not to be shared with the plaintiff. Later, in the course of a case conference, the defendants provided an index in word format but plaintiff's counsel asserted that the voluminous documents were simply not searchable. The production of voluminous documentation in a form that does not provide meaningful access is not acceptable." *Solid Waste Reclamation Inc. v. Philip Enterprises Inc.* (1991), 2 OR (3d) 481 (CanLII) (Gen Div.).

viewing the same collection of searchable electronic records,[159] since parties will then not be able, in their review, to take advantage of technologies that can greatly enhance review efficiency and search accuracy.

- Each printed set required for hard copy production adds to the cost of reproduction, shipping and storage, whereas multiple electronic copies can be made at a nominal cost. The use of electronic productions creates opportunities for cost sharing, particularly in multi-party actions, where savings can be significant.
- Producing documents in electronic format is better for the environment.

Comment 8.b. Agreeing on a Format for Production

The parties should agree on how they are going to produce documents at the early stages of litigation or during discovery plan conferences. It is preferable if each party designates the form in which it wishes ESI to be produced. Given the fact that there are so many different litigation support programs available today, each party may have different production requirements. While it is acceptable for the parties to produce documents in different formats, it is strongly recommended that

159. See *Sycor, supra* note 111. Where the cost of printing and photocopying e-mail for production was estimated at $50,000, "[a]t the very least there should be consideration given to electronic production of documents that are required and perhaps the use of computer experts to identify what exists and what is truly relevant to the issues that are actually in dispute."

parties develop a framework for resolving disputes over the form of production.[160]

For a number of reasons, ESI should wherever possible be produced in native format. First, the native version is the truest, most accurate version of the document; second, native files are easier, faster and cheaper to transfer, upload and search than are any other format; third, conversion to other formats entails the loss of information; and fourth, native versions contain all of the application-level and user-created metadata for the files, some of which may be crucial to understanding the true meaning of the files. User-generated metadata is information about the document that is entered by a user at the file level—for example, the fields that can be populated in the Properties tab of a Microsoft Office document. In addition, many kinds of electronic files contain information that can be lost if it is simply converted to an image or other non-native format. Examples of such information include that which is: (a) in spreadsheets: macros, formulas, conditional formatting rules and hidden columns/rows/worksheets; (b) in presentations: speaker notes; (c) in word-processing documents: text-editing notations ("track changes"); and (d) in virtually all file types: comments, sticky notes and highlighting. Such information is as much a part of the document as the visible text and, in some investigations or litigation, could be highly relevant. Parties should therefore be prepared to produce files in native format or explain why they prefer not to. Parties should also be aware that most modern native file processing tools can extract metadata that indicates

160. *Kaymar, supra* note 119. The Master observed that a well-crafted discovery plan that contains dispute resolution mechanisms can avoid motions practice, including on issues such as the format of production.

whether an individual file contains this kind of normally-hidden information and that these metadata fields (e.g. "contains hidden text") can be provided as part of the production.

Where parties prefer to receive files converted from native format to an image format—such as PDF or TIFF—they should so specify. The fact that one party prefers to receive documents in PDF/TIFF format, however, does not preclude another party from asking that the production to it be made in native format.[161] It is customary and acceptable practice to convert documents that are to be redacted into image format, but parties producing redacted images should make sure that the rest of the document is searchable, by performing optical character recognition (OCR) on the redacted images and including the resulting text in the production.

Where parties do not specify a form of production, or where a producing party objects to a requested form of production, the producing party should notify the other party of the form in which it intends to produce the information. It is recommended that production occur either (1) in the form in which the information is ordinarily maintained or (2) in a reasonably usable form. It is rarely appropriate to downgrade the usability

161. *Quizno's*, *supra* note 127 at paras 128–131. The Court disagreed with the defendant's refusal to re-produce copies of Excel documents in Excel format. The documents had originally been produced in TIFF format pursuant to the discovery plan. There would be no hardship to the defendant to produce the Excel files. The Court found ". . .generally speaking a court should not allow the significant effort to establish a plan becoming a waste of time and effort by not holding parties to their agreement, discovery plans are just that, they are a plan and there is an old maxim that it is a bad plan that admits of no modification." (para 130) The Court ordered copies of the already produced documents, if readily available, to be produced again in Excel format.

or searchability of produced information without the consent of the receiving party or an order of the Court.

There is also an expectation that trials will increasingly be conducted electronically (which requires that documents be produced in an electronic format). In *Bank of Montreal v. Faibish*,[162] the Court rejected the proposition that the trial be conducted both through paper and digital information. "Paper must vanish from this Court and, frankly, the judiciary cannot let the legal profession or our court service provider hold us back."[163]

Comment 8.c. Affidavits and the Format and Organization of Record Lists

Court rules in most provinces require the preparation of a list that describes all relevant documents, with information to permit individual documents to be separately identified. Depending on the province, this might be called an affidavit of documents, affidavit of records, affidavit disclosing documents or list of documents.[164] The applicable rules of court may also require the parties to provide a list of documents that may be relevant but are not within the care and control of the producing party, and a list of documents that are being withheld on the basis of privilege.

---

162. 2014 ONSC 2178.

163. Although this type of decision was rare at the time of the drafting and publication of this edition of *The Sedona Canada Principles Addressing Electronic Discovery*, it is anticipated that this type of decision and order will be made more common in the future.

164. Such lists are called an affidavit of records in Alberta, and an affidavit disclosing documents (individual/corporation) in Nova Scotia. In all other provinces that have this requirement it is known as ether an affidavit of documents or list of documents.

The requirement for the above dates back to an era when parties produced only paper documents. The document list was the only method of providing organization to a paper collection. This practice remains today, although as noted further below, it is evolving.

Where parties exchange paper productions or electronic productions of paper records which have been digitized, the document lists are usually manually coded using information obtained from the (face) content of the record. The standard fields exchanged typically include: Production Number; Record Type; Author; Recipient(s); Date; Document Title; or Subject; and, sometimes, Page Count.

When creating such lists (either for paper or native productions), parties should consider using the metadata associated with electronic records to populate the above standard fields instead of manually coding information from the content of the record, even if the original native files are converted to an image format prior to production. This practice is particularly applicable to the production of e-mails, where the metadata clearly indicates the Record Type, Author, Recipient(s), Record Date and Record Title (subject). For non-e-mail records, the metadata, file type or file-extension value can be used to denote the Record Type, the filename or pathname could represent the Record Title and last modified timestamp could represent the Record Date. The suitability of using metadata instead of manually coded information should be based on whether using the metadata will result in the production of information sufficient to uniquely identify each record being produced.

As noted above, the need to provide these "Lists of Documents" is evolving, given the nature of electronic documents and the ways they can be searched and sorted. In *Cameco Corp.*

v. Canada,[165] the respondent had argued that the use of metadata to describe all documents was unsatisfactory and had resulted in a "maldescription" of the documents. In some cases, the Author and Date information obtained from the metadata differed from the Author and Date information on the face of the document. The respondent noted that it would be more helpful to have only the document identifier in the list of documents with no author and no date, with which the Court agreed. "So long as the appellant has provided sufficient description of the documents using a numerical identifier for each document, its identification of the document is satisfactory."

Document lists often are part of an Affidavit of Documents that must be sworn by clients verifying that all relevant documents have been produced. In light of the volume of ESI available for discovery in modern litigation, and the fact that it is impossible to verify that all relevant documents have been produced, courts and rules committees may have to reassess the utility of affidavits verifying full disclosure of records. In all cases, the affidavits should be carefully reviewed in order to ensure that the content of the affidavit can be sworn or affirmed by the client, particularly in circumstances where the affiant may not have personal knowledge of the efforts involved in the collection, processing and review of the documents exchanged in production.

165. 2014 TCC 45 (CanLII).

Principle 9. During the discovery process, the parties should agree to or seek judicial direction as necessary on measures to protect privileges, privacy, trade secrets and other confidential information relating to the production of electronically stored information.

Comment 9.a. Privilege

Solicitor-client privilege is intended to facilitate and encourage full and frank communication between a lawyer and client in the seeking and giving of legal advice. Litigation privilege is intended to secure for the litigant a zone of privacy within which to prepare its case against opposing parties. A party potentially waives the solicitor-client privilege, litigation privilege or both if that party, or even a third party, voluntarily discloses or consents to the disclosure of any significant part of the matter or communication, or fails to take reasonable precautions against inadvertent disclosure. Due to the ever-increasing volume of ESI that is potentially relevant, there is an increased risk of the inadvertent disclosure of privileged information. Notably, the privilege review phase can be the most expensive phase of discovery.

Comment 9.a.i. Inadvertent Disclosure

Canadian courts have generally accepted that inadvertent disclosure does not waive solicitor-client privilege.[166] Nev-

166. See *Elliot v. Toronto (City)* (2001), 54 OR (3d) 472 (SC) at para 10 (CanLII); John Sopinka, Sidney N. Lederman & Alan W. Bryant, THE LAW OF EVIDENCE IN CANADA, 2d ed. (Toronto: Butterworths, 1999) at 766–67; *Dublin v. Montessori Jewish Day School of Toronto*, 2007 CarswellOnt 1663 (SCJ); *Sommerville Belkin Industries Ltd. v. Brocklesh Transport and Others* (1985), 65 BCLR 260 (SC) (CanLII); *National Bank Financial Ltd. v. Daniel Potter et al.*, 2005 NSSC

ertheless, one Court held that the privilege was lost after inadvertent disclosure of a privileged communication, deciding that it was possible to introduce the information into evidence if it was important to the outcome of the case and there was no reasonable alternative form of evidence that could serve that purpose.[167] In contrast, see *L'Abbé v. Allen-Vanguard Corp.*,[168] in which the Ontario Superior Court of Justice held that truly inadvertent disclosure should not be treated as waiver of privilege unless the party making the disclosure is truly reckless or delays in reasserting the privilege or certain other conditions are met. Privilege may be lost through inadvertent disclosure based on considerations including: the manner of disclosure, the timing of disclosure, the timing of reassertion of privilege, who has seen the documents, prejudice to either party or the requirements of fairness, justice and search for truth.[169]

The issue of volume was also addressed in *L'Abbé v. Allen-Vanguard Corp.* where the Master held that court inspection

---

113, 233 NSR (2d) 123 (CanLII) [*Daniel Potter*]; *National Bank Financial Ltd. v. Daniel Potter*, 2004 NSSC 100, 224 NSR (2d) 231 (CanLII); *Autosurvey Inc. v. Prevost*, [2005] OJ No 4291 (CanLII) (ONSC).

167. See *Metcalfe v. Metcalfe*, 2001 MBCA 35 at para 28, 198 DLR (4th) 318 (CanLII).

168. See *L'Abbé, supra* note 51. See also *Minister of National Revenue v. Thornton*, 2012 FC 1313 (CanLII) and *McDermott v. McDermott*, 2013 BCSC 534 (CanLII).

169. The Federation of Law Societies Model Code of Professional Conduct, October 2014, Rule 7.2-10, provides: A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent must promptly notify the sender. http://flsc.ca/wp-content/uploads/2014/10/ModelCodeENG2014.pdf. This principle has been adopted by Law Societies in Canadian jurisdictions. See e.g. *Aviaco International Leasing Inc. v. Boeing Canada Inc.*, 2000 CanLII 22777 (ON SC), at para 10–13.

of 6,000 inadvertently produced documents over which privilege was claimed was not a viable option. Instead, the Master placed the obligation of narrowing the dispute in relation to those documents on the parties. In so doing, he directed the parties to first try to reach a meeting of the minds with respect to probative value and relevance of the documents and then to attempt to come to agreement on categories of the documents that should be available at trial. Finally, once the number of documents was reduced, the parties were to consider what process could be used to filter the documents for relevance and privilege, including considering technological solutions. The Master held that "cost effectiveness, practicality and privilege should be the touchstones. The exercise should be governed by the '3Cs' of cooperation, communication and common sense."[170]

Comment 9.a.ii. Protective Measures

With the extremely large numbers of electronic documents involved in litigation matters, conducting a review of relevant electronic documents for privilege and confidentiality can be very costly and time consuming. Parties must employ reasonable, good-faith efforts[171] to detect and prevent the production of privileged materials. Good-faith efforts will vary from case to case, ranging from a manual page-by-page review for a small data set, to an electronic search for words or phrases likely to locate privileged materials where the data set is larger. In many cases, a combination of the two is appropriate. Other technological tools such as predictive coding and concept clustering

170. *L'Abbé, supra* note 51 at para 98.

171. See *West Jet, supra* note 151 at para 20, where the Court rejected the request for an order protecting against the waiver of privilege where a "quick peek" type of production was being proposed. But see also *L'Abbé, supra* note 51.

may also assist with the identification and segregation of potentially privileged records.

Comment 9.a.iii. Sanctions

Courts have imposed a spectrum of sanctions when counsel has obtained and reviewed privileged communications from an opposing party without that party's consent. These sanctions can include striking pleadings, the removal of counsel from the file and costs. The removal of counsel has been ordered where the evidence demonstrated that, despite the fact counsel or the party knew or should have known that it had acquired an opposing party's solicitor-client communications, counsel took no steps to seek directions from the Court or to stop the review and notify the privilege holders.[172]

Comment 9.a.iv. Use of Court-Appointed Experts

In certain circumstances, a court may appoint a neutral third party (i.e. a special master, judge or court-appointed expert, monitor or inspector) to help mediate or manage electronic discovery issues.[173] A benefit of using a court-appointed neutral expert is the probable elimination of privilege waiver concerns with respect to the review of information by that neutral expert. In addition, a neutral expert may speed the resolution of disputes by fashioning fair and reasonable discovery plans based upon specialized knowledge of electronic discovery or other technical expertise along with the pertinent facts in the case.

172. See *Daniel Potter, supra* note 166; *Auto Survey Inc. v. Prevost*, 2005 CanLII 36255 (ONSC); and *Celanese, supra* note 95.

173. *Catalyst Fund General Partner 1 Inc. v. Hollinger Inc.*, 2005 CanLII 30317 (ONSC).

Where necessary and practical in the circumstances of a particular matter, parties should cooperate and agree upon the appointment of a neutral expert.

The Supreme Court of Canada has endorsed the practice that review of documents seized under an Anton Piller order be undertaken by a lawyer who then prepares a report detailing conclusions reached.[174]

Comment 9.a.v. Protection of Privileged Information

Given the expense and time required for pre-production reviews for privilege and confidentiality, parties should consider entering into an agreement to protect against inadvertent disclosure, while recognizing the limitations in the applicable jurisdiction of such an agreement vis-à-vis courts and third parties. These agreements are often called "clawback" agreements.[175] Court approval of the agreement should be considered. The agreement or order would typically provide that the inadvertent disclosure of a privileged document does not constitute a waiver of privilege. The privileged communication or document should be returned, or an affidavit sworn that the document has been deleted or otherwise destroyed. The agreement should provide that any notes or copies will be destroyed or deleted and any dispute will be submitted to the Court. It is preferable that any such agreement or order be obtained before any production of documents take place. The agreement should clearly specify the process and steps to be taken in the event a party or its counsel determine that a privileged communication has been inadvertently disclosed.

---

174. *Celanese, supra* note 95.

175. See *West Jet*, *supra* note 151; see also *Zubulake v. UBS Warburg* LLC, 216 FRD 280, 290 (SDNY 2003) (WL).

Parties should exercise caution when relying on clawback agreements as such agreements may not eliminate counsel's obligation to use reasonable good-faith efforts to exclude privileged documents prior to initial disclosure. In *Nova Chemicals (Canada) Ltd. v. Ceda-Reactor Ltd.*, a party invoked a clawback agreement concerning inadvertently produced documents, but the Court rejected its argument and set out principles to be considered in such determinations.[176] Also, a clawback agreement may not be enforceable against a party who is not a signatory to the agreement.[177]

In the case of very large data sets, parties to litigation could consider a more aggressive type of clawback agreement, perhaps even agreeing to a reduced pre-production search methodology requirement. Such clawback agreements, however, should be approved by the Court to ensure enforceability.

There is a growing body of evidence from the information-science field that the use of technologically-based search tools may be more efficient and more accurate than manual searches.[178] The Working Group recommends that Courts consider this body of evidence in assessing whether reasonable steps were taken in a privilege review.

---

176. *Nova Chemicals (Canada) Ltd. v. Ceda-Reactor Ltd.*, 2014 ONSC 3995 (CanLII).

177. *Hopson v. Mayor of Baltimore*, 232 FRD 228 (D Md 2005) (WL Can).

178. Feng C. Zhao, Douglas W. Oard & Jason Baron, *Improving Search Effectiveness in the Legal E-Discovery Process Using Relevance Feedback* (paper delivered at the 12th International Conference on Artificial Intelligence and the Law (ICAIL09 DESI Workshop) (2009)); Maura R. Grossman & Gordon V. Cormack, *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review* (2011), 17:3 Rich JL & Tech 11.

Comment 9.b. Protection of Confidential Information

Confidentiality concerns can arise when there is sensitive or proprietary business information that may be disclosed in discovery. Protective orders can be sought to protect confidential information produced over the course of discovery. The availability of protective orders is the product of an attempt to balance the competing values of an open and accessible court proceeding and the public interest in a fair judicial process against serious risks of harm to commercial interests of one or more litigants.

The seminal decision on this topic is *Sierra Club of Canada v. Canada (Minister of Finance)*,[179] a case involving the judicial review of proceedings initiated by an environmental organization, the Sierra Club, against a Crown Corporation, Atomic Energy of Canada Ltd. ("Atomic Energy"), which concerned the construction and sale to China of nuclear reactors. The Sierra Club sought to overturn the federal government's decision to provide financial assistance to Atomic Energy. At the heart of this decision were confidential environmental assessment reports originating in China, which Atomic Energy sought to protect by way of a confidentiality order. Atomic Energy's application before the Federal Court, Trial Division[180] was rejected, and the appeal from this decision was dismissed by all but one judge of the Federal Court of Appeal.[181] On further appeal to the Su-

179. *Sierra Club of Canada v. Canada (Minister of Finance)* (2002), 211 DLR (4th) 193 (CanLII) (SCC), 2002 SCC 41 (CanLII).

180. *Sierra Club of Canada v. Canada (Minister of Finance)* (1999), 1999 CarswellNat 2187 (FCTD).

181. *Sierra Club of Canada v. Canada (Minister of Finance)* (2000), 2000 CarswellNat 3271 (FCA).

preme Court of Canada, Atomic Energy was ultimately successful in obtaining relief. In arriving at its conclusion, a unanimous Supreme Court reasoned:

> A confidentiality order should only be granted when (1) such an order is necessary to prevent a serious risk to an important interest, including a commercial interest, in the context of litigation because reasonably alternative measures will not prevent the risk; and (2) the salutary effects of the confidentiality order, including the effects on the right of civil litigants to a fair trial, outweigh its deleterious effects, including the effects on the right to free expression, which in this context includes the public interest in open and accessible court proceedings. Three important elements are subsumed under the first branch of the test. First, the risk must be real and substantial, well grounded in evidence, posing a serious threat to the commercial interest in question. Second, the important commercial interest must be one which can be expressed in terms of a public interest in confidentiality, where there is a general principle at stake. Finally, the judge is required to consider not only whether reasonable alternatives are available to such an order but also to restrict the order as much as is reasonably possible while preserving the commercial interest in question.[182]

Also, the long-standing practice of redacting documents to prevent the disclosure of irrelevant, confidential or privileged

182. See head note of *Sierra Club*, *supra* note 179.

communications remains in effect with respect to the production of ESI. The use of redactions to protect confidential or privileged information from disclosure is a tool that should be used, provided that the reason for the redaction is clearly and properly identified. If necessary, parties can obtain an appropriate court order, or incorporate terms into a Discovery Plan, for the redaction of confidential or personal information. The use of electronic tools for redactions should also be considered as such tools can greatly reduce the time and expense associated with manual redaction.

Comment 9.c. Privacy Issues

Confidentiality orders, the common law and civil procedure rules may limit the extent to which commercially sensitive or personal information may be disclosed. Canada and its provinces, to varying extents, have comprehensive privacy legislation[183] governing the collection, use and disclosure of personal

183. Legislation regulating the public sector includes: the *Privacy Act*, RSC 1985, c P-21; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165; *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25; *Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.0I; *Freedom of Information and Protection of Privacy Act*, CCSM c F-175; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F-31; *An Act respecting access to documents held by public bodies and the protection of personal information*, LRQ c A-2.1; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5; *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05; *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01; *Access to Information and Protection of Privacy Act*, SNL 2002, c A-1.1. Legislation governing the private sector includes the *PIPEDA, supra* note 33; *Personal Information Protection Act*, SBC 2003, c 63; *Personal Information Protection Act*, SA 2003, c P-6.5; *An Act respecting the protection of personal information in the private sector*, LRQ c P-39.1.

information,[184] in both the public and private sectors, that may affect the discovery process. Privacy issues can arise in a wide variety of contexts and can include the privacy rights of non-parties.

The courts have not been sympathetic to objections to producing relevant information based on privacy legislation. Courts do, however, consider privacy issues in assessing whether discovery requests are too broad or whether non-relevant private information can be protected.[185]

It is important to note that the deemed undertaking rule,[186] i.e. the implied undertaking rule, is a rule in the discovery process only; it does not provide privacy protection per se. For example, in Ontario, the deemed undertaking rule only applies to evidence obtained in the actual discovery process, and it specifically does not apply to evidence filed with the court or referred to during a hearing. A court order can also be obtained to relieve compliance with the deemed undertaking rule.[187]

Comment 9.c.i. Social Media

A party should consider whether social media content and documents are relevant and should be preserved and listed in an affidavit or list of documents or records. A court may order private portions of a party's social media profiles and pages to be disclosed where the information is relevant and the probative value of the information justifies the invasion of privacy

184. Generally defined as information about an identified or identifiable individual.

185. See *Dosanjh v. Leblanc*, 2011 BCSC 1660 (CanLII).

186. Generally, the deemed undertaking rule prohibits parties from disclosing evidence and information obtained during the discovery process outside the confines of the litigation.

187. *Ontario Rules*, *supra* note 10, 30.1.01.

and the burden of production.[188] The mere fact however that a party has a social media presence does not presumptively mean that the private aspects of an account are relevant.[189] For example, in *Bishop v. Minichiello*, the defendants sought production of the plaintiff's hard drive to determine the time the plaintiff spent on Facebook.[190] The plaintiff's computer was used by all members of his family. To protect the privacy rights of the non-party family members, the Ontario Court ordered the parties to agree on the use of an independent expert to review the hard drive. In *Fric v. Gershman*,[191] the Supreme Court of British Columbia similarly sought to protect the privacy of third parties when it ordered production of certain photographs posted on the plaintiff's Facebook page. The plaintiff was permitted to edit the photographs prior to disclosure to protect the privacy of other individuals who appeared in them. The Court in *Fric* refused to order production of commentary from the Facebook site, however, holding that if such commentary existed, the probative value of the information was outweighed by the competing interest of protecting the private thoughts of the plaintiff and third parties.[192]

---

188. See *Leduc v. Roman*, 2009 CanLII 6838 (ON SC); *Frangione v. Vandongen*, 2010 ONSC 2823 (CanLII); *Murphy v. Perger*, [2007] OJ No 5511 (WL Can); *McDonnell v. Levie*, 2011 ONSC 7151 (CanLII); and *Casco v. Greenhalgh*, 2014 CarswellOnt 2543 (Master).

189. *Schuster v Royal & Sun Alliance Insurance Company of Canada*, [2009] OJ No 4518 (WL) (ON SC); and see *Stewart v. Kemptster*, 2012 ONSC 7236 (CanLII); *Garacci v. Ross*, 2013 ONSC 5627 (CanLII); and *Conrod v. Caverley*, 2014 NSSC 35 (CanLII).

190. 2009 BCSC 358 (CanLII), leave to appeal for further production dismissed, 2009 BCCA 555 (CanLII).

191. *Fric v. Gershman*, 2012 BCSC 614 (CanLII).

192. *Fric v. Gershman*, 2012 BCSC 614 (CanLII) at para 75, citing *Dosanjh v. Leblanc and St. Paul's Hospital*, 2011 BCSC 1660.

If necessary in the circumstances, social media content and documents should be collected and produced in a forensically sound manner. As an example, screen captures and printed paper versions may be unreliable.[193]

Generally, a lawyer is not permitted to have contact with a represented opposing party without the party's counsel present. The lawyer needs to keep that rule in mind if reviewing social media of an opposing party. The social media site may advise the opposing party that the lawyer has viewed the site, and, if counsel has gone beyond merely viewing publicly available pages and has actually engaged with the opposing party in some fashion, such as e-mailing or "friending" that party, this may violate the no-contact rule.

Comment 9.c.ii. Employee Privacy on Employer-Issued Devices

An employee's right to privacy on an employer owned device (e.g. desktop computer, laptop, tablet, or phone) will continue to be a fact-specific determination. In *R. v. Cole*, the Supreme Court of Canada confirmed that employees do have limited privacy rights on employer-issued computer devices.[194] The Court held that employees may have a reasonable expectation of privacy where personal use is permitted or reasonably expected. Ownership and workplace policies were held to be relevant for consideration but not determinative of whether privacy was protected in a particular situation. In *International Union of Elevator Constructors, Local 50 v. Otis Canada Inc.*,[195] the

193. 2013 CanLII 3574 (ON LRB).

194. 2012 SCC 53.

195. *International Union of Elevator Constructors, Local 50 v. Otis Canada Inc*, 2013 CanLII 3574 (ON LRB).

Labour Relations Board held, however, that if an employee chooses to use a company vehicle to and from home, the company is not restricted from using technological devices to monitor the vehicle at all times.

In juxtaposition to the above are the rights of the employer with respect to its proprietary and confidential information when an employee uses his or her own device for work (commonly referred to as a "bring your own device" or BYOD). Many businesses acknowledge and accept the use by employees of employee-owned digital devices on corporate networks. BYOD policies are essential if employees are using their own devices. These policies need to set out who owns the data, and provide a means to allow the organization to gain access to that data if necessary.

Comment 9.c.iii. Criminal Records and Investigations

In cases that involve criminal or regulatory investigations or proceedings, a number of privacy rights arise. The seizure of electronic evidence during a regulatory or criminal investigation or process brings into play the right to be free against unreasonable search or seizure under section 8 of the *Canadian Charter of Rights and Freedoms* ("the *Charter*").[196]

Where the electronic evidence required for a proceeding forms part of a parallel criminal investigation, the principles and screening process identified in *D.P. v. Wagg*[197] should be applied to obtain the appropriate court orders and protections if required. Prior to the release of criminal investigation materials,

196. Everyone has the right to be secure against unreasonable search or seizure. Section 8, *Canadian Charter of Rights and Freedoms*. See e.g. *R v. Cole*, 2012 SCC 53 (CanLII).

197. 2004 CanLII 39048 (ON CA) [*Wagg*].

including the contents of computer hard drives seized by authorities, the Crown must be notified and provided the opportunity to review the materials for third-party privacy and public interest concerns.

Comment 9.d. Data Security

Corporations, public organizations, law firms and individuals are all potential targets for data breaches and the theft or loss of valuable information. To secure the protection of privilege, privacy, trade secrets and other confidential information, parties, counsel and service providers should take reasonable steps to safeguard their own documents and data, and those produced to them by opposite parties.

These steps may include appropriate chain-of-custody processes, secure and limited access to the data, encryption and password protection. Parties must also have appropriate procedures in place to secure the data during production and receipt at the completion of a project.

Appropriate chain-of-custody logs and procedures should be used to maintain the integrity of the data from collection to production in court. The chain of custody should document that: the data has been properly copied, transported and stored; the information has not been altered in any way; and all media have been secured throughout the process. The custody log should also include provision for the return of the data to the client or opposing counsel at the conclusion of the project.

At a minimum, data should be password protected, and preferably two-factor authentication[198] should be required.

198. Two factor identification requires a user to provide two different security components to access information, such as a password and USB stick with a secret token, or a card and a PIN.

Hackers have frequently targeted law firms and may view them as soft targets. In addition to technological security, access should be restricted to those with a "need to know," and both physical storage facilities and computer servers should be secured from unauthorized access.

Comment 9.e. Document Lists—Producing Coded Information

In some cases, courts have required the producing party to produce not only electronic records but also the objective coding created by the producing party when processing its records.[199] Producing selected contents of a litigation database, however, should not be confused with producing the software used to create and manage the database, which courts generally have not required.

The following decisions may assist counsel in understanding the Canadian approach to these issues.

- In *Wilson v. Servier Canada*,[200] the Court granted the plaintiff's motion for an order directing the defendant to release the objective coding of the documents in their litigation support database in order to meaningfully satisfy its disclosure requirements, given the volume of documents.
- In *Logan v. Harper*,[201] the defendants had produced the documents along with a searchable

199. For a discussion of coding, including a definition of objective coding, see *supra*, Introduction, section F.8 ("Advanced Technology Can Help to Organize, Search and Make Sense of ESI") and note 27.

200. *Servier, supra* note 111.

201. *Logan, supra* note 125.

index in electronic form. The index did not permit full-text searching of the documents, although the version of the application used by counsel for the defendants did offer that feature. The Master considered litigation support and document management software not normally subject to disclosure, and accepted as reasonable that the plaintiff's counsel purchase a licence for the software for access to the full-text search feature.

- In *Jorgensen v. San Jose Mines et al.*,[202] the defendants sought delivery of the electronic database used by the plaintiff to compile the list of documents. In this case, the Court ordered the plaintiff to provide a copy of the database to the defendants in electronic format and ordered the defendants to pay $4,000 to the plaintiff's firm as a reasonable proportion of the costs of preparing the database.
- More recently, however, in *Gamble v. MGI Securities Inc.*,[203] the Ontario Superior Court ordered all relevant Summation load files be delivered to the plaintiff in a DVD format, as requested by the plaintiff, at no cost above that of a blank DVD, rejecting the defendant's argument that the plaintiff should share in some of the costs resulting from preparing, coding and scanning the documents into the litigation support database. The Court noted that cost sharing may be

202. 2004 BCSC 1653 (CanLII).

203. 2011 ONSC 2705.

> warranted in some circumstances, but that various circumstances militated against it in this case, including the fact that the defendant had scanned many more documents than what were ultimately deemed relevant and the wide discrepancy between the financial abilities of the two parties—the plaintiff being a former employee of the corporate employer. It is noteworthy too that the Court accepted the plaintiff's argument that cost sharing in this case would be contrary to Sedona Canada Principle 12 which states that the reasonable costs of producing, collecting and viewing of documents to be produced will normally be borne by the producing party.[204]

Principle 10. During the discovery process, the parties should anticipate and respect the rules of the forum or jurisdiction in which the litigation takes place, while appreciating the impact any decisions may have in related proceedings in other forums or jurisdictions.

A single subject matter may give rise to proceedings in different forums (e.g. civil court, criminal court, arbitration, administrative or regulatory hearing) or jurisdictions (e.g. local, provincial, federal and other nations such as the U.S., Europe and elsewhere). Even within a single jurisdiction, there may be several related proceedings in different forums to which distinct discovery rules apply. These proceedings may take place concurrently or at different times.

---

204. *Ibid*.

In any proceeding, counsel must comply with specific discovery rules applicable to the particular forum or jurisdiction. Counsel need to appreciate that the rules of discovery across the applicable forums or jurisdictions may be in conflict with each other. In Canada alone, the rules of discovery vary among the common law provinces, and the discovery process in Quebec differs from discovery processes in the common law provinces. For example, in Ontario, "relevant" documents must be produced, whereas, in Alberta, "relevant and material" documents must be produced. In addition, there are some significant procedural and substantive differences in the discovery process, and in the privilege, privacy and evidence rules, between Canada and the United States.

Accordingly, when there are related proceedings, counsel must make good-faith efforts to ensure that there are no breaches of the rules of any applicable forum or jurisdiction. Counsel should take care to fully explain to clients the governing discovery process in the forum or jurisdiction so that the clients can make informed decisions on how to proceed. This requires counsel to take a proactive approach at the earliest possible stage in a proceeding to ensure that clients are not compromised in one forum or jurisdiction by actions taken in another.

The recommended cooperative process offers an ideal opportunity to identify and resolve any possible forum related rules conflicts at the earliest stage of a matter when possible. While negotiating a discovery plan, counsel should also consider how efforts can be coordinated to reduce the duplication of work so that the preservation, collection, review and production of ESI and other documents for all related matters can occur in the most cost-effective manner.

Comment 10.a. Geographic Jurisdictions and Cross-Border Litigation

When there is related litigation in other geographic jurisdictions, counsel should identify and consider the implications of the differences in procedural and related substantive law. While not intended to provide a comprehensive discussion, the following issues should be considered in any cross-border litigation matters:

i. **Procedure.** The procedures regarding the timing of discoveries, the need for discovery plans and the process for handling undertakings and refusals on discovery can often be very different.

ii. **Scope of Discovery.** The scope of what is discoverable and the obligations to produce can vary greatly between jurisdictions, including whether there is a positive obligation to produce relevant evidence versus producing documents in response to a written request.

iii. **Custody, Possession, Power or Control.** Production obligations can extend to documents not in the custody or possession of a party, but in their power or control, including documents held by a third-party "cloud" service provider, perhaps in a different jurisdiction. For example, if a party located in Canada has relevant documents stored on a server in Europe and can retrieve those at any time by logging in or asking for them, those records will likely be subject to an obligation to produce.

iv. **Affidavit of Documents.** The responsibility for swearing or affirming the completeness of the collection of documents produced in the proceeding can vary by jurisdiction and can affect the decisions regarding a proportionate discovery plan. Counsel and the client may have

different risk analyses regarding the steps to be taken to preserve and produce documents.

v. **Deemed Undertaking and Subsequent Use.** The deemed undertaking rule that exists in many Canadian provinces does not exist in the U.S. Counsel should consider the need for consent, and for protective or sealing orders, regarding subsequent use of information disclosed in the course of the discovery process. Orders in the foreign jurisdiction may be required to protect the deemed undertaking in cross-border litigation.

vi. **Non-Parties.** The process to obtain relevant evidence and documents from non-parties varies greatly among jurisdictions. In the common law provinces, non-parties can only be examined with leave of Court, and while a non-party's documents can be compelled prior to trial, the process to obtain such orders is very different from requesting documents from a party.

vii. **Privacy and Confidentiality.** Privacy laws in foreign jurisdictions can be very different. This includes the expectation of privacy and the privacy afforded to employees on employer-issued devices and computers. The legal test and process for obtaining protective and sealing orders can also vary significantly. Obligations pursuant to privacy legislation also need to be considered for cross-border data transfers and processing.

viii. **Privilege.** While most jurisdictions provide some protection to solicitor/client communications, the availability and scope of other privileges (e.g. "litigation" or "work product" privilege, privilege protection for communications with in-house lawyers, privilege protection for settlement negotiations, and the common-interest privilege) can vary significantly in foreign jurisdictions. Waiver of

privilege and counsel's obligation regarding inadvertently disclosed privileged documents also vary in foreign jurisdictions. Counsel should be aware of the variations in privilege rules so as not to inadvertently waive privilege in another jurisdiction.

ix. **Costs.** Rules regarding costs relating to discovery, disclosure and the proceeding differ in foreign jurisdictions. Further, the availability of "cost shifting" will vary from jurisdiction to jurisdiction.

x. **Specific E-Discovery Provisions.** Foreign jurisdictions have different protocols, preservation standards and expectations for electronic discovery. Proportionality and obligations for discovery plans are not principles shared by all jurisdictions. Sanctions can vary in severity as well as the activities or misconduct that would attract sanctions. Some jurisdictions have specific requirements concerning the format or the electronic searchability of the production of e-documents. It is also important to remember that The Sedona Conference's principles addressing electronic discovery also differ between Canada and the U.S. to reflect the different legal systems and rules.

In addition, in cross-border litigation, it may be necessary to obtain documents or information from outside the jurisdiction. The procedure and legal tests for obtaining that evidence can vary. For further information, counsel should consult *The Sedona Canada Commentary on Enforcing Letters Rogatory*, which contains a succinct summary of the key differences in the

rules governing cross-border evidence in Canada and the United States.[205]

The Sedona Conference® International Overview of Discovery, Data Privacy and Disclosure Requirements also provides an overview of discovery and data privacy laws in a number of countries around the world.[206]

Comment 10.b. Forums

Different procedural and substantive laws can also apply in different forums within the same geographic jurisdiction. One common example is in cases involving allegations of securities fraud, which may involve parallel bankruptcy proceedings, criminal proceedings and regulatory proceedings within the same jurisdiction.

Where there are parallel administrative, regulatory or criminal proceedings in the same jurisdiction, counsel should make good-faith efforts to become informed of any procedural and legal differences in disclosure and protection. As with cross-border disclosure, counsel should ensure appropriate protection orders or consents are in place prior to cross-forum disclosure. A proactive approach to obtain the necessary orders or consents will decrease the time and costs of any coordination required.

---

205. The Sedona Conference, *The Sedona Canada Commentary on Enforcing Letters Rogatory Issued by an American Court in Canada: Best Practices & Key Points to Consider* (June 2011 public comment version), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/463>.

206. The Sedona Conference, *International Overview of Discovery Data Privacy and Disclosure Requirements* (2009), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/62>.

Comment 10.b.i. Seized Evidence and Investigation Materials in Criminal or Regulatory Investigations

Criminal investigation materials can include a broad range of compelled evidence, the improper disclosure of which can impact privacy rights, privilege rights, the criminal justice system, Crown immunity and the administration of justice. When electronic evidence is seized in the course of a regulatory or criminal investigation, potential issues arise regarding section 8 of the Canadian Charter of Rights and Freedoms and an accused's right to a fair trial.[207] Where electronic evidence has been seized, warrants and various search and seizure provisions of the *Criminal Code* can be implicated.[208]

Materials seized pursuant to warrant or other regulatory compulsion will often be much broader in scope than what would be disclosed in a civil proceeding. Where the requested electronic evidence forms part of a parallel criminal investigation, prior to use or disclosure in any other proceeding, the principles and screening process identified in *D.P. v. Wagg*[209] should be applied to obtain the appropriate court orders to protect, as necessary, privacy rights and privilege rights.[210] Prior to the dis-

207. See e.g. *Kelly v. Ontario*, [2008] OJ No 1901, 91 OR (3d) 100 (CanLII) (ON SC). At issue in *Kelly* were the seizure of a computer in a child pornography investigation and the claims that the seizure and cross-forum disclosure violated the accused's Charter rights. See also the related decisions *College of Physicians and Surgeons of Ontario v. Peel Regional Police*, 2009 CanLII 55315 (ON SCDC), and *Kelly v. Ontario*, 2014 ONSC 3824 (CanLII) [*College of Physicians*].

208. *Criminal Code* RSC, 1985, c C-46.

209. *Wagg, supra* note 197.

210. The need to obtain consent of the Crown is also required in parallel regulatory proceedings, even where the regulatory body has the statutory

closure of evidence obtained in a criminal investigation, the process identified in *Wagg* requires the Crown to be notified and provided the opportunity to review the materials for third-party privacy and public interest concerns.[211]

Regulatory bodies also have the ability to compel the production of evidence through enforcement provisions in the governing legislation.[212] In addition to the power to compel, the regulatory body may have the power to control subsequent disclosure and use of the compelled evidence.[213] It is important to note, however, that where a regulatory body seeks access to criminal investigation materials, it must also comply with the general principles in *Wagg* and provide the Crown the opportunity to raise public interest concerns that may militate against production.[214]

Matters that involve cross-border criminal or regulatory proceedings require particular consideration of the different

---

ability to compel evidence. See *College of Physician and Surgeons of Ontario v. Peel Regional Police*, [2009] OJ No 4091, 98 OR (3d) 301 (CanLII) (ONSCDC).

211. To obtain and use criminal investigation materials in a civil proceeding in Ontario, a motion pursuant to Rule 30.10 of the *Rules of Civil Procedure* would be brought on notice to the Attorney General.

212. For example, sections 11 through 13 of the Ontario *Securities Act*, RSO 1990, c S.5, and sections 142–144 of the British Columbia *Securities Act*, RSBC, C 418, provide for the issuance of Investigation Orders and the appointment of an investigator, and also outline the power of the authority to compel evidence.

213. For example, Ontario *Securities Act*, *supra* note 212, s 16–18, and *BC Securities Act*, RSBC, 1996 c 418, s 148, gives the respective Commissions the ability to limit and place restrictions on the subsequent disclosure or use of the seized evidence.

214. *College of Physicians and Surgeons of Ontario v. Metcalf*, (2009) 98 O.R. (3d) 301, 2009 CanLII 55315 (ON SCDC), see paras 68–77.

self-incrimination and procedural protections afforded to witnesses. For example, witnesses in Canada are entitled to protection under section 15 of the *Canada Evidence Act* and related provincial legislation,[215] which restricts the use of compelled testimony in other proceedings. In such cross-border situations, the Court may impose terms on any orders compelling the protected evidence.[216]

Comment 10.b.ii. Arbitration

Compared to domestic court litigation, the scope of document production is generally narrower in arbitration proceedings.

Particularly in international arbitration, and subject to the rules specified in the arbitration agreement, a party is typically required to produce only the documents upon which it relies and those responsive to focused requests made by the other party. Some assistance in defining an appropriate standard for document production in arbitration may be derived from the International Bar Association's *Rules on the Taking of Evidence in International Arbitration* (the "*IBA Rules*").[217] Article 3 of the *IBA Rules* provides an "admirably clear" process by which requests for documents are made, the requested documents are either produced or objection is made to the request, and any remaining disputes are resolved by the tribunal—importantly, and

215. *Canada Evidence Act*, RSC 1985, c C-5; see also the *Ontario Evidence Act*, RSO 1990 c E.23.

216. See e.g. the principle in a civil case, *Treat America Limited v. Nestle Canada Inc.*, 2011 ONSC 617 (CanLII); and *Treat America Limited v. Nestlé Canada Inc.*, 2011 ONCA 560 (CanLII).

217. *IBA Rules on the Taking of Evidence in International Arbitration* (29 May 2010), online: International Bar Association <www.ibanet.org> [*IBA Rules*].

consistent with the *Sedona Canada Principles*, against a clear standard of both relevance and materiality to the outcome of the dispute, as well as considerations of proportionality and burden.[218] The *IBA Rules* provide that a party seeking document production in an arbitration should frame the request with some precision, ideally identifying particular documents but at least referring to the desired category of documents. Unless the mere fact of the other party's possession of the documents is relevant, only documents that are not otherwise available to the requesting party from other sources should be sought.[219]

While the scope of production in domestic arbitration proceedings more frequently approaches that of domestic court litigation, the flexibility of the arbitral process provides the opportunity to more readily limit document production in accordance with principles of proportionality. Indeed, although the *IBA Rules* were developed in the international commercial arbitration context, "the rules provide a very helpful framework for the production and exchange of documents in any arbitration, whether international or domestic."[220]

With respect to the production of electronic information, the commercial arbitration field faces much of the same pressures as the litigation field, as commentators have noted.[221] Fortunately, the flexibility that is inherent in the arbitral process, if

---

218. Nigel Blackaby and Constantine Partasides, *Redfern and Hunter on International Arbitration*, 5th ed. (Oxford: Oxford University Press, 2009) at 6.108.

219. *IBA Rules*, *supra* note 217 at art 3.

220. J. Brian Casey, *Arbitration Law of Canada: Practice and Procedure*, 2nd ed. (Huntington, New York: JurisNet LLC, 2011) at 204.

221. See e.g. Richard D. Hill, *The New Reality of Electronic Document Production in International Arbitration: A Catalyst for Convergence?* (2009) 25:1 Arb.

harnessed by counsel and arbitrators, may assist in managing the issue more effectively. The *Sedona Canada Principles* provide a useful framework for addressing these issues in the arbitration context. Indeed, referring to the Sedona Conference's *Sedona Principles*,[222] developed for a United States audience, one commentator has observed that they "reflect the concern of the *IBA Rules* for reasonableness and proportionality, avoiding overly burdensome document production requests, and permitting data sampling, searching and selection criteria to be employed to satisfy a party's good-faith obligation to produce."[223]

Parties engaged in arbitration proceedings should be aware that, while the scope of their production obligation may be more limited, it may be important to account for possible other proceedings in which the scope of that obligation may be broader. Efficiencies of scale and scope can be obtained by integrating those other proceedings with the project plan developed for the arbitration proceedings. Conversely, projects developed to collect and process ESI for litigation proceedings should account for and include both the categories of ESI likely to be relied upon by the party in related arbitration proceedings, and the ESI that can reasonably be anticipated to be requested by other parties in the arbitration proceedings. While the actual

---

Intl at 87; and Robert H. Smit & Tyler B. Robinson, *E-Disclosure in International Arbitration*, (2008) 25:1 Arb Intl at 105.

222. See The Sedona Conference, *The Sedona Principles Addressing Electronic Document Production, Second Edition* (2007), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/81> [*U.S. Sedona Principles*].

223. Richard D. Hill, *The New Reality of Electronic Document Production in International Arbitration: A Catalyst for Convergence?* (2009) 25:1 Arb Intl at 93. See also Nigel Blackaby and Constantine Partasides, *Redfern and Hunter on International Arbitration*, 5th ed. (Oxford: Oxford University Press, 2009) at 6.117–6.123.

scope of production may be more limited in arbitration proceedings, the initial scope of preservation and collection generally does not differ materially in practice.

Principle 11. Sanctions should be considered by the Court where a party will be materially prejudiced by another party's failure to meet its discovery obligations with respect to electronically stored information.

In certain circumstances, when parties fail to meet their discovery obligations for ESI, the fair administration of justice may be undermined. Absent appropriate sanctions for intentional, bad faith or reckless destruction or non-production of electronic evidence, the advantages that a party may receive from such conduct (e.g. having actions brought against them dismissed for lack of evidence or avoiding potential monetary judgments) may create inappropriate incentives regarding the treatment of ESI.

Not all non-production is intentional or the result of bad faith or recklessness. Given the continuing changes in information technology, the volatility and rapid obsolescence of certain forms of ESI and the burdens and complications that will inevitably arise when dealing with growing volumes of ESI, litigants may inadvertently fail to fully preserve or disclose all relevant material. In considering the impact of non-preservation or non-production, the role of the Court is to weigh the context, scope and impact of nondisclosure and to impose appropriate sanctions proportionate to the culpability of the non-producing party, the prejudice to the requesting party and the impact that the loss of evidence may have on the Court's ability to fairly dispose of the issues in dispute.

In some cases, it will be important to distinguish between penalties imposed for deterrent purposes on a wrongdoer whose conduct has resulted in spoliation or non-production,

and remedies made available to the requesting party who may have been prejudiced, even without any intent or ill will on the part of the responding party. Courts should be flexible in tailoring penalties and remedies to suit the particular case.

Comment 11.a. The Law of Spoliation

In the common law provinces in Canada, the common law that governs the destruction of evidence (i.e. spoliation) continues to develop, particularly as its principles apply to ESI. The law of spoliation originates from the principle of "*omnia praesumuntur contra spoliatorem*," an evidentiary principle that permits a court to draw a negative inference against a party that has been guilty of destroying or suppressing evidence.[224]

In Nova Scotia, the rules of civil procedure have been amended to include provisions that expressly deal with the duties to preserve and disclose electronic information, and the consequences of their breach.[225]

---

224. *Zahab v. The Governing Council of the Salvation Army in Canada et al* (2008) CanLII 41827 at para 20 (ON SC), citing *Prentiss v. Brennan*, [1850] OJ No 283 (Upper Canada Court of Chancery). But see *Gladding Estate v. Cote*, 2009 CarswellOnt8102 at para 36, 55 ETR (3d) 191 (SCJ): The court will only draw a negative inference where there is "real and clear evidence of tampering."

225. Rules 16.13 and 16.15 address destruction of electronic information, providing that deliberate or reckless deletion of relevant electronic information (and related activities) may be dealt with under Rule 88—Abuse of Process. Rule 88 lists various remedies for an abuse of process. Such remedies include an order for dismissal or judgment, an order to indemnify the other party for losses resulting from the abuse and injunctive relief. Nova Scotia *Civil Procedure Rules*, Royal Gazette Nov 19, 2008, online: The Courts of Nova Scotia <http://www.courts.ns.ca?Rules/toc.htm>.

The most comprehensive review of the Canadian jurisprudence on the common law of spoliation is found in *McDougall v. Black and Decker Canada Inc*.[226] In that decision, the Court summarized the Canadian law of spoliation in the following way:

- Spoliation currently refers to the intentional destruction of relevant evidence when litigation is existing or anticipated.[227]
- The principal remedy for spoliation is the imposition of a rebuttable presumption of fact that the lost or destroyed evidence would be detrimental to the spoliator's cause. The presumption can be rebutted by evidence showing the spoliator did not intend, by destroying the evidence, to affect the litigation, or by evidence to prove or defend the case.
- Even where evidence has been unintentionally destroyed, remedies may be available in the Court's rules and its inherent ability to prevent abuse of process. These remedies may include such relief as the exclusion of expert reports and the denial of costs.
- The courts have not yet found that the intentional destruction of evidence gives rise to an intentional tort, nor that there is a duty to preserve evidence for purposes of the law of negligence,

226. 2008 ABCA 353 (CanLII) at para 29.

227. See also *Stilwell v. World Kitchen Inc.,* 2013 ONSC 3354 (CanLII) at para 55 and *Blais v. Toronto Area Transit Operating Authority*, 2011 ONSC 1880 (CanLII) at para 72.

although these issues, in most jurisdictions, remain open.

- Generally, the issues of determining whether spoliation has occurred and what is the appropriate remedy for spoliation are matters best left for trial where the trial judge can consider all of the facts and fashion the most appropriate response.
- Some pretrial relief may be available in the exceptional case where a party is particularly disadvantaged by the destruction of evidence. Generally, this is accomplished through the applicable rules of court, or the Court's general discretion with respect to costs and the control of abuse of process.

As noted, there is an open question as to whether spoliation exists as an independent tort in Canada.[228] The British Columbia Court of Appeal in *Endean v. Canadian Red Cross Society*[229] held that spoliation will not ground an independent tort. The question, however, remains unsettled in other Canadian jurisdictions.

---

228. *See Spasic (Estate) v. Imperial Tobacco Ltd.* [2000] OJ No 2690 (ON CA), 49 OR (3d) 699, 2000 CanLII 17170 (CA) (SCC denied leave to appeal). In *Spasic*, the defendant brought a motion to strike certain paragraphs of the plaintiff's statement of claim on the basis that they disclosed no reasonable cause of action. The Motions Judge granted the motion at first instance for the paragraphs regarding the claims for spoliation on the grounds that a separate cause of action for spoliation did not exist in Ontario. On appeal, the Court of Appeal held that the claims for spoliation should not be struck out and that the claims pleaded should be allowed to proceed to trial as the few Canadian cases which have considered the issue were not definitive.

229. [1998] BCJ No 724 (BC CA), 157 DLR (4th) 465 (CanLII).

Significant judicial attention has been directed towards making proactive orders intended to ensure that documents are preserved as early as possible, whether in the form of Anton Piller orders or through more conventional document preservation orders.[230] Where such orders are sought, followed and enforced, evidence may remain available, avoiding the need for consideration of spoliation altogether.

Comment 11.b. Sanctions for Spoliation and Nondisclosure

Canadian jurisprudence regarding the appropriate response to a party's failure to comply with its document discovery obligations is limited but developing.[231] Courts have a wide discretion to impose suitable sanctions proportionate to the nature of the nondisclosure and its relative seriousness in the particular context.

While remedies for spoliation are generally considered at trial, pretrial relief for spoliation may be available in the exceptional case where a party is particularly disadvantaged by the destruction of evidence. Generally, where pretrial relief is awarded, the facts show either intentional conduct or indicate that a litigant or the administration of justice will be prejudiced

230. *CIBC World Markets Inc. v. Genuity Capital Markets*, 2005 CanLII 3944 (ON SC); *Canadian Derivatives Clearing Corp. v. EFA Software Services Ltd.*, 2001 ABQB 425 (CanLII); *Portus Alternative Asset Management Inc. (Re)* (2005), 28 OSC Bull 2670; *XY LLC v. Canadian Topsires Selection Inc.*, 2013 BCSC 780 (CanLII) and *Teledyne Dalsa, Inc. v. BinQiao Li*, 2014 ONSC 323 (CanLII).

231. Note that there is considerable U.S. jurisprudence on the issue of sanctions for spoliation; however, US jurisprudence should be considered only persuasive, given the significant differences in rules of court including cost consequences for nondisclosure and spoliation.

in the preparation of the case for trial.[232] Courts have awarded pretrial relief for spoliation through the applicable rules of court, or the Court's general discretion with respect to costs and the control of abuse of process.[233]

Courts may make such orders as are necessary to sanction parties appropriately for nondisclosure, particularly the intentional or reckless destruction of ESI. Canadian courts have shown a willingness to order production of documents, including ESI,[234] with sanctions following a party's noncompliance with such an order. Generally, deficiencies in disclosure have been reflected in an award of costs (whether for the other party's out-of-pocket expenses or wasted costs)[235] or the drawing of an adverse inference.[236] Other conditions may be imposed, including restrictions on the use of records subsequently located.[237] Other possible direct remedies include punitive monetary awards, jury instructions by the judge, exclusion of testimony or exhibits, findings of liability and case dismissal. Absent bad faith or significant prejudice, however, the consensus of the

---

232. *Cheung v. Toyota*, 2003 CanLII 9439 (ON SC); *Western Tank & Lining Ltd. v. Skrobutan*, 2006 MBQB 205 (CanLII).

233. *McDougall v. Black & Decker Canada Inc*., 2008 ABCA 353 (CanLII) at para 29; see also *Chow-Hidasi v. Hidasi*, 2013 BCCA 73 (CanLII), which confirms that spoliation requires intentional conduct (with "intentional" defined as "knowledge that the evidence would be required for litigation purposes" at para 29).

234. See e.g. *Spar Aerospace Limited v. Aerowerks Engineering Inc.*, 2007 ABQB 543 (CanLII), in which the Court ordered production of a party's hard drives.

235. *Farro v. Nutone Electrical Ltd.* (1990), 72 OR (2d) 637 (CanLII) (CA); *Endean v. Canadian Red Cross Society*, 1998 BCJ No 724, 157 DLR (4th) 465 (CanLII) (BCCA).

236. *Logan*, *supra* note 125.

237. *Jay v. DHL*, 2009 PECA 2 (CanLII).

Working Group is that striking a pleading may be too harsh in most circumstances.

The factors for determining the appropriate sanction for failure to comply with the obligation to disclose documents (or for other similar failures) were considered in *Zelenski v. Jamz*.[238] The Court held it was appropriate to take into account such factors as: 1) the quantity and quality of the abusive acts; 2) whether the abusive acts flow from neglect or intent; 3) prejudice, in particular with respect to the impact of the abuse on the opposing party's ability to prosecute or defend the action; 4) the merits of the abusive party's claim or defence; 5) the availability of sanctions short of dismissal that will address past prejudice to the opposing party; and 6) the likelihood that a sanction short of dismissal will end the abusive behaviour.

In *Brandon Heating and Plumbing (1972) Ltd. et al v. Max Systems Inc.*,[239] the plaintiff provided undertakings to preserve certain hardware, disks and documents as they were key to the defendant's defense. Instead, however, the hardware and software were replaced as part of the normal replacement cycle, making the evidence unavailable. The Court concluded the destruction was a willful act and the resulting prejudice was sufficient to lead to the dismissal of the plaintiff's case.

Comment 11.c. Rebutting the Presumption of Spoliation

Unlike in the United States, where Rule 37(f) of the Federal Rules of Civil Procedure (FRCP) provides for a formal "safe harbor" for the routine, good-faith operation of an electronic information system which results in the destruction or deletion of

238. *Zelenski v. Zelenski*, 2004 MBQB 256, 189 Man.R. (2d) 151 (CanLII).

239. 2006 MBQB 90, 202 Man R (2d) 278 (CanLII).

electronic evidence,[240] no formal exemption or defense against spoliation exists in Canadian court rules. The Canadian common law jurisprudence, however, reveals that courts make inquiries into the circumstance in which evidence becomes unavailable, and parties that can show that evidence became unavailable under reasonable circumstances may be able to rebut the presumptions which favour sanctions.[241]

Where a responding party asserts that a record no longer exists, a court may make an inquiry into the records management practices and policies of that party. For example, in *HMQ (Ontario) v. Rothmans Inc.*, Master Short stated that the document retention policies were relevant to the issues on the motion, and "[t]o the extent that such a policy would suggest whether, at any particular time period, a specific type of document, would or

240. Rule 37(e) provides that, absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide ESI lost as a result of the routine, good-faith operation of an electronic information system. It responds to the routine modification, overwriting and deletion of information from the normal use of electronic information systems and is intended to capture the alteration or overwriting of information that takes place without the operator's specific direction or awareness. US jurisprudence, however, suggests that the protections of FRCP Rule 37(e) applies only to information lost due to the routine operation of an information system, and only if such operation was in good faith: "The good faith requirement of Rule 37(f) [later renumbered to 37(e)] means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve." Committee Notes on Rules—2006 Amendment, online: <http://www.law.cornell.edu/rules/frcp/rule_37>. A revised Rule 37(e) ("Failure to Preserve Electronically Stored Information" [with a proposed heading in which "Preserve" replaces "Provide"] has been approved by the United States Judicial Conference and is pending Supreme Court Review as of the time of this publication.)

241. *Leon v. Toronto Transit Commission*, 2014 ONSC 1600 (CanLII) and *Stilwell v. World Kitchen Inc.*, 2013 ONSC 3354 (CanLII).

would not have been retained (and for how long) is helpful."[242] It is generally settled in Canada that records disposal under a reasonable records management policy, made in the usual and ordinary course of business, in compliance with regulatory and statutory requirements and in the absence of a legal hold, is valid and will rebut an inference of spoliation.[243] In contrast, courts have been willing to draw adverse inferences in circumstances where litigants have failed to produce relevant records and no retention policy exists,[244] and where a failure to produce a document is tied to the destruction of a document through an ad hoc procedure.[245]

Similarly, if an organization has an information governance or records management policy for retaining documents but does not follow its own policy and destroys relevant documents inconsistently with that policy, further discovery is appropriate both on the merits and to determine whether spoliation has occurred.[246]

---

242. *HMQ (Ontario) v. Rothmans Inc.*, 2011 ONSC 1083 (CanLII) at para 92.

243. *Stevens v. Toronto Police Services Board*, 2003 CanLII 25453 (ON SC). See also *Moutsios c Bank of Nova Scotia*, [2011] QJ No 1014 at para 19, 2011 QCCS 496 (CanLII) (Madame Justice Picard), in which the Court held that the bank's policy of disposing of all closed and inactive documents after six years was reasonable. To require the bank to retain guaranteed investment certificates to prove payment of these certificates would force the bank to retain its documents *ad infinitum* and that was unreasonable.

244. *Fareed v. Wood,* 2005 CanLII 22134 (ON SC); *Sunderji v. Alterna Savings*, 2010 ONSC 1223 (CanLII).

245. *Moezzam Saeed Alvi v. YM Inc.* (2003) OJ No 3467, [2003] OTC 799 (ON SC) (CanLII); *Ontario v. Johnson Controls Ltd*. (2002) OJ No 4725, [2002] OTC 950 (CanLII) (ON SC).

246. *Apotex Inc. v. H. Lundbeck A/S*, [2011] FC 88, 91 CPR (4th) 274 (CanLII).

Canadian courts have not as yet addressed the issue of parties having document retention policies with deliberately-set short retention periods after which documents are destroyed, so that destruction will happen as a matter of course before any obligation to preserve has arisen. If a policy is designed to defeat the ability of claimants to obtain evidence where the destroying party knew the destroyed documents could be relevant, however, a court may be inclined to fashion appropriate sanctions or remedies.

Finally, in some instances, parties have digitized records and can no longer produce the paper originals. The digitization of records will generally not be sufficient to ground a presumption of spoliation. For the purpose of determining admissibility of digitized electronic records in lieu of paper originals, some jurisdictions permit evidence to be presented regarding standards and best practices used by organizations and applied to the creation and storage of the digitized records.[247]

---

247. See *Canada Evidence Act*, RSC 1985, c C-5, s. 31.2; Alberta *Evidence Act*, RSA 2000, c A-18 s. 41.4; Saskatchewan *Evidence Act*, SS 2006, c E-11.2, s. 56; Manitoba *Evidence Act*, CCSM c E150, s. 51.3; Ontario *Evidence Act*, RSO 1990, c E.23, 34.1(5.1); Nova Scotia *Evidence Act*, RSNS 1989, c 154, s. 23D; An *Act to Establish a Legal Framework for Information Technology*, CQLR c C-1.1, s. 6.; and see reference to section 23(F) of the *Evidence Act*, RNS, 1989, c 154 by *Saturley v CIBC World Markets Inc.*, [2012] NSJ No 313, 2012 NSSC 226, 317 NSR (2d) 388, 2012 NSSC 226 (WL). These standards are not mandatory. Some common standards in use by organizations include: the Canadian General Standards Board, online: Public Works and Government Services Canada <http://www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-eng.html>; Standards Council of Canada, CAN/CGSB 72.34-2005 Electronic Records as Documentary Evidence, online: Standards Council of Canada <http://www.scc.ca/en/standardsdb/standards/22952>; Standards Council of Canada, Micrographics and Electronic Images as Documentary Evidence (CAN/CGSB-72.11-93 as amended 2000); International Organization for Standardization

The costs of identifying potentially relevant ESI can, in many cases, be reduced in circumstances where an organization has a well-designed and implemented information governance and records management policy ("Information Governance Policy"). Such a policy can serve as a guide in identifying the type, nature and location of information (including ESI) that is relevant to the legal proceeding as well as the potential sources of data. An Information Governance Policy could also include:

- information about an organization's information governance structure as reflected in a data map;[248]
- guidelines for the routine retention and destruction of ESI as well as paper, and for necessary modifications to those guidelines in the event of litigation;
- processes for the implementation of legal holds, including measures to validate compliance;

(ISO), ISO/CD 15489-1 Information and Documentation Records Management, Part 1 and Part 2, online: ISO <http://www.iso.org/>; Guidelines ISO/TR15489-2, online: ISO <http://www.iso.org/>; and ARMA International's Generally Accepted Recordkeeping Principles® (The Principles®), online: ARMA <http://www.arma.org>.

248. A data map is a visual reproduction of the ways that ESI moves throughout an organization, from the point it is created to its ultimate destruction as part of the organization's information governance and document retention program. Data maps address how people within the organization communicate with one another and with others outside the organization. A comprehensive data map provides legal and IT departments with a guide to the employees, processes, technology, types of data and business areas, along with the physical and virtual locations of data throughout the organization. It includes information about data retention policies and enterprise content management programs and identifies servers that contain data for various departments or functional areas within the organization.

- processes for auditing IT practices to control data proliferation (redundant backups, use of links to documents rather than attachments, etc.) and to institutionalize other good record-keeping practices; and
- guidelines on the use of social media in the business context.

It should also be noted, however, that in cases involving allegations of fraud, conspiracy, misappropriation of funds or unlawful disclosure of confidential information, the relevant ESI (which would likely include the metadata) may include records beyond the category of business records listed in the Information Governance Policy. Thus, while an Information Governance Policy should be consulted at the identification and preservation stages of e-discovery, the examination and consideration of such a policy should not limit the level of inquiry to only those types of records listed in the Information Governance Policy.

Effective information governance and records management policies will enable the parties to present a more accurate picture of the cost and burden to the Court when refusing further discovery requests, or when applying for orders shifting costs to the receiving party in appropriate cases. A detailed discussion of information governance and records retention policies is beyond the scope of this paper. Readers are encouraged to consult The Sedona Conference's *Commentary on Information Governance.*[249]

249. The Sedona Conference, *Commentary on Information Governance* (December 2013), online: The Sedona Conference <https://www.thesedonaconference.org/download-pub/3421>.

Principle 12. The reasonable costs of all phases of discovery of electronically stored information should generally be borne by the party producing it. In limited circumstances, it may be appropriate for the parties to arrive at a different allocation of costs on an interim basis, by either agreement or court order.

In most Canadian provinces and territories, the costs of discovery are traditionally borne by the producing party and any shifting of costs to the receiving party typically occurs at the end of the litigation, at which time an unsuccessful receiving party may be required to contribute, in whole or in part, towards the costs (fees and disbursements) of the successful party.[250] This generally includes allocation of the costs of producing ESI. This can be contrasted with the practice when paper

250. See e.g. Supreme Court of British Columbia, *Practice Direction Re: Electronic Evidence* (July 2006) at s 3.1, online: The Courts of British Columbia <http://www.courts.gov.bc.ca/supreme_court/practice_and_procedure/electronic_evidence_project.aspx>. The Practice Direction provides that the reasonable costs of complying with the Practice Direction, "including the expenses of retaining or utilizing necessary external or in-house technical consultants," may be claimed as costs under the *Rules of Court*. See also *Doucet v. Spielo Manufacturing Inc*., 2012 NBQB 324 (WL). At issue was an assessment of the defendant's Bill of Costs following completion of a trial and appeal. Prior to trial, a document production order had been made requiring the defendants to provide the plaintiff with access to their computer system. The Motions Judge was aware, when the order was made, of the potential cost and extent of the operation. An amount of $40,000 was the estimated cost stated at the motion hearing. The final cost was $22,926.81. Despite the plaintiff's argument that the defendants could have fulfilled the order through a more economical method, the Registrar awarded the defendants the full costs of the computer consultant's report. While the defendants were the producing party, and therefore incurred the costs arising during the pretrial phase, the defendants were ultimately successful at trial and therefore entitled to reimbursement of these costs by the plaintiff, in accordance with the

documents are produced where the receiving party has traditionally been responsible for the immediate costs of the production, such as copying, binding and delivery costs.

While litigants are properly expected to bear the costs, on at least an interim basis, of producing ESI in the ordinary course, different considerations are engaged when extraordinary effort or resources will be required to first restore data to an accessible format (e.g. accessing disaster recovery tapes, residual data or data from legacy systems). In such cases, if the data is producible at all, requiring the producing party to fund the significant costs associated with restoring such data may be unfair, and may hinder the party's ability to litigate the dispute on the merits. Accordingly, it may be appropriate that the party requesting such extraordinary efforts should bear, at least on an interim basis, all or part of the costs of doing so. Parties are encouraged to consider these issues when they negotiate a discovery plan.[251]

In Canada, a court is empowered to order that the costs of producing accessible ESI be shifted in certain circumstances.[252] In deciding whether to make an order on an interim

---

traditional approach to discovery costs. See also *Bank of Montreal v. 3D Properties,* [1993] SJ No 279 at para 30, 111 Sask. R 53 (WL) (QB): "All reasonable costs incurred by the plaintiff, including *inter alia*, searching for, locating, editing and producing said 'documents': computer records, discs and/or tapes for the applicant shall be at the applicant's cost and expense."

251. See Supreme Court of British Columbia, *Practice Direction Re: Electronic Evidence* (July 2006) at s 6 online: The Courts of British Columbia <http://www.courts.gov.bc.ca/supreme_court/practice_and_procedure/electronic_evidence_project.aspx>, which recommends that parties consider the issue of transferring the costs of the search for, and the discovery of, ESI.

252. See e.g. *Warman v. National Post Company*, 2010 ONSC 3670 (CanLII), in which the Master held that the costs of the expert who would conduct a forensic examination of a limited subset of the data on the plaintiff's hard drive would be paid initially by the defendant seeking production of the

basis shifting the costs of production of electronically stored information, the Working Group recommends that a court consider the following factors:

1. whether the information is reasonably accessible as a technical matter without undue burden or cost;
2. the extent to which the request is specifically tailored to discover relevant information;
3. the likelihood of finding information that is important and useful;
4. the availability of such information from other sources, including testimony, requests for admission and third parties;
5. the producing party's failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessible sources, and the reasons for that lack of availability;
6. the total cost of production (including the estimated costs of processing and reviewing retrieved documents), compared to the amount in controversy;
7. the total cost of production (including the estimated costs of processing and reviewing retrieved documents), compared to the resources available to each party;

---

drive, with the ultimate responsibility for that expense being in the discretion of the Trial Judge. In addition, in *Borst v. Zilli*, 2009 CanLII 55302 (ONSC), the Court found that the plaintiffs' request to conduct an inspection of the defendant's electronic data was similar to a request to inspect property under Rule 32 of the Ontario *Rules of Civil Procedure*. The costs of such inspection by an independent computer consultant were therefore to be borne by the plaintiffs. The Court did order that the costs of an independent solicitor to review the documents for privilege and relevance were to be shared by the parties given that such review could have been done by defendant's counsel but the plaintiff refused that option.

8. other burdens placed on the producing party, including disruption to the organization, lost employee time and other opportunity costs;
9. the relative ability of each party to control costs and its incentive to do so;
10. the importance of the issues at stake in the litigation; and
11. the relative benefits to the parties of obtaining the information.[253]

Courts still often continue to follow the traditional rule and refuse to shift the costs of production of ESI at the discovery stage. In *Gamble v. MGI Securities*,[254] the Court ordered the defendant to deliver its productions in CSV format and refused to shift the costs of doing so to the plaintiff. In doing so, the Court took into account The Sedona Canada Principle 12 and the disparity in the parties' abilities to pay for production. Similarly, in *GRI Simulations Inc. v. Oceaneering International Inc.*,[255] the Court found no reason to depart from the traditional approach to costs at the production stage. Costs were therefore to be borne by the producing party.

E-discovery may involve significant internal client costs as well as counsel fees and disbursements for outsourced services. There may be a need for the cost rules to be clarified so that internal discovery costs are regarded as a recoverable disbursement in appropriate cases. Disbursements made to a third party or billed to a client for electronic document management

253. See the discovery plan and proportionality rules under the *Ontario Rules*, *supra* note 10 (Rules 29.1 and 29.2); [U.S.] Federal Rules of Civil Procedure 26(b)(2)(B); *U.S. Sedona Principles*, *supra* note 222, Comment 13.a.

254. *Gamble v. MGI Securities*, 2011 ONSC 2705 (CanLII).

255. *GRI Simulations Inc. v. Oceaneering International Inc.*, 2010 NLTD 85 (CanLII). See also *Veillette v. Piazza Family Trust*, 2012 ONSC 5414 (CanLII).

should now be considered a standard disbursement.[256] These costs could also, therefore, be subject to a cost-shifting order.

As e-discovery costs may be significant and given that cost shifting occurs relatively infrequently, parties should adopt strategies to control the costs of e-discovery. Good Information Governance policies and practices are the most proactive method of reducing costs associated with e-discovery and maintaining proportionality in the discovery process.[257] Given the potential for an interim cost award in an e-discovery context, a party seeking production of electronic documents should also carefully consider the cost implications as early as possible.[258] A producing party may wish to limit the scope of its e-discovery obligations, through negotiation, appropriate admissions or motions. It may also wish to consider whether the costs should be partially or completely shifted to the receiving party.[259]

---

256. See *Harris v. Leikin Group*, 2011 ONSC 5474 (CanLII).

257. The Sedona Conference, *Commentary on Information Governance* (December 2013), *supra* note 249.

258. Some Canadian jurisdictions have practice directions in place for managing electronic evidence, including cost benchmarking. See e.g. Supreme Court of British Columbia, *Practice Direction Re: Electronic Evidence* (July 2006), online: The Courts of British Columbia <http://www.courts.gov.bc.ca/supreme_court/practice_and_procedure/electronic_evidence_project.aspx>; Sandra Potter, *Guidelines on Benchmarking of Costs*, online: Canadian Judicial Council <https://www.cjc-ccm.gc.ca/english/news_en.asp?selMenu=news_publications_en.asp>.

259. *Barker v. Barker*, 2007 CanLII 13700 (ONSC). The defendants moved for orders requiring the plaintiffs to pay one-third of the cost of scanning and coding the documents; the other two-thirds to be borne equally by the Crown and the defendant physicians. The motions were opposed by the plaintiffs. The Court agreed that the benefits to the plaintiffs justified an order for the sharing of the costs of conversion.

Shifting the costs of extraordinary discovery efforts, however, should not be used as an alternative to making a well-founded objection to undertaking such efforts in the first place. Extraordinary discovery efforts and any associated cost shifting should be required only where the requesting party demonstrates substantial need or justification. The courts should discourage burdensome requests that have no reasonable prospect of significantly contributing to the discovery effort, even if the requesting party is willing to pay.

SSPPU: A TOOL FOR AVOIDING JURY CONFUSION

*Mark Snyder**

INTRODUCTION

The law of patent infringement damages has long relied principally on the construct of a hypothetical negotiation between a patent owner and an infringer. That construct requires a fact finder to determine a reasonable royalty by applying economically sound principles. In most cases, one or more of the factors set forth in *Georgia-Pacific* are used to guide the fact finder in its task. The reasonable royalty framework—and the *Georgia-Pacific* analysis in particular—has long been notable for its adaptability to a variety of factual circumstances, an attribute that is sensible in light of the statutory requirement that the patentee be compensated "for the use made of the invention by the infringer." Recently, however, there has been a concerted effort to impose a rigid structure on the calculation of a reasonable royalty to put downward pressure on the royalties paid for those patented technologies. Certain advocates urge the use of a concept known as "smallest salable patent-practicing unit" ("SSPPU"), as a one-size-fits-all methodology for calculating a reasonable royalty. Nowhere is this more evident than in the debate involving valuation of standards-essential patents ("SEPs")—those patents that are necessarily infringed by products that practice a technical standard that reads on those patents.

 Mr. Snyder is a Senior Vice President and Patent Counsel at Qualcomm Incorporated. The views and opinions expressed in this paper are those of the author, and not those of the author's employer.

But SSPPU cannot be transformed into something it is not. SSPPU was created as one tool judges could use as an evidentiary safeguard to mitigate the risk that jurors will be confused by high revenue numbers when calculating reasonable royalties and produce unreasonably high royalty awards. By focusing a jury on calculating a reasonable royalty based on the smallest salable patent practicing unit sold by the infringer, the court can avoid having the jury reach a damages verdict that is not consistent with the value that the infringer gains through use of the patented invention. For example, if the SSPPU is further incorporated into other products sold by the infringer, and the patentee cannot establish a basis for use of the entire market value of the accused product as the royalty base, then a court might instruct the jury only to consider the revenues from sales of the SSPPU when establishing a base for the calculation of a reasonable royalty. In doing so, SSPPU conceals from juries revenue numbers related to other potential bases an economist might consider for calculating damages. Far from being a substantive legal rule, SSPPU is a narrow tool to be used only in certain circumstances.

Nonetheless, there are advocates who urge that application of the SSPPU concept should be dramatically expanded. Some contend that SSPPU should be mandatory in all jury trials, even where there is no risk of confusion. Some contend that SSPPU should be mandatory in all patent trials of any kind. And some even go so far as to contend that SSPPU should control the range of acceptable royalties in *private* market transactions.

These absolutist proponents of SSPPU are mistaken in this respect, and this paper seeks to explain why. Part I of this paper provides some necessary background on the law of patent damages. Part II discusses the possible problem of jury confusion in patent trials, and how the problem may have its basis in a behavioral-economics concept called "anchoring." Part III

discusses SSPPU's origins and its treatment in the Federal Circuit. Finally, Part IV examines some of the problems associated with converting SSPPU from an evidentiary safeguard into a substantive rule of law.

THE REASONABLE ROYALTY DAMAGES FRAMEWORK

A finding of patent infringement entitles a patentee to "damages adequate to compensate for the infringement, but in no event less than a reasonable royalty for the use made of the invention by the infringer."[1] Whether this damages award takes the form of lost profits, a reasonable royalty, or a combination of the two, the damages floor is the same: "in no event less than a reasonable royalty."[2] So-worded, the statute has been interpreted as "expansive rather than limiting"—"[i]t affirmatively states that damages must be adequate, while providing only a lower limit and no other limitation."[3] Indeed, the Supreme Court has admonished courts not to invent limitations on patent infringement damages, explaining that "[w]hen Congress wished to limit an element of recovery in a patent infringement action, it said so explicitly."[4]

In determining a reasonable royalty, the best evidence of a *reasonable* royalty for a given patent is an *established* royalty for

---

1. 35 U.S.C. § 284.

2. Rite-Hite Corp. v. Kelley Co., 56 F.3d 1538, 1544–45 (Fed. Cir. 1995); *see also* DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc., 567 F.3d 1314, 1335 (Fed. Cir. 2009) (referring to "the statutory damages floor of 35 U.S.C. § 284").

3. *Rite-Hite Corp.*, 56 F.3d at 1544.

4. Gen. Motors Corp. v. Devex Corp., 461 U.S. 648, 653 (1983) (refusing to limit a court's authority to award interest); *see also* Bilski v. Kappos, 561 U.S. 593, 602 (2010) ("This Court has more than once cautioned that courts should not read into the patent laws limitations and conditions which the legislature has not expressed." (internal quotation marks omitted)).

that patent.[5] When an established royalty is unavailable, though, courts turn to a hypothetical negotiation between the plaintiff and the defendant.[6] This hypothetical negotiation "requires the court to envision the terms of a licensing agreement reached as the result of a supposed meeting between the patentee and the infringer at the time infringement began,"[7] and involves consideration of fifteen factors set forth in *Georgia-Pacific*.[8] Importantly, though, the hypothetical negotiation is "constructed on hypothetical assumptions," including infringement, validity of the patent, willingness of the parties to negotiate an agreement, and that the infringer's degree of efficiency is irrelevant.[9]

When the accused device contains both patented and unpatented features, measuring a reasonable royalty requires "a determination of the value added by such features," a process

---

5. *See* Monsanto Co. v. McFarling, 488 F.3d 973, 978–79 (Fed. Cir. 2007) ("An established royalty is usually the best measure of a 'reasonable' royalty for a given use of an invention because it removes the need to guess at the terms to which parties would hypothetically agree.").

6. *See id.* Infrequently courts use "the so-called 'analytical approach,'" which involves "subtract[ing] the infringer's usual or acceptable net profit from its anticipated net profit realized from sales of infringing devices." TWM Mfg. Co. v. Dura Corp., 789 F.2d 895, 899 (Fed. Cir. 1986). But the hypothetical negotiation framework is far more common. In fact, at times the Federal Circuit has defined a reasonable royalty based on a hypothetical negotiation. *See, e.g.*, Fujifilm Corp. v. Benun, 605 F.3d 1366, 1372 (Fed. Cir. 2010) ("To determine a reasonable royalty, a jury must find the royalty that would have been agreed to in a hypothetical negotiation between a willing licensee and willing licensors at the time infringement began.").

7. *Rite-Hite Corp.*, 56 F.3d at 1554.

8. *See* Georgia-Pacific Corp. v. U.S. Plywood Corp., 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970).

9. Aqua Shield v. Inter Pool Cover Team, 774 F.3d 766, 771 (Fed. Cir. 2014).

called "apportionment."[10] The Supreme Court articulated the apportionment rule well over a century ago in *Garretson v. Clark*: "The patentee . . . must in every case give evidence tending to separate or apportion the defendant's profits and the patentee's damages between the patented feature and the unpatented features, and such evidence must be reliable and tangible, and not conjectural or speculative."[11] "The essential requirement [of apportionment] is that the ultimate reasonable royalty award must be based on the incremental value that the patented invention adds to the end product."[12] Of course, a patented invention may contribute to *all* of the value of the end product. For this situation, courts have derived the "the entire market value rule" (or "EMVR"), which states that when the patented invention drives demand for the end product or substantially creates the value of the component parts, damages may likewise be based on the entire market value of the product.[13]

JURY TRIALS CAN PRESENT A UNIQUE APPORTIONMENT CONCERN

Because a reasonable royalty is a question of fact, juries are often responsible for apportionment.[14] In a jury trial, the jury must decide (usually after hearing from experts on both sides) how much value the patented invention adds to the infringing product(s) and then express their conclusion in the form of a royalty, often calculated by multiplying together a royalty base and a royalty rate. Logically, of course, apportionment may be

10. Ericsson, Inc. v. D-Link Sys., Inc., 773 F.3d 1201, 1226 (Fed. Cir. 2014).

11. 111 U.S. 120, 121 (1884) (internal quotation marks omitted).

12. *Ericsson*, 773 F.3d at 1226.

13. VirnetX, Inc. v. Cisco Sys., Inc., 767 F.3d 1308, 1326 (Fed. Cir. 2014).

14. *See* Riles v. Shell Expl. & Prod. Co., 298 F.3d 1302, 1308 (Fed. Cir. 2002).

accomplished by calibrating the royalty base "to reflect the value added by the patented feature," by calibrating the royalty rate "so as to discount the value of a product's non-patented features," or by some combination of the two.[15]

Some courts, however, have questioned whether juries are capable of this analysis. Specifically, the concern is that juries will produce excessive royalties when they rely on excessive royalty bases. Said another way, juries may be misled by large revenue numbers. In such situations, courts have discretion to devise mechanisms to avoid misleading the jury.[16]

In essence, the fear is "anchoring." Anchoring is the behavioral-economics term for the human tendency to rely too heavily on the first piece of information received. The concept was made famous by psychologists Amos Tversky and Daniel Kahneman, who posited that people often "make estimates by starting from an initial value that is adjusted to yield the final answer," but that those "adjustments are typically insufficient."[17] "That is, different starting points yield different estimates, which are biased toward the initial values."[18] As an example of this bias, Tversky and Kahneman described an experiment in which subjects were shown what they thought were randomly generated numbers (though in fact the numbers

15. *Ericsson*, 773 F.3d at 1226.

16. *Cf.* FED. R. EVID. 403 ("The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, *misleading the jury*, undue delay, wasting time, or needlessly presenting cumulative evidence." (emphasis added)).

17. Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124–31 (1974).

18. *Id.*

were always either 10 or 65), and then asked to estimate the percentage of African countries in the United Nations.[19] On average, the estimates tended toward the initial numbers—subjects shown 65 estimated a larger percentage of African countries in the United Nations, and subjects shown 10 estimated a smaller percentage of African countries in the United Nations.[20]

In the patent context, the "anchor" is the royalty base. If the royalty base is high, the argument goes, then the jury is in danger of deciding upon an excessive royalty, because the jury may not be capable of determining an appropriate royalty rate to be applied to that base.

Before moving to a supposed solution to this problem, one should consider whether there actually *is* a problem to solve. Juries are asked to unravel complex problems every day. To name just a few, juries are entrusted with cases involving commercial contracts, securities transactions, medical malpractice, antitrust violations, and products liability. Many of these cases require juries not only to hear and digest huge volumes of evidence, but also to apply detailed laws and standards to that evidence. Thus, to the extent that juries are worthy fact-finders in other complex cases, there is little basis for singling out apportionment as too complicated for juries.[21]

Even assuming that patent trials have an anchoring problem, it is important to keep in mind that calibrating an anchoring-minimizing royalty base in a particular jury trial requires a

19. *Id.*

20. *Id.*

21. *Cf. In re* U.S. Fin. Sec. Litig., 609 F.2d 411, 429–30 (9th Cir. 1979) ("The opponents of the use of juries in complex civil cases generally assume that jurors are incapable of understanding complicated matters. This argument unnecessarily and improperly demeans the intelligence of the citizens of this Nation. We do not accept such an assertion.").

judge to know at least the "right" magnitude of the royalty, which will vary by invention and by accused product. This necessitates addressing the issue case-by-case. One size does not fit all.

THE GENESIS AND EVOLUTION OF THE SSPPU CONCEPT

Judge Rader proposed a solution to the jury anchoring problem in *Cornell University v. Hewlett-Packard Co.*, minting the term "smallest salable patent-practicing unit."[22] The case concerned Cornell's patented "method for instruction issuance within a computer processor."[23] The claimed method was carried out within a component of an instruction reorder buffer within a computer processor.[24] The computer processors were further incorporated into CPU modules, which were further combined into CPU "bricks" that were ultimately assembled into a server.[25] Hewlett-Packard ("HP") sold computer processors, CPU modules, CPU bricks, and servers—many different products in the assembly chain of servers and workstations, all of which included the component that practiced the claimed invention. At first, Cornell's damages expert sought to testify to the jury that the appropriate royalty base was the entire market value of servers and workstations sold by HP.[26] But because the expert offered no reliable evidence to justify the use of the entire market value of the servers and workstations as the royalty

22. 609 F. Supp. 2d 279 (N.D.N.Y. 2009) [hereinafter *Cornell II*]. At the time, Judge Rader was a Circuit Judge of the United States Court of Appeals for the Federal Circuit, sitting by designation in the United States District Court for the Northern District of New York.

23. *Id*. at 283.

24. *Id.*

25. *Id.*

26. Cornell Univ. v. Hewlett-Packard Co., No. 01-CV-1974, 2008 WL 2222189, at *2 (N.D.N.Y. May 27, 2008) [hereinafter *Cornell I*].

base, Judge Rader excluded the testimony.[27] Undeterred by the court's admonition, the same expert next testified that a reasonable royalty should be calculated on the basis of CPU bricks sold by HP, the next rung in the assembly ladder of products sold by HP.[28] Judge Rader rejected this testimony for a lack of reliable supporting evidence to justify the use of the entire market value of the CPU bricks as the royalty base.[29] Running throughout these rulings was Judge Rader's concern that an unjustifiably large royalty base "would mislead the jury to award damages far in excess of their compensatory purpose."[30] No doubt the concern assumed even greater prominence for Judge Rader in light of the unwillingness of Cornell's expert to abide by the court's rulings.[31] In the end, Judge Rader concluded that the appropriate royalty base was the processor itself, which he dubbed the smallest salable patent-practicing unit sold by the infringer, HP.[32]

For Judge Rader, the SSPPU concept—applied to reduce the royalty base to the lowest rung in the infringing assemblies

27. *Id.* at *3–4.

28. *See Cornell II*, 609 F. Supp. 2d at 287–90.

29. *Id.*

30. *Id.* at 284.

31. *See id.* at 288 ("Indeed, on more than one occasion and in contravention of this court's order, Dr. Stewart continued to advise the jury that, in his opinion, server and workstation revenues were the appropriate royalty base. . . . Dr. Stewart's decision to cling to his excluded opinion is telling. Rather than present a damages case accounting for this court's order, Dr. Stewart and Cornell relied on the same evidence and reasoning that proved insufficient to support application of the entire market value rule in the server and workstation context only slightly revising those contentions to show entitlement to the entire market value of the CPU bricks.").

32. *Id.* at 292.

sold by HP—was no more than an evidentiary safeguard designed to avoid jury confusion. Indeed, it is not clear from the decision that Judge Rader considered SSPPU distinct from requiring the principled application of the EMVR where the infringer sold multiple subassemblies all containing the infringing technology. His *Cornell II* opinion neither announced a substantive rule, nor held that SSPPU was even relevant outside of the narrow set of facts before him. Under *Garretson*, the substantive rule is apportionment. And Judge Rader accomplished apportionment, in part, by rejecting an award of damages arrived at through an improper reference to the entire market value of the accused product, and instead, calculating the award using the smallest subassembly sold by the infringer that wholly contained the claimed invention.

Since *Cornell II*, only a few Federal Circuit cases have referred to SSPPU, and each opinion focused on the risk of jury confusion.[33]

Better than any other Federal Circuit opinion, *Ericsson, Inc. v. D-Link Sys., Inc.* carefully explained the critical distinction between "the substantive statutory requirement of apportionment" and the "evidentiary principle" to which SSPPU is linked:

---

33. *See, e.g.*, Ericsson, Inc. v. D-Link Sys., Inc., 773 F.3d 1201, 1226 (Fed. Cir. 2014) ("[C]are must be taken to avoid misleading the jury by placing undue emphasis on the value of the entire product."); VirnetX, Inc. v. Cisco Sys., Inc., 767 F.3d 1308 (Fed. Cir. 2014) (referring to "the fundamental concern about skewing the damages horizon" by "using a base that misleadingly suggests an inappropriate range" to the jury); LaserDynamics, Inc. v. Quanta Comput., Inc., 694 F.3d 51, 68 (Fed. Cir. 2012) ("Admission of such overall revenues, which have no demonstrated correlation to the value of the patented feature alone, only serve to make a patentee's proffered damages amount appear modest by comparison, and to artificially inflate the jury's damages calculation beyond that which is adequate to compensate for the infringement." (internal quotation marks omitted)).

> There is one substantive legal rule, and there is a separate evidentiary principle[.] . . . The essential requirement [of the substantive legal rule of apportionment] is that the ultimate reasonable royalty award must be based on the incremental value that the patented invention adds to the end product. Our cases have added to that governing legal rule an important evidentiary principle. The point of the evidentiary principle is to help our jury system reliably implement the substantive statutory requirement of apportionment of royalty damages to the invention's value. The principle, applicable specifically to the choice of a royalty base, is that, where a multi-component product is at issue and the patented feature is not the item which imbues the combination of the other features with value, care must be taken to avoid misleading the jury by placing undue emphasis on the value of the entire product. It is not that an appropriately apportioned royalty award could never be fashioned by starting with the entire market value of a multi-component product—by, for instance, dramatically reducing the royalty rate to be applied in those cases—it is that reliance on the entire market value might mislead the jury, who may be less equipped to understand the extent to which the royalty rate would need to do the work in such instances.[34]

There are three important points to note about *Ericsson*. First, no one who has read *Ericsson* can reasonably think that the concept of SSPPU is a substantive rule of Federal Circuit law.

34. *Ericsson*, 773 F.3d at 1226–27.

Ericsson left no room for doubt. Second, *Ericsson* did not say that the SSPPU concept is *itself* an evidentiary principle. The evidentiary principle "is that, where a multi-component product is at issue and the patented feature is not the item which imbues the combination of the other features with value, care must be taken to avoid misleading the jury by placing undue emphasis on the value of the entire product."[35] Indeed, the SSPPU concept is nothing more than a shorthand expression for the cautious application of the EMVR, and simply *one way* a court may administer the evidentiary principle of avoiding jury confusion. Third, *Ericsson* did not say that the evidentiary principle of avoiding jury confusion (which has always existed in the form of Federal Rule of Evidence 403) requires the exclusion of evidence in *every* jury trial. Only "*undue* emphasis on the value of the entire product" is a problem.[36] In cases where there is evidence supporting valuation of the patent by reference to the end product, the concept of SSPPU has not been used to restrict the jury's access to that evidence. Indeed, *Ericsson* itself affirmed the admission of expert testimony "regarding licenses in which royalties were set by reference to the value of an end product."[37] Whether emphasis on the value of the end product is "undue" will largely depend on the gap between the value added by the patented invention and the value of the end product. Put differently, the less important the patented invention is to the end product, the greater the potential risk that a jury will put too much emphasis on the value of the end product.

More recently, the *Ericsson* view of SSPPU was confirmed in *Commonwealth Scientific & Industrial Research Organisation v. Cisco Systems, Inc.* ("*CSIRO*"), where damages were calculated

35. *Id.* at 1226.

36. *Id.* (emphasis added).

37. *Id.* at 1227.

for infringement of a Wi-Fi SEP.[38] The infringer, Cisco, did not contest infringement or validity, and the parties agreed to a bench trial on damages.[39] Cisco proposed a damages model basing royalties on the prices of the chips used in implementing the 802.11 Wi-Fi standard—what Cisco contended was the SSPPU.[40] The district court rejected Cisco's damages model and created its own damages methodology, using the dollar-per-unit ranges of the parties' prior negotiations as a starting point and considering adjustments based on the *Georgia-Pacific* factors.[41]

On appeal, Cisco argued for a rule "which would require all damages models to begin with the smallest salable patent-practicing unit."[42] The Federal Circuit flatly rejected Cisco's rule as "untenable."[43] Instead, the Federal Circuit found that Cisco's proposed rule "conflicts with our prior approvals of a methodology that values the asserted patent based on comparable licenses," and noted *Ericsson*'s holding, "that otherwise comparable licenses are not inadmissible solely because they express the royalty rate as a percentage of total revenues, rather than in terms of the smallest salable unit."[44] The Federal Circuit thus made it clear that SSPPU is not the exclusive rule for determining reasonable-royalty damages in patent infringement cases.

38. 809 F.3d 1295 (Fed. Cir. 2015).
39. *Id*. at 1297–99.
40. *Id.* at 1299–1301.
41. *Id.* at 1299–1300.
42. *Id.* at 1303.
43. *Id.*
44. *Id.*

THE SSPPU CONCEPT IS NOT AND SHOULD NOT BECOME A SUBSTANTIVE LEGAL REQUIREMENT FOR PATENT DAMAGES

Despite the crystal-clear explanation in *Ericsson*—and the holding in *CSIRO*—there are those who seek to convert the concept of SSPPU into a mandatory legal rule. The extent of their misunderstanding ranges from "SSPPU should govern all jury trials," to "SSPPU should govern all trials," and even to "SSPPU should govern all *private* transactions." Contrary to these assertions, the SSPPU concept should not be converted into a mandatory legal rule.

Mandatory SSPPU Would Be Inconsistent with Apportionment.

Mandatory application of the concept of SSPPU in patent damages determinations would establish an artificial ceiling on royalties. If utilized as advocated by some, the SSPPU concept would limit the royalty base in a reasonable royalty determination to the cost of the component in which the patented invention is primarily implemented, which can prevent the very outcome apportionment requires—a royalty commensurate with the value added by the patented invention to the end product.[45] Consider a hypothetical. Suppose that a patented invention is largely, but not entirely, implemented in a $20 component of a $500 device. Suppose further that the use of the patented invention in the device adds $150 of value. In a world of the mandatory application of the SSPPU concept to reduce the royalty base to components of devices sold by infringers, the royalty base *must* be the $20 component, which means that no royalty rate of

45. *See* Ericsson, Inc. v. D-Link Sys., Inc., 773 F.3d 1201, 1226 (Fed. Cir. 2014) (stating that a reasonable royalty reflects "the value added by [the patented] features"). Note that this formulation differs substantially from Judge Rader's original use of the term to describe the infringing device *sold by the infringer*; in *Cornell II*, the processors used by Judge Rader as the base to calculate a reasonable royalty were sold separately by the infringer HP.

100% or less can capture the value added by the patented invention.[46] If a jury (or a court, for that matter) is unlikely to award a royalty rate of greater than 100%, then the cost of the component will effectively operate as a royalty cap that is inconsistent with apportionment.[47]

Relatedly, mandatory application of the SSPPU concept as advocated improperly assumes a necessary economic relationship between the *value* of an invention and the *cost* of a component in which that invention is primarily implemented. As Judge Davis of the Eastern District of Texas put it, "[b]asing a royalty solely on chip price is like valuing a copyrighted book based only on the costs of the binding, paper, and ink needed to actually produce the physical product."[48] "While such a calculation captures the cost of the physical product, it provides no

46. An advocate of mandatory application of the SSPPU concept might reply that royalty rates should be permitted to exceed 100% where the royalty base is the SSPPU and a royalty rate between 0% and 100% cannot express the value added by the patented invention. Ironically, however, anchoring—the very behavioral-economics insight that gave birth to the concept of SSPPU—advises against this fix. Tversky and Kahneman concluded that estimates follow anchors, no matter in which direction the anchors stray. As a result, low royalty bases *and* high royalty bases are capable of mischief and worthy of suspicion. And if mandatory application of SSPPU is justifiable only if royalty rates can exceed 100%, then the SSPPU becomes a low anchor that is every bit as problematic in anchoring terms as the cost of the end product.

47. This royalty ceiling is also inconsistent with Section 284 and cases interpreting it. *See* Rite-Hite Corp. v. Kelley Co., 56 F.3d 1538, 1544 (Fed. Cir. 1995) ("[Section 284] affirmatively states that damages must be adequate, while providing only a lower limit and no other limitation.").

48. Commonwealth Sci. & Indus. Research Organisation v. Cisco Sys., Inc., No. 6:11-CV-343, 2014 WL 3805817, at *11 (E.D. Tex. July 23, 2014), *vacated*, 809 F.3d 1295 (Fed. Cir. 2015).

indication of its actual value."[49] It is not hard to find other illustrations. A blank DVD disk may *cost* $1, but if the disk contains patented software, then the DVD disk may be *valued* at $100. The point is that the value of the DVD disk can vary depending on the software stored on it, all while the cost of the blank DVD disk remains constant.

Mandatory Application of SSPPU Ignores Established Royalties.

The forced application of SSPPU in cases where there is market-based evidence of an established royalty could result in exclusion of the best evidence of value. Established royalties are the "best measure[s] of a reasonable royalty."[50]

Many large, competitive industries have long calculated royalties on the basis of end products.[51] A review of intended royalty rates by holders of SEPs to the 4G LTE cellular-phone standard found that *every* reporting patentee announced an intended royalty rate using an end product as a royalty base.[52]

Nevertheless, mandatory application of SSPPU would require courts to ignore such long-standing industry practices, which violates a central tenet of patent-damages law. If the best evidence of a reasonable royalty for a given patent is an established royalty for that patent,[53] and the established royalty relied

49. *Id.*

50. *See* Monsanto Co. v. McFarling, 488 F.3d 973, 979 (Fed. Cir. 2007).

51. *See* Lucent Techs., Inc. v. Gateway, Inc., 580 F.3d 1301, 1339 (Fed. Cir. 2009) ("[S]ophisticated parties routinely enter into license agreements that base the value of the patented inventions as a percentage of the commercial products' sales price.").

52. Eric Stasik, *Royalty Rates And Licensing Strategies For Essential Patents On LTE (4G) Telecommunication Standards*, LES NOUVELLES, at 114 (Sept. 2010), *available at* http://www.investorvillage.com/uploads/82827/files/LESI-Royalty-Rates.pdf.

53. *See Monsanto*, 488 F.3d at 979.

on an entire-device royalty base, then mandatory application of SSPPU requires exclusion of the best available evidence. As the studies above indicate, for some industries this rule would eliminate *most* comparable licenses.

Mandatory Application of SSPPU Would Be Inconsistent with SSPPU's Purpose of Avoiding Jury Confusion.

The SSPPU concept is, at most, an evidentiary safeguard designed to facilitate compliance with the evidentiary principle of avoiding jury confusion. Simply put, there is no basis for expanding the concept of SSPPU beyond the confines of jury trials for which it was created.[54]

In the Federal Circuit's view, jurors struggle to apply the substantive apportionment rule when exposed to large revenue numbers in cases where the value added by the patented invention is but a portion of the total value of the infringing product.[55]

But judges are different. Judges are well-equipped to understand both the apportionment rule and the mathematical interplay between royalty base and royalty rate, as judges regularly apportion damages by means of complex methodologies. No prophylactic rule designed to prevent misunderstandings or miscalculations is necessary for judges.

Besides, *Ericsson* could not have been any clearer that application of the SSPPU concept is applicable only to jury trials: "The point of the evidentiary principle"—and, therefore, the

54. Some advocates for expanding the application of the SSPPU concept argue that it should apply outside the United States, where typically judges, and not juries, determine patent damages.

55. *See, e.g.*, VirnetX, Inc. v. Cisco Sys., Inc., 767 F.3d 1308, 1327 (Fed. Cir. 2014) ("[R]eliance on the entire market value of the accused products . . . 'cannot help but skew the damages horizon for the jury.'" (quoting Uniloc USA, Inc. v. Microsoft Corp., 632 F.3d 1292, 1320 (Fed. Cir. 2011))).

tool used to effectuate that principle, SSPPU—"is to help our *jury system* reliably implement the substantive statutory requirement of apportionment of royalty damages to the invention's value."[56] No argument for the expansive use of the SSPPU concept in bench trials is reconcilable with *Ericsson*.

Mandatory Application of SSPPU Would Be Inconsistent With Cases Rejecting Rigid Patent Damages Limitations.

Both the Federal Circuit and the Supreme Court have carefully avoided the imposition of rigid limitations on patent damages. For example, the Federal Circuit has held that "[t]he correct measure of damages is a highly case-specific and fact-specific analysis."[57] Similarly, the Supreme Court "has more than once cautioned that courts should not read into the patent laws limitations and conditions which the legislature has not expressed."[58]

In short, "[w]hen Congress wished to limit an element of recovery in a patent infringement action, it said so explicitly."[59] Section 284 contains no indication (much less an explicit one) that Congress intended a mandatory SSPPU rule, and so none should be read into the statute.

---

56. 773 F.3d at 1226 (emphasis added).

57. Mars, Inc. v. Coin Acceptors, Inc., 527 F.3d 1359, 1366 (Fed. Cir. 2008), *amended on other grounds*, 557 F.3d 1377 (Fed. Cir. 2009); *see* Hebert v. Lisle Corp., 99 F.3d 1109, 1119 (Fed. Cir. 1996) ("The adequacy of the damages measure depends on the circumstances of each case.").

58. Bilski v. Kappos, 561 U.S. 593, 602 (2010) (internal quotation marks omitted); *see also* Octane Fitness, LLC v. ICON Health & Fitness, Inc., 134 S. Ct. 1749, 1756 (2014) (stating that courts should not "superimpose[] an inflexible framework onto statutory text that is inherently flexible"); KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 419 (2007) ("Helpful insights . . . need not become rigid and mandatory formulas.").

59. Gen. Motors Corp. v. Devex Corp., 461 U.S. 648, 653 (1983).

The SSPPU Concept Cannot Be Used to Limit Privately Negotiated License Agreements.

Some advocates of mandatory application of SSPPU go so far as to urge that SSPPU should dictate the royalty bases in private commercial arrangements between willing licensors and willing licensees—at least for licenses covering SEPs. No case has ever held that the SSPPU is a limit on the freedom of contract in private transactions, and there is no justification for converting the concept of SSPPU into such a limit.

SSPPU is a creature of the courts, not the market. As explained above, the concept Judge Rader dubbed "SSPPU" was designed "to help our *jury system* reliably implement the substantive statutory requirement of apportionment of royalty damages to the invention's value."[60] The goal of avoiding jury confusion has no application in a private negotiation between sophisticated market participants, because no one could reasonably contend that sophisticated market participants struggle to negotiate a fair royalty when dealing with high revenue and profit numbers. Furthermore, the *way* that the concept of SSPPU is applied to help a jury to reliably implement apportionment is by concealing revenue and profit data from them. Concealing revenue and profit data from participants in a private negotiation would be neither useful nor, in most cases, even possible.

What is more, applying the concept of SSPPU to private negotiations would require patent-by-patent and component-by-component negotiations, which would be impossible in the numerous transactions involving large, diverse patent-portfolios.[61] Rather than invite the exorbitant transaction costs associ-

60. *Ericsson*, 773 F.3d at 1226 (emphasis added).

61. Nor is there reason to think that cases involving SSPPU even contemplated application of the theory to a voluminous patent-portfolio. *See,*

ated with patent-by-patent analysis, real-world license agreements involving large patent-portfolios tend to license on a portfolio-wide basis (or at least by major class of patents within a portfolio). This sensible approach not only avoids interminable negotiations, but also results in an easily administrable license. The royalty base is the end product, and the risk of infringement is obviated because all the licensor's patents are part of the license.

The SSPPU Concept Cannot Be Employed to Rewrite RAND Licensing Commitments.

The most obvious attempt to entrench the SSPPU concept as a substantive rule for determining patent damages is taking place in the development of intellectual property rights policies of standard-setting organizations ("SSOs"), such as the Institute of Electrical and Electronics Engineers Standards Association ("IEEE"). This possibility, or the threat of its application in court, is motivating many advocates to rewrite the contours of the reasonable and nondiscriminatory ("RAND") terms and

e.g., *Ericsson*, 773 F.3d at 1209–11 (three patents); VirnetX, Inc. v. Cisco Sys., Inc., 767 F.3d 1308, 1315 (Fed. Cir. 2014) (two patents); LaserDynamics, Inc. v. Quanta Comput., Inc., 694 F.3d 51, 56 (Fed. Cir. 2012) (one patent); Cornell Univ. v. Hewlett-Packard Co., 609 F. Supp. 2d 279, 282 (N.D.N.Y. 2009) [hereinafter *Cornell II*] (one patent). Indeed, recent discussions with Judge Rader on October 7, 2015, at the IEEE-SIIT conference held in Mountain View, California, on the applicability of his concept of SSPPU confirm that he never intended it to apply to the valuation of portfolios of patents. Judge Rader recognizes the virtual impossibility of attempting to apply the SSPPU concept to a portfolio because of the necessary correlation of the concept to the elements of the infringed claims.

conditions by which members of SSOs may agree to grant licenses.[62] Doing so would enable implementers of standardized technology to pressure SEP holders into below-market royalty agreements, fundamentally altering the terms of the RAND bargain and stifling innovation.

RAND licensing strikes a balance. Implementers of standardized technologies can obtain access to SEPs and the benefits of standardization, provided they enter into licenses on RAND terms that compensate innovators fairly and adequately for the use of their SEPs. RAND licensing allows implementers to obtain access to proven technology in a standard developed through collaborative engineering efforts to gain efficiency and predictability. In return, innovators receive a sufficient return on substantial investment in research and development, incentivizing innovation that benefits everyone. As a contractual commitment between the owners of SEPs and the SSOs to which they belong, RAND must be interpreted to give effect to the intent of the parties and, therefore, this balance.

But mandatory application of the SSPPU concept to valuing SEPs would upset that balance. This is precisely what is happening in IEEE, one of the world's largest SSOs, and the SSO where Wi-Fi standards are created. Recent events at IEEE, which led to changes in the IEEE's long-standing RAND Patent Policy, have created enormous uncertainties for SEP owners and implementers alike. The IEEE's new definition of a "reasonable royalty" sets forth SSPPU as a valuation standard that courts should consider in valuing patents essential to IEEE standards where the SEP owner has made a commitment to license under the new IEEE policy. For those SEP owners, the new

62. In some cases, SSOs express the same concept as "fair, reasonable and non-discriminatory" or "FRAND" license terms. For the purposes of this article, the two terms, RAND and FRAND are interchangeable.

policy will in practical terms make it mandatory for courts to apply the SSPPU concept, not as an evidentiary tool on a case-by-case basis to avoid misleading the jury, but as the basis for determining value in all cases. To be sure, there are other controversial changes to the IEEE's policy. But the extension of the SSPPU concept—indeed, its required acceptance as a valuation metric by any SEP owner that makes compliant licensing assurances—strikes directly at the balance of value that is the heart of a RAND commitment. The IEEE's new policy is intended not to shield juries from being misled, but instead to influence negotiation of new licenses and constrain the way future licenses are structured. Moreover, for licensors of large portfolios of SEPs that are often the companies that invest the most in risky research and development to develop the standard, the use of SSPPU is completely unworkable as a valuation construct and may lead to increased litigation.

Imposing a royalty cap in the form of a royalty base specified by the concept of SSPPU on RAND licenses puts a veritable anvil on the scale in favor of implementers. Already, several members of IEEE have publicly stated that they will not make licensing assurances under the new policy.[63] What that means for the development of new standards by IEEE and the ability to attract the best technology contributions remains to be seen, particularly as IEEE will undoubtedly face increased competition with other SSOs to develop future wireless communications standards. It is hard to understand the wisdom behind the IEEE's decision to put a cloud over the tremendous standardization engine at IEEE. If the response is that companies will no

63. *See* Richard Lloyd, *Ericsson and Nokia the latest to confirm that they will not license under the new IEEE patent policy*, IAM (Apr. 10, 2015), http://www.iam-media.com/blog/detail.aspx?g=d07d0bde-ebd6-495a-aa72-4eecb9dac67d.

longer make RAND commitments, or will contribute their technologies to other SSOs without such onerous policies, or will not invest in the risky research and development that has been the hallmark of the success in the wireless communications industry, then that could cost consumers more than anyone.

CONCLUSION

SSPPU is a purpose-built tool for a specific problem presented in U.S. jury-based patent litigation. In cases where juries must apportion the value added by a patented invention to an end product, judges should operate as gatekeepers to ensure damages awards are based on sound economic principles. In some cases, that responsibility may require courts to prevent misleading evidence from reaching the jury. With those principles in mind, and faced with an unruly expert unabashedly attempting to mislead a jury about a minor component that added little value to a larger set of devices, Judge Rader fashioned an evidentiary safeguard to solve the specific problem before him. Where there is no risk of jury confusion—like where the patented invention adds significant value, or where *there is no jury*—the ground for applying the concept of SSPPU falls away. This is why no court has applied any concept of SSPPU outside of the jury trial context, and certainly no court has held that application of SSPPU should be mandatory outside of court.

It should come as no surprise that there are technology implementers who think SSPPU should be expanded far beyond the context of its origins. After all, implementers see the opportunity to manipulate the concept of SSPPU as a way to achieve below-market royalties through the courts, or through the policies of SSOs. Why worry about stagnating "the progress

of science and useful arts"[64] if implementers can raise profits today?

Don't be fooled. There is no ambiguity and should be no confusion on this point: The concept of SSPPU is an evidentiary safeguard and *only* an evidentiary safeguard. Courts, governmental authorities, and SSOs should keep it that way, lest innovation suffer.

64. U.S. CONST. art. I, § 8, cl. 8.

THE SEDONA CONFERENCE PRACTICAL IN-HOUSE APPROACHES FOR CROSS-BORDER DISCOVERY & DATA PROTECTION*

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

Author: The Sedona Conference

Editor-in-Chief: Jennifer L. Hamilton

Contributing Editors: Taylor M. Hoffman & Jerami Kemnitz

Contributors:

Katelyn Flynn

Cecil A. Lynn III

David Moncure

David C. Shonka

Natasha Williams

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference's Working Group 6. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Sustaining and 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.

PREFACE

Welcome to the final, June 2016, version of The Sedona Conference *Practical In-House Approaches for Cross-Border Discovery and Data Protection*, a project of The Sedona Conference Working Group Six on International Electronic Information Management, Discovery, and Disclosure (WG6). WG6 is best known for its groundbreaking publication, The Sedona Conference *International Principles on Discovery, Disclosure and Data Protection* ("International Litigation Principles"). The Sedona Conference *Practical In-House Approaches for Cross-Border Discovery and Data Protection* aims to provide the practical guidance that organizations and In-House counsel need to navigate challenging cross-border data transfer and discovery issues, and to effectively implement the International Litigation Principles.

This publication represents the collective effort of many contributors and members of WG6 who have worked to draft a practical, consensus-based commentary. The public comment version of The Sedona Conference *Practical In-House Approaches for Cross-Border Discovery and Data Protection* was published for public comment in September 2015 after more than two years of member dialogue, review, and revision, including:

- focus of dialogue during panels at The Sedona Conference International Programmes on Cross-Border Discovery and Data Protection Laws in London, UK, in July 2014 and Hong Kong in June 2015;
- focus of a special WG6 session at The Sedona Conference "All Voices" meeting in New Orleans, LA, USA, in November 2014;
- multiple WG6 member review-and-comment periods; and

- incorporation of comments and feedback from WG6 members representing myriad professions, backgrounds, perspectives, and stakeholders in cross-border discovery and Data Protection Laws.

After nearly a three month public comment period, the editors fully considered and incorporated as appropriate the comments received from the public into this final version.

I thank Katelyn Flynn, Jerami Kemnitz, Cecil Lynn, David Moncure, David Shonka, and Natasha Williams for their diligent efforts and commitments in time and attention to this project. I particularly acknowledge the efforts of Editor-in-Chief Jennifer Hamilton, who shepherded this project through its various stages, and Taylor Hoffman, who led the drafting effort of The Sedona Conference *eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations*, found in Appendix A of this publication.

We continue to welcome comments for consideration in future updates. You are encouraged to submit comments by email to comments@sedonaconference.org.

Craig Weinlein
Executive Director
The Sedona Conference
June 2016

TABLE OF CONTENTS

1. INTRODUCTION

In 2013, a committee[1] of The Sedona Conference Working Group Six (WG6) surveyed selected companies about their experience with cross-border discovery.[2] The committee also interviewed In-House eDiscovery experts about the challenges they face in reconciling U.S. discovery obligations and foreign Data Protection Laws. The committee concluded from the survey and interviews that companies need practical guidance to build on the value of The Sedona Conference *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") and The Sedona Conference *Cross-Border Data Safeguarding Process + Transfer Protocol* ("Protocol"), published by The Sedona Conference in December 2011.[3] As a result, the committee prepared this publication, The Sedona Conference

---

1. The Committee on Corporate Outreach would like to extend a special thank you to David Shonka and Katelyn Flynn for their invaluable input and assistance.

2. *See* Jennifer L. Hamilton & Christian Zeunert, In-House Perspective - Practical Experience with Cross-Border Discovery & Data Privacy: Conclusions from the Sedona Conference International Principles Survey & Expert Interviews (2013) (unpublished manuscript) (on file with The Sedona Conference) [hereinafter In-House Perspectives].

3. The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation*, *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20International%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection [hereinafter International Litigation Principles]. The Sedona Conference *Cross-Border Data Safeguarding Process + Transfer Protocol* [hereinafter Protocol] is included as Appendix C in the International Litigation Principles. Capitalized terms used in this document, and not otherwise defined herein, are defined in the International Litigation Principles.

Practical In-House Approaches for Cross-Border Discovery and Data Protection ("Practical Approaches") to offer solutions to common cross-border challenges.[4] These solutions may not be applicable in all circumstances and practitioners should apply them in good faith and under a standard of reasonableness.

2. IN-HOUSE PERSPECTIVES ON DISCOVERY AND DATA PROTECTION

Discovery and Data Protection Laws vary widely around the world, and these laws may conflict. Therefore, counsel must make choices regarding compliance and create balance to satisfy conflicting obligations.

a. Differing Notions of Privacy

Because member states of the European Economic Area (EEA) follow civil law regimes that differ from the U.S. common law approach and embody vastly different notions about "personal and private" information, they restrict pre-trial discovery and access to information far more than the U.S. For EEA member states, data privacy is a fundamental right, which embraces a much broader view of "personal data" than what generally prevails in the U.S. For example, the 1995 EU Data Protection

4. Companies often address eDiscovery and Privacy functions in different ways. *See* In-House Perspectives, *supra* note 2, at 5. Whereas some In-House litigators may coordinate directly with In-House privacy counsel, eDiscovery counsel may be a one-stop shop for common data protection issues. *Id.* This paper focuses on practical issues for In-House counsel who deal with eDiscovery in coordination with privacy counsel when appropriate.

Directive[5] and similar legislation of each member state[6] protect against the unauthorized processing or transfer of "personal data," which includes any information relating to an identifiable individual.

U.S. concepts of "personal data" and "Processing" of data differ greatly from those in the EEA and many other countries. This difference contributes to difficulties in cross-border communication and collaboration. Similarly, the concept of workplace privacy in the U.S. is often diminished, or even nullified, by the prevalence of computer-use policies that purport to extinguish a worker's right of privacy. In cross-border litigation,[7] this may lead to a misunderstanding of the term "personal data" as it is used in the European Union (EU). The concept of "personal data" in the U.S. is restricted to specific types of personal and sensitive information, such as medical, social security, and banking information. In the EU, this would be considered "personal sensitive information," which commands an even greater degree of protection.

---

5. 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) 31–50, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [hereinafter EU Data Protection Directive].

6. It is important to understand that EEA member states implement the EU Data Protection Directive in different ways, and some member states have chosen to give additional protection to personal data. Thus, parties should consider the effect of the laws of the jurisdiction governing processing of any personal data.

7. Although this paper primarily focuses on litigation, many of the practice points and concepts discussed may also be applicable in the context of government investigations and regulatory inquiries. The Sedona Conference has other work product underway that focus on such inquiries.

In the EU Data Protection Directive, the concept of "Processing" is broadly defined as "any operation or set of operations," whether manual or automated, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[8] In contrast, in the U.S., "Processing" generally relates solely to technical actions specifically related to eDiscovery, such as conversion from one format to another, deduplication, high-level filtering, indexing, and sampling.[9] It is critical to understand these semantic differences in any dialogue regarding these issues.[10]

b. Differing Notions of Discovery or Disclosure

Common law jurisdictions differ from civil law jurisdictions in their litigation procedures, particularly pretrial discovery. Common law practitioners assume that active involvement of individual litigants within an adversarial system is most likely to achieve fair administration of justice. In contrast, civil law practitioners assume that the state, through active participation of an experienced judiciary, is best suited to direct disclosure in the litigant process and protect the privacy of individuals as an inalienable human right. Invariably, the scope of

8. EU Data Protection Directive, *supra* note 5.

9. Even personal data in the hands of third-party contractors and agents is included under the EU Data Protection Directive. *See also* M. James Daley, *Preservation of Electronic Records of Third-Party Contractors*, THE PRACTICAL LITIGATOR (Jan. 2007), *available at* http://files.ali-cle.org/thumbs/datastorage/lacidoirep/articles/PLIT_PLIT0701-Daley_thumb.pdf (U.S. perspective).

10. For more on these issues, *see* International Litigation Principles, *supra* note 3.

permissible pretrial discovery differs dramatically between the U.S. and the rest of the world.

The scope of pretrial discovery in the U.S. is the most expansive of any common law country. The recently revised Federal Rules of Civil Procedure (Fed. R. Civ. P.) generally allow for discovery of "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."[11] Even with the anticipated benefits of limiting discovery with the Fed. R. Civ. P. Amendments, the U.S. will still be the most expansive discovery regime of any common law country.

In contrast, most civil law countries allow little or no pretrial discovery and do not require any disclosure of evidence beyond what is necessary to prosecute or defend a case. For example, in Germany, litigants are not required to disclose "non-beneficial" documents to the other party. Instead, the parties need only produce those documents that will support its own claims. These documents must be authentic, original, and certified, but the party seeking the document must appeal to the court to order production of the document.

---

11. FED. R. CIV. P. 26(b)(1). The scope of discovery prior to the implementation of the 2015 Amendments was more expansive in that it permitted discovery into any nonprivileged matter "if the discovery appear[ed] reasonably calculated to lead to the discovery of admissible evidence."

Some civil law countries also have enacted blocking statutes to curb the broad reach of discovery from the U.S.[12] For example, in 1980 France criminalized the act of obtaining discovery from France for use in litigation or investigations outside of the country. French Penal Law No. 80-538 provides:

> Subject to international treaties or agreements and laws and regulations in force, it is forbidden for any person to request, seek or communicate, in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures or in the context of such procedures.[13]

Such statutes are often viewed critically and skeptically by U.S. judges. This can lead to a direct conflict between discovery requirements in the U.S. and data protection obligations outside the U.S.[14]

---

12. *But see In re* Activision Blizzard, Inc. Stockholder Litig., 86 A.3d 531 (Del. Ch. 2014).

13. CODE CIVIL [C. CIV.] art. 1134 (Fr.), CODE PÉNAL [C. PÉN.] art. 111-4 (Fr.), art. 1 bis of law n° 68-678 dated July 26th, 1968, amended by law n° 80-538 dated July 16th, 1980.

14. *See, e.g.*, *In re* Activision Blizzard, Inc. Stockholder Litig., 86 A.3d 531 (Del. Ch. 2014).

3. THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION

This document identifies potential approaches to minimizing conflict through the application of the International Litigation Principles.[15] While the International Litigation Principles are advisory and do not carry the force of law, they can:

> provide guidance to public and private parties, counsel, data protection authorities, and the judiciary regarding the management of conflicts that may arise when there is an obligation in one jurisdiction to preserve or produce information from a second jurisdiction in circumstances where the laws of the second jurisdiction may limit the preservation, processing, or transfer of such information.[16]

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection:

Principle 1	With regard to data that is subject to preservation, disclosure, or discovery, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.
Principle 2	Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.

15. International Litigation Principles, *supra* note 3.

16. *Id.* at Preface (v).

Principle 3	Preservation or discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.
Principle 4	Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.
Principle 5	A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.
Principle 6	Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

4. PRACTICE POINTS FOR CONDUCTING CROSS-BORDER DISCOVERY IN VIEW OF DATA PROTECTION AND DATA PRIVACY REGULATIONS

Practice Point #1: Balance the need for urgency in preserving information with the need to proceed deliberately in countries with comprehensive Data Protection Laws.

In order to demonstrate due respect for foreign data protection and privacy laws,[17] *counsel can: (1) identify the cross-border data sources that apply to the matter; (2) diligently research applicable laws that apply to these sources; and (3) confer with specialized Privacy counsel how best to preserve data from these sources in compliance with the law. In-House counsel can balance the enhanced time these processes may require by adopting a preservation plan unique to cross-border discovery matters.*

Hypothetical:

You are employed by a multinational corporation using Model Contract Clauses for transfer of data (instead of Binding Corporate Rules). The company receives a third party subpoena for information relating to the overseas shipment of products manufactured in both the U.S. and the EU. The company retains Outside counsel who has some experience with transferring data out of countries with comprehensive Data Protection Laws and wants to consult with Local counsel in the EU.

Opportunity:

When data sources exist in countries with comprehensive data protection regimes, application of International Litigation Principle 1 suggests counsel should balance speed with "due respect" for foreign Data Protection Laws. Reflexively ordering employees in these countries to preserve all potentially relevant records may trigger a conflict for the employee and company under that country's Data Protection Laws. This can also be confusing to employees who are not accustomed to receiving these types of preservation or legal holds. At the same time, counsel needs to act quickly to identify relevant sources of data to meet

17. International Litigation Principle 1 states that: "courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws." *See* International Litigation Principles, *supra* note 3, at 7.

U.S. preservation obligations and err on the side of inclusion rather than exclusion.

One practical approach for balancing the urgency to preserve with data protection compliance may be to triage identification and preservation of U.S. data separately from data in the EU, issuing one legal hold notice to U.S. employees separate from EU employees. Prior to or contemporaneously with issuing the EU hold, counsel may consult Privacy counsel to understand the full scope of risk.

Analyzing complex or unfamiliar Data Protection Laws before issuing a legal hold may require more time than may be considered reasonable by a U.S. court, which could lead to sanctions. As a practical matter, counsel may need to consider alternate ways to preserve data outside the U.S. prior to issuing a legal hold notice, such as whether to take snapshots of data and preserve them in the protected country as a backup until the legal hold notice can be issued. Taking this preservation approach will likely constitute processing under EU Data Protection Laws, which will require additional steps to comply with the strict processing requirements.

If a company faces these issues on a recurring basis, it can minimize the risk of a potential lag time by developing and implementing routine internal guidelines based on EU law for processing and production of Protected Data. See Appendix A, *infra*, for an example of such model guidelines. These model guidelines and other documentation may help drive the dialogue with foreign data privacy officials in defense of the process and better inform U.S. courts and Opposing counsel why these additional steps are necessary and important.

Practice Point #2: As early as possible, meet and reach agreements with key stakeholders on a plan that sets expectations regarding legal obligations, roles and responsibilities, and a reasonable timeline.

Early discussions with counsel regarding which documents may be relevant to the matter and where they exist can start a productive dialogue to identify which Data Protection Laws may govern the transfer of data outside the country.

Hypothetical:

You are In-House counsel assigned to a multi-jurisdictional litigation matter and have engaged U.S. counsel. The partner is willing to defer to the In-House procedures as long as it does not slow down investigation of the merits. Outside counsel wants to collect data from Japan and China[18] in the next two to three weeks and is in direct contact with the business team, recommending certain dates for collection.

Opportunity:

International Litigation Principle 2 supports making reasonable decisions when faced with potentially conflicting laws: "[A] party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness." This principle encourages counsel to make decisions that compare legal needs with a variety of stakeholder needs, clearly communicate those decisions to the work team, and document the process.

---

18. Japan and China have extensive data protection regulatory schemes. Regarding Japan, *see, e.g.*, Act on the Protection of Personal Information ("APPI") (pending Sept. 2017 amendments); regarding China, *see, e.g.*, Decision of the Standing Committee of the National People's Congress on Strengthening Internet Information Protection (Dec. 28, 2012); Law on Protection of Consumer Rights and Interests (Mar. 15, 2014); Measures for the Punishment of Conduct Infringing the Rights and Interests of Consumers (Mar. 15, 2015); Guideline for Personal Information Protection (Feb. 1, 2013) [not legally binding]; State Secrecy Protection, XIANFA art. 53 (1982); and Law of the People's Republic of China on Guarding State Secrets ("State Secrets Law") (May 1, 1989).

In the hypothetical, the challenge for In-House counsel is to balance these needs with the deadlines that Outside counsel is setting. While Outside counsel may want to focus on the substance of the legal matter, it is important in the beginning stages to get both business and legal buy-in that there are additional considerations that need to factor into decisions like the timeline. The data privacy considerations need to be part of, and in some cases, drive those decisions to achieve the objective in International Litigation Principle 2 of good faith and reasonableness.

The number of internal stakeholders that In-House counsel needs to consult before the case team starts taking action can complicate matters. Here, assume that the legal team recommends arriving in Japan to do a large-scale data collection the week of a national holiday. In addition to complying with U.S. law, it is wise for counsel to consider what effect the timing of a large, in-country collection will have on the business as well as cooperation from the employees at that location. Teaming up with Human Resources may become a high priority to achieve the desired legal outcome. Likewise, for potentially high profile matters, Corporate Communications may need to be consulted about the approach the legal team wants to take.

Furthermore, the issues are complex and difficult to explain to the affected stakeholders on an expedited basis. To gain credibility, In-House counsel may need to circulate the International Litigation Principles to attorneys on the case team. For non-legal stakeholders, summaries in the form of Frequently Asked Questions and visual aids, like infographics, can more quickly build understanding of these issues.[19]

---

19. *See, e.g.*, Appendix C, *infra*, Talking Points Infographic for Internal Business Clients and Employees.

To handle the volume of tasks, In-House counsel may want to use a template case management form.[20] The template case management form can be tailored to the matter and dovetail with court-ordered deadlines and a case management plan. In addition to grouping related tasks, the form formalizes roles and responsibilities. Documentation, like the form, may help support a finding of good faith and reasonableness in the event of a challenge.

Practice Point #3: Identify and define privacy issues with opposing parties or regulators through Outside counsel where possible.

Consider when may be appropriate to start a dialogue on the scope of individual privacy rights and to document any agreement concerning U.S. and non-U.S. obligations.

Hypothetical:

Assume the same facts as the prior hypothetical, but eDiscovery and Privacy counsel are engaged at the earliest stages of the matter.

Opportunity:

International Litigation Principle 4 suggests that seeking a stipulation or court-mandated protective order may help minimize cross-border conflicts and protect personal data.[21] Where possible, counsel may seek such protection to demonstrate to non-U.S. custodians and data protection authorities that reasonable efforts have been taken to protect the confidentiality and

---

20. *See* Appendix B, *infra*, Template Cross-Border Discovery Management Form for In-House eDiscovery Teams.

21. Protective orders may not be available in the context of responding to a government inquiry or conducting an internal inquiry, but an early dialogue with regulators can foster an understanding that may have a similar effect.

guard against dissemination of personal information. By seeking a stipulation from Opposing counsel or moving the court to issue a protective order, counsel will also have the opportunity to explain the nature and extent of the foreign Data Protection Laws and any legal impediments to producing data from outside the U.S., as well as raise the issues of costs and timing.[22]

The challenge for In-House eDiscovery counsel may not be in ultimately getting this additional stipulation in a protective order, but in convincing either In-House or Outside counsel to introduce the data protection issues to Opposing counsel early enough to negotiate these terms. Outside counsel may be understandably concerned that Opposing counsel will view data protection considerations as pain points to exploit. For this reason, counsel should consider raising data protection issues in early discussions about scheduling orders to avoid having to later contend that it cannot meet its deadlines due to data protection issues. Raising cost issues early can also start the process of building a record with the Court that complying with non-U.S. Data Protection Laws can be expensive and potentially outweigh the value of that data to a particular matter. Proportionality was emphasized during the recent revisions to the Fed. R. Civ. P.: "Parties may obtain discovery . . . that is . . . 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."[23]

---

22. The Model Protective Order in Appendix B of the International Litigation Principles, *supra* note 3, contains a detailed and thorough set of safeguards for counsel to use as a starting point in discussions with Opposing counsel or the court.

23. FED. R. CIV. P. 26(b)(1).

Developing internal, written guidelines that discuss these types of protective orders can help Outside counsel enter into these early negotiations.[24] Furthermore, the process of developing these internal documents will drive the necessary cultural education and behaviors that further underscore Outside stakeholders' confidence that complying with Data Protection Laws is a necessary and achievable part of the discovery process.

Practice Point #4: Set up transparency "checkpoints," beginning with preservation and continuing through the life of the matter, to avoid revocation of consent.

The Article 29 Working Party states in its paper on the interpretation of Article 26(1) that "relying on consent may . . . prove to be a 'false good solution,' simple at first glance but in reality complex and cumbersome."[25] *Consider that consent to transfer may be revoked at any time according to the EU Directive. To minimize that risk, counsel can set up several transparency "checkpoints" throughout the life of the matter, granting custodians an opportunity to understand and agree to the process. Individuals or organizations outside the company may also require periodic notice of the status of proceedings.*

Hypothetical:

During litigation, In-House and Outside counsel discover that an employee located in the EU may have documents

---

24. *See* Appendix A, *infra*, The Sedona Conference, *eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations*.

25. *See* Working document of the Article 29 Working Party on a 'common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995,' WP 114 at 11 (Nov. 25, 2005), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf.

relevant to the matter in the U.S. Outside counsel suggests calling this employee to ask about his documents. In your experience, it is common for Outside counsel to "collect" relevant documents during the course of such a phone call. Outside counsel has no prior experience with foreign Data Protection Laws.

Opportunity:

The hypothetical presents several questions regarding scope of preservation and validity of consent. U.S. parties may be concerned that contacting the employee without first issuing a hold could lead to spoliation. On the other hand, issuing a legal hold before knowing whether the employee has relevant data is the type of overly-broad preservation that may concern relevant EU data protection authorities. In-House counsel also grapple with whether to request consent upon issuing the legal hold or before collecting potentially protected data. Outside counsel may worry that if the employee refuses to consent to preserve, the company is subject to U.S. court sanctions for failing to perform one of its most fundamental tasks during the discovery process.

One approach is to think of gaining consent not as a potential barrier to success but as a way to open the conversation and ultimately gain the trust of employees in data protected countries.[26] The goal is not to achieve a certain number of communications but to confirm and convey that the company and

26. Consent not freely given does not guarantee a legitimate transfer of data. Specifically, it might be difficult to qualify consent as freely given in an employment context, due to the subordinate nature of the relationship between employer and employee. Therefore, the Article 29 Working Party suggests that employers not rely solely on their employees' consent when transferring their data unless they can show that the employees would not suffer any consequences by either withholding their consent or by subsequently withdrawing it. This limitation places a peculiar burden on U.S. defendants with business units in Europe, where a legal matter requires the

counsel will: (1) respect the employee's rights vis-a-vis the company's responsibility; (2) commit to achieving compliance to the best of their ability; and (3) be as transparent as possible about how the company proposes to balance the rights of the employees and the company. Accordingly, providing transparency documents with a request for consent would more fully advance these goals.[27] Furthermore, graphics or diagrams and a detailed collection script may help clarify these steps for employees, who may know nothing about these legal conflicts. Companies that document their efforts to keep employees informed may further demonstrate the reasonableness of the activity under European Data Protection Authority rules.[28]

Transparency can be achieved by other means as well. Full transparency may include giving employees opportunities to review data and confirm their acceptance of transfer of the documents for a cross-border legal matter. This review might occur during the collection interview after counsel explains the issues at stake and identifies personal data that does not need to be collected. Counsel may also provide employees with an opportunity to review personal folders or emails and remove them

---

company to transfer documents with personally identifiable information across national borders. Although consent of employees may not suffice as an independent basis for transferring private data, transparency throughout the life of the matter may resolve most employee concerns about what will happen with their data and minimizes the risk that employees will subsequently withdraw their consent. *See also* In-House Perspectives, *supra* note 2.

27. Consider whether transparency documents require translation for the recipients, depending on legal requirements and the employee's fluency in a particular business unit.

28. International Litigation Principle 5 states: "[a] Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted." International Litigation Principles, *supra* note 3, at 19.

from the collection process. Furthermore, some companies have given employees the opportunity to conduct their own privacy review after the company collects documents and before transfer or production of the data. These transparency steps, in addition to obtaining consent, may achieve the company's objective of compliance with legal obligations as well as data protection and privacy laws, while satisfying key stakeholders in the process—the employees. Full transparency may pose a significant challenge in larger matters with lots of custodians. Counsel may need to find alternative ways to avoid increasing burden and expense in achieving transparency.

Practice Point #5: Plan a successful in-country collection with detailed surveys of appropriate systems well in advance, and by soliciting support from key stakeholders, both in corporate departments and local business units.

Counsel can reduce the expense and risk of in-country collections by learning about key stakeholders, key systems, and country customs. The logistics involved should be planned in detail as soon as counsel knows that he or she must collect information from any non-U.S. country.

Hypothetical:

After an in-country data collection commences, the Information Technology (IT) department discloses that the server where the EU employee saves data is shared with non-company business units located in the same industrial business park.

Opportunity:

International Litigation Principle 3 states that "[p]reservation or discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's

claim or defense in order to minimize conflicts of law and impact on the Data Subject."[29] Planning for a targeted collection may help balance conflicting interests. Even so, there is much work to be done prior to an in-country collection, starting with identifying key IT contacts in the targeted locations.

In the hypothetical, after counsel discovered that key servers were "shared" with other businesses, counsel may want to identify the right people to engage at these other businesses. For example, counsel would probably want to consider: (1) whether to contact the Chief Executive Officer or the Chief Information Officer; (2) who has the authority to sign any type of transparency or consent form to permit access to the data at other companies using the servers; and (3) the requirements counsel must follow to minimize the risk of infringing on data protection and privacy laws.[30]

In addition, this scenario points to the value, as identified under Practice Point #1, of having a plan in place before discovery issues even arise. Next time, before commencing collection, counsel may want to conduct surveys of systems that potentially store relevant data. Such surveys typically include: (1) the key witnesses; (2) the business owners; and (3) any IT owners of the systems. This reduces the chance of learning too late that several independent companies share the same file servers.

---

29. Recall that the European privacy model encourages limiting the collection to what is necessary to the matter rather than employing a "take it all now, figure it out later" approach.

30. Of course, in an ideal situation, counsel would have been aware of the shared servers prior to litigation or an investigation. As a practical matter, this is not always the situation despite good faith diligence of counsel.

Practice Point #6: Use the Processing stage of discovery as an opportunity to balance compliance with both discovery and Data Protection Laws, thereby demonstrating due respect for Data Subjects' privacy rights.

Early discussions regarding data Processing can address requirements related to both Data Protection Laws and local court procedures and demonstrate due respect to any Data Subject with rights under applicable Data Protection Laws.

Hypothetical:

In-House and Outside counsel meet to determine the best way to cull and filter the large amount of collected data. They do not ask a business representative to join this meeting. Outside counsel wants to use a U.S.-based vendor to process the data because of the preferred rates offered by the vendor's local office.

Opportunity:

After collecting information potentially relevant to a lawsuit or investigation, organizations must "process" that information before producing it. "Processing," as used in U.S. eDiscovery, is the automated ingestion of electronically stored information (ESI) into a program to extract metadata and text and create a static image of the source ESI according to a predetermined set of specifications, in anticipation of loading the information into a database for review. Processing specifications may include filtering data based on metadata or full text contents to include or exclude the results of such filtering in the final work product for review.

The Processing stage is an opportunity under the International Litigation Principles to protect privacy while complying with discovery obligations. International Litigation Principle 3 states, in part, that "discovery of Protected Data should be limited in scope to that which is relevant and necessary to sup-

port any party's claim or defense." Before Processing any collected data, counsel may want to meet with key business representatives and learn the business language that relates to the pending legal matter. After learning relevant business terms, names, and dates, a keyword search list can be developed to help eliminate irrelevant information from the data set. Decisions made throughout this process should be documented, pursuant to International Litigation Principle 5, to demonstrate reasonableness and due respect for data protection obligations. The search process should be iterative, and the results should be continuously analyzed by counsel and revised as necessary.

Counsel can include terms and set parameters that will help identify Protected Data. For example, the names of financial institutions may help isolate an individual's banking records that he or she has kept in an email or document files. Similarly, unless the employee has used his or her personal email to conduct company business, email domain addresses often associated with personal emails, such as hotmail.com or gmail.com, may be isolated to help identify non-work related communications for removal from the potentially relevant data set.

The Processing phase also serves as a key decision point regarding the transfer of data out of the country from which it was collected. Under International Litigation Principles 1 and 2, parties may try to perform culling and filtering exercises in the country where the data was collected so irrelevant Protected Data can be removed from the data set prior to transfer. If data must be transferred out of country for review, an initial culling before transferring the information may help demonstrate respect for local Data Protection Laws while complying with any conflicting discovery obligations outside the country. Parties should take advantage of technological advances and the ability to perform processing activities nearly anywhere in the world to balance privacy rights with disclosure obligations.

Practice Point #7: During review of data for production and disclosure, parties may consider ways to limit the production of Protected Data; when production of Protected Data is necessary, safeguards can be established to demonstrate due respect for both discovery and Data Protection Laws.

The review and production stages may be used to protect privacy interests of the Data Subjects whose data has been collected for use in the legal matter. The Model Protective Order in Appendix B of the International Litigation Principles provides one way to balance discovery and disclosure obligations with individual data protection rights.

Hypothetical:

Hundreds of thousands of documents remain in the data set after culling and filtering. Outside counsel wants to use its U.S. based associates to perform a linear document-by-document review of the material. In-House counsel usually employs a document review vendor that has facilities throughout the world and uses a review platform that includes the latest technology assisted review functionality. Before Outside counsel meets with Opposing counsel to discuss production formats and timelines, In-House and Outside counsel meet to develop document review guidelines and to set parameters around production.

Opportunity:

After culling and filtering the data set, parties generally perform some level of "eyes on" review of the documents before production to Opposing counsel. Document review may range from a high level spot check of a sample of the collected and filtered data to a full document-by-document review of every item in the data set. The goal of review is to isolate and produce only that information which is relevant to the claims or defenses of a party.

One key decision is whether to review data in the country in which it was collected ("in-country review") or, if in-country

review is not possible, in a country with similar Data Protection Laws ("near-country review"—a distinction based on regulatory rather than geographic proximity). Accordingly, an "eyes on" review in- or near- country may further demonstrate compliance with Data Protection Laws, creating an added safeguard against the production of non-responsive Protected Data while balancing the need for production with the protection of individual privacy rights. See International Litigation Principles 1, 2, and 3.

Parties may wish to consult with Local Privacy counsel, Outside eDiscovery counsel, and technology vendors to consider additional available review options and to ensure they are both technologically feasible and, more importantly, compliant with local data privacy regulations.

In-House and Outside counsel should consider drafting document review guidelines (DRGs) for attorneys performing the review. These DRGs may include protocols for tagging documents with Protected Data—particularly non-responsive documents that may contain Protected Data. For example, among the responsive/non-responsive issue tags, counsel may include tags labeled "responsive – personal data" and "non-responsive – personal data." This will allow counsel to determine the volume of "responsive – personal data" and formulate a disclosure plan. One benefit of tagging "non-responsive – personal data" is that if a large amount of "non-responsive - personal data" is identified in the initial collection(s), collection criteria could be modified to minimize the amount of such data in any subsequent collections.

If Protected Data must be produced to Opposing counsel, the responding party should consider safeguards to limit production of such data, such as producing data in an anonymized or redacted format. For example, an employee roster that iden-

tifies all workers on a particular project may have multiple columns of Protected Data, including name, address, phone number, personal identification numbers (PINs), and nationality. If this document must be produced, PINs could be redacted, and addresses and phone numbers could be anonymized to include one single business address and phone number. The nationality field might also be aggregated to show only the number of workers representing each nationality. Anonymization, pseudonymization, redaction, and aggregation are often applied to productions if required by local laws/regulations and are consistent with the guidance of International Litigation Principles 1, 2, and 3.

Tiered or staged productions offer another method of limiting the production of Protected Data. Oftentimes, employees maintain duplicative, or nearly duplicative, emails and project files. To balance data protection rights with discovery obligations, parties may agree to review U.S. productions first. Afterwards, the parties may be able to agree that further production from non-U.S. custodians is not necessary. If further production is necessary, parties might agree on an extended review and production timeline to accommodate the additional time needed to review and produce data from outside the U.S.

To protect responsive data containing Protected Data that must be produced, parties can agree on a protective order similar to the Model Protective Order in Appendix B of the International Litigation Principles.[31] As International Litigation Principle 4 states, "where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect

31. *See* International Litigation Principles, *supra* note 3, at Appendix B. Note, however, that such stipulations and protective orders are usually not available in government investigations.

Protected Data and minimize the conflict." Such an agreement can be used, for example, to limit the number of people allowed to view the Protected Data, and impose immediate destruction requirements on Protected Data, as detailed in International Litigation Principle 6, either after that information is reviewed by the requesting party or as soon as it is no longer needed for the matter.

Practice Point #8: To avoid keeping data longer than necessary, counsel should prepare to release legal holds and return or dispose of data promptly upon termination of a matter.

Once a matter is concluded, legal holds may be released and data returned or disposed of depending on its retention requirements. A matter is fully concluded when, for example: (1) a final settlement agreement and release has been signed by all parties; (2) a dismissal with prejudice has been entered as to all parties and the deadline for any appeals has run; (3) any judgment has become final; or (4) in government investigations, when the government has indicated that the investigation has been concluded, for example, through a letter of declination, return of documents, or any other formal notice of the conclusion of the investigation.[32]

Hypothetical:

The U.S. Litigation involving the employee in the EU has settled and the data collected is no longer needed for litigation or other purposes. However, the company would like to keep the data in the event that similar, although unanticipated, claims arise in the future. The company is primarily motivated by the high cost and significant amount of time required to retrieve

32. Under Fed. R. Civ. P. 52(b) a party has 28 days to move the court to make additional findings or amend its findings or judgement. Under Fed. R. Civ. P. 59, a party has 28 days to seek a new trial.

and search the data and engage Outside counsel to navigate potential privacy issues with regulators and Opposing counsel. The company's primary argument for retaining the data is that all personal data should have been purged during EU-based document review prior to its transfer and the company would rather have this information available should it need the data again in litigation.

Opportunity:

As noted in International Litigation Principle 6, "[o]rganizations should take good faith, reasonable efforts to retain, manage, and dispose of inactive data both on a prospective and retrospective basis." This approach comports with the European data protection authorities' preference for "data minimization," as the less personal data collected or retained by an organization, the lower the cost and risk associated with data protection. This approach also supports sound records management practices, which have been interrupted by imposition of preservation steps taken in connection with the legal action.

Throughout the proceeding, In-House counsel should maintain a record, or inventory, of all locations where data is preserved, collected, or produced during the matter, whether it is stored on the company's U.S. server; or with Outside counsel, third party vendors, or opposing parties and their vendors. At the end of the matter, counsel may use this inventory to seek return of the data or otherwise certify its disposal in accordance with its discovery protocols. By doing so, counsel will demonstrate compliance with foreign Data Protection Laws and also build a record that will provide insights for the company in future actions.

While counsel may prefer to retain indefinitely all EU data that has been legitimately transferred to the U.S. for litigation purposes, doing so would contravene International Litigation Principle 6 as well as the EU Directive. The EU Directive

provides that Protected Data should be retained only as long as necessary to satisfy legal or business needs. The company's purported business need (i.e., the high cost of obtaining the data weighed against the possibility of future litigation) would appear to be outweighed by the privacy rights of non-U.S. citizens under the EU's strong policy of protecting personal data. Moreover, the company's assertion that all personal data related to the EU employee (and others) was removed "in-country" largely ignores the probability that some personal data may have remained in the production due to its relevance to the subject matter of the litigation. The argument also ignores the fact that prior to production of the personal data, the litigation parties may have entered into confidentiality agreements or a protective order dictating appropriate use and disposal of the data.

The company is responsible for ensuring the return or disposal of personal data. Post-litigation disposition of personal data comports with International Litigation Principle 6 and prior Commentary.[33] Prompt disposal of data also provides assurance to non-U.S. data protection and privacy authorities that U.S. companies enforce legitimate preservation obligations rather than collect information based on a legal action that may occur in the future.

5. CONCLUSION

Cross-border discovery presents a growing challenge for courts, privacy authorities, companies, employees, counsel, and requesting parties. Practical solutions are necessary to reconcile potentially conflicting obligations in a reasonable manner. This Practical Approaches document is one additional step to achieve these solutions.

---

33. *See, e.g.*, The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265, 259 (2010).

6. PRACTICAL APPROACHES APPENDICES: THE SEDONA CONFERENCE IN-HOUSE TOOL KIT FOR DATA PROTECTION AND CROSS-BORDER DISCOVERY

The tools in the following appendices were designed to help companies approach cross-border discovery and Data Protection Laws on a practical level. Developing a set of internal tools for cross-border discovery is not a small task and not every company will have the need or resources to do so. However, the process of developing even one of these tools results in more than just guidance on future legal matters. It forces key stakeholders to educate each other about important legal and cultural considerations; to grapple with philosophical issues and make proactive decisions; and to develop a network of internal contacts that can act quickly when these situations arise. The education alone that the stakeholders receive may be worth the effort, even more so where the company has locations in multiple jurisdictions around the world or faces these issues on a regular basis.

A. The Sedona Conference eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations

B. Template Cross-Border Discovery Management Form for In-House eDiscovery Teams

C. Talking Points Infographic for Internal Business Clients and Employees

D. Exemplar Heat Map of Data Protection and Data Privacy Regulations

APPENDIX A: THE SEDONA CONFERENCE EDISCOVERY AND DATA PROTECTION MODEL GUIDELINE: PROCESSING & PRODUCTION OF PROTECTED DATA IN LIGHT OF PRESERVATION & DISCLOSURE OBLIGATIONS

What it is: A customizable roadmap describing steps a company may take to minimize potential conflict of eDiscovery and Data Protection Laws in line with the International Litigation Principles.

Who it is for: In-House counsel, eDiscovery Team, privacy officers, and Outside counsel.

Why it is important: Provides consistent basis to approach individualized matters and demonstrates reasonableness and good faith.

How to use it: To be applied in conjunction with the company's policies to legitimize company processes and educate stakeholders for matters that may require significant resources.

Appendix A Table of Contents

Preface

In 2013, The Sedona Conference (TSC) formally launched the Committee on Corporate Outreach of Working Group Six on International Electronic Information Management, Discovery, and Disclosure (WG6). The committee's mandate is an important one, i.e., strengthening the practical applicability of The Sedona Conference *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"). In its first year, the committee conducted its first annual TSC International Principles Survey, reporting the results for In-House eDiscovery and data protection experts and underscoring the need for practical guidance for In-House eDiscovery experts, including a need for materials such as an eDiscovery and Data Protection Model Guideline. This Sedona Conference *eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations* ("Guideline" or "Model Guideline") is one of the tools included in the appendix to the *Practical In-House Approaches for Cross-Border Discovery & Data Protection* document ("Practical Approaches").

Each section of this Guideline includes model guideline language and a comment section. The Guideline language contains building blocks corporations can use for their In-House guidelines, recognizing the potential need to modify the language given the individual corporation's circumstances (e.g., industry, countries of operation, cultural specifics). The comment sections highlight key issues as well as potential areas of modification. It does not, however, attempt to address all potential considerations for modification.

1. Introduction/Guideline Purpose:

Model Guideline Language

The Sedona Conference *eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations* ("Guideline" or "Model Guideline") provides guidance for Company to address both its U.S. eDiscovery and non-U.S. data protection obligations during litigation in the U.S. and to minimize any potential legal cross-border conflicts arising between the two.[34] By applying this Guideline under a standard of reasonableness and good faith, potential conflicts can be minimized. The Guideline is not meant to be a step-by-step manual and may not be appropriate or applicable in every matter. The assigned In-House counsel should consult on specific matters as needed with eDiscovery counsel/team and appropriate Company Data Protection Officer (DPO).

This Guideline is to be applied in conjunction with Company's Group Data Protection Policy and other relevant policies.

Comment

This Model Guideline focuses on U.S. eDiscovery and non-U.S. data protection obligations.[35] Companies may need to

34. While the Guideline and companion FAQ have been crafted to address data protection issues in the context of litigation, Company may consider leveraging them in part to address transactional and compliance-related uses of protected Company data. Please note that WG6 anticipates preparing an additional Guideline and companion FAQ to address internal and government investigations in conjunction with a related WG6 public comment publication that is in the process of being finalized.

35. Non-U.S. data protection obligations include data privacy obligations as covered by the EU Data Directive (and the laws enacted by its member states or other countries that have modelled their data protection

consider including more tailored language for the various regions/countries at issue and/or providing more specific guidance regarding country-specific issues (e.g., blocking statutes or relevant penal codes), depending on the circumstances. In addition, companies may want to clarify specific privacy issues depending on the Company's industry and the regulatory environment in which it operates (e.g., banking consumer data or medical data). In addition to modifying the Model Guideline scope, companies may want to specify the goal(s) of their guideline. For example, some companies may want to streamline an approved process for "standard" matters and define parameters for "exceptional" matters. Others may focus their intent on building a consistent approach.

Companies must also determine how best to internally market or roll out their guideline. A guideline introduced without sufficient internal buy-in and education faces greater challenges in being consistently implemented. The corresponding FAQ to the Model Guideline provides examples of questions which may arise for employees who are not frequent practitioners of cross-border discovery but may benefit from guidance and big-picture issue flagging. Obviously, they should be modified both in scope and specificity depending on the company's needs.

2. Principles:

Model Guideline Language

This Guideline incorporates, where appropriate, the *International Principles on Discovery, Disclosure and Data Protection: Best Practices, Recommendations & Principles for Addressing the*

schemes on the EU Directive), state secrecy laws as found in China, banking secrecy laws such as those found in Switzerland, to name a few.

Preservation Discovery of Protected Data in U.S. Litigation ("International Litigation Principles"), published by The Sedona Conference in December 2011.[36] While the International Litigation Principles are advisory and do not carry the force of law, they are intended to provide guidance to public and private parties, counsel, data protection authorities, and the judiciary regarding the management of conflicts that may arise when there is an obligation in one jurisdiction to preserve or produce information from a second jurisdiction in circumstances where the laws of the second jurisdiction may limit the preservation, processing, or transfer of such information. Capitalized terms used in this Guideline, and not otherwise defined herein, are defined in the International Litigation Principles.

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection

Principle 1	With regard to data that is subject to preservation, disclosure, or discovery, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.
Principle 2	Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or

36. The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation*, *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20International%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection [hereinafter International Litigation Principles].

data protection authority under a standard of good faith and reasonableness.

Principle 3 Preservation or discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.

Principle 4 Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.

Principle 5 A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.

Principle 6 Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

Comment

The Model Guideline includes all of the International Litigation Principles in a separate section here because they are cited throughout the Model Guideline and provide its foundation. However, for purposes of length, companies may consider merely incorporating them by reference or including the specific

International Litigation Principles throughout the guideline when applicable.

3. Intended Audience and Case Kick-off:

Model Guideline Language

The intended audience for this Guideline is Company's internal personnel in Legal, IT, Compliance and other functions who manage legal proceedings involving U.S. eDiscovery and non-U.S. Protected Data.

To ensure that data preservation, collection, hosting, review, and production are performed consistently and to minimize potential conflicts between Company's U.S. eDiscovery and non-U.S. data protection obligations, the eDiscovery Team must be consulted in all eDiscovery matters involving non-U.S. data.

For each specific matter, the relevant Company DPO, In-House Litigation counsel, In-House eDiscovery counsel, and eDiscovery project manager should consult on the relevant sources of data and custodians, as well as which regional/country-specific data regulation applies to each data source and custodian. At this early stage, these individuals should also begin to address issues to be raised with Opposing counsel in a subsequent meet-and-confer (e.g., potential protective orders, whether a Hague Convention request or letters rogatory may be needed, etc.). Each of these individuals brings specific knowledge and skill sets that will assist the Company in complying with both its U.S. eDiscovery and non-U.S. data protection obligations, and in minimizing any potential legal cross-border conflicts arising between the two.

Comment

Companies should modify this language to reflect their organizational structure and naming conventions (for example,

some smaller companies with limited litigation profiles may not even have an In-House dedicated eDiscovery Team). However, companies should only exclude a functional equivalent of any of the above-named roles (i.e., personnel in Legal, IT, Compliance, and other functions who manage legal proceedings involving U.S. discovery and non-U.S. Protected Data) after careful consideration. These roles should consult and come to agreement on the guideline and specific processes and procedures prior to a specific matter arising requiring U.S. discovery of non-U.S. Protected Data. Again, depending on regional and national scope, and the domestic regulatory environment, regional or local roles should also be consulted (e.g., a Company DPO specializing in Protected Data residing in Asia). Broad stakeholder buy-in at the time of implementation is key to ensure that the guideline is followed consistently across various lines of business or internal Company silos and does not create conflicts with existing Company policies that may otherwise overlap with the guideline.

On a per-matter basis, companies may consider whether it is necessary to consult all of these functional roles and instead delegate to a subset after all of the functional roles have approved an overall process. If these functional roles are not included on a per-matter basis, they should regularly consult to ensure that the approved processes and procedures are still appropriate. Moreover, individuals handling specific matters should consult frequently and raise any unusual circumstances or unfounded assumptions.

The Model Guideline references the meet-and-confer with Opposing counsel at an early stage in the spirit of TSC's *Cooperation Proclamation*,[37] and because early communication of

37. The Sedona Conference, *Cooperation Proclamation*, 10 SEDONA CONF. J. 331 (2009 Supp.).

potential cross-border transfer concerns can minimize subsequent disputes among parties.

4. Preservation (Legal Hold) Process and Data Protection Safeguards:

Model Guideline Language

In the U.S., parties are required to identify, locate, and preserve data that is potentially relevant to pending or reasonably anticipated U.S. Litigation. This duty is rooted in the U.S. common law requirement to avoid spoliation of relevant evidence.[38] Non-U.S. data protection regulations, on the other hand, define this preservation as "Processing" even if the Protected Data is not transferred, creating a potential tension between the two regulatory regimes. The process outlined below provides a framework for Company to comply with its preservation obligations while also taking account of appropriate non-U.S. data protection safeguards.

a. Scoping and Data Minimization

Data minimization, i.e., preserving only the data potentially relevant to any party's claim or defense, is an effective data protection safeguard.[39]

The scope of a Legal Hold should be determined at the direction of counsel and in compliance with applicable preservation obligations. In light of the data minimization safeguard,

---

38. The Sedona Conference, *Commentary on Legal Holds: The Trigger and The Process*, 11 SEDONA CONF. J. 265 (2010).

39. *See* International Litigation Principles, *supra* note 36, Principle 3 ("Preservation, disclosure, and discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.").

the Legal Hold should be appropriately limited with respect to the (1) data custodians (i.e., the individuals placed on hold), (2) data categories, and (3) relevant time frame.

Scoping and data minimization does not conclude with the initial Legal Hold but instead is an iterative process. As the matter evolves (e.g., through an amended complaint or a better understanding of the facts based on custodian interviews), the scope of the Legal Hold should be appropriately adjusted.

b. Transparency and Employee Acknowledgement

Transparency, i.e., taking reasonable steps to notify non-U.S. Data Subjects of the purpose(s) for which their personal data may be processed, is also an effective data protection safeguard.[40] Company is not required to seek notification and/or consent where it is prohibited by law or where an exception is provided by law.

The Legal Hold Notice issued to non-U.S. Data Subjects should explain the purpose, scope of information to be preserved, potential subsequent use of preserved information, and potential consequences of not preserving relevant information. In addition, the Legal Hold Notice should include a notice of rights to access, modify, and oppose processing of personal data. Transparency, in addition to being good data protection practice, reduces opposition from custodians throughout the discovery process.

---

40. *See* International Litigation Principles, *supra* note 36, Principle 5 ("A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.").

For current employees, the standard language in a Legal Hold Notice may request confirmation from non-U.S. data custodians[41] that they understand the Legal Hold and potential data protection implications. Company obtains consent from non-U.S. employees departing Company as part of the off-boarding process.[42] In instances in which it becomes known that a non-U.S. former employee has not provided consent, Company will take reasonable steps to contact the individual using last known contact information. Depending on the country of the custodian, it may be appropriate for Company to offer the non-U.S. data custodian an opportunity to assess and limit the potential privacy impact by reviewing and tagging as "private" certain communications. In-House Litigation counsel, In-House eDiscovery counsel, the relevant Company DPO, and any applicable body such as a Company Works Council in Germany, or the local data protection authority (DPA), such as the National Commission on Informatics and Liberty (CNIL) in France or the Information Commissioner's Office (ICO) in England and Wales, will address how to proceed with respect to any country-specific requirements if a conflict arises between the interests of the non-U.S. data custodian and Company.

---

41. A "data custodian" refers to the employee whose mailbox is collected in contrast to a "Data Subject," which more broadly refers to an individual whose personal data may be included in data custodian's mailbox. Obviously, it is often impractical to obtain consent from every Data Subject and, thus, Company should undertake other appropriate safeguards in furtherance of Principle 3.

42. While not all data protection authorities may view consent as sufficient, consent nevertheless furthers the goal of transparency.

c. Legal Hold Release and Data Disposal

Releasing Legal Holds and disposing of data that is subject to the corresponding Legal Holds are effective data protection safeguards.[43] Company's preservation obligation is limited in duration to the time during which a legal action is pending or remains reasonably anticipated.

At the conclusion of a matter (e.g., when the applicable time period for appeal has expired or litigation is no longer reasonably anticipated), Company provides employees subject to the Legal Hold with a written Legal Hold Release Notice. If the Protected Data is not subject to another Legal Hold, it is then maintained according to applicable records retention guidelines. With appropriate consultation with In-House counsel and the Records Management Group, the Protected Data previously subject to a Legal Hold will be destroyed under the management of the eDiscovery Team if (1) the applicable records retention schedule has expired; (2) the Protected Data is not subject to another Legal Hold or other legal obligation; and (3) there is no other valid reason to maintain the Protected Data (e.g., business requirement).

Comment

This Model Guideline language highlights the inherent tension between U.S. preservation obligations and the non-U.S. definition of "Processing." Even ideal circumstances (consent from the data custodian and approval from the Company DPO

43. *See* International Litigation Principles, *supra* note 36, Principle 6 ("Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards."); s*ee also* International Litigation Principles, *supra* note 36, Principle 3 regarding data minimization.

and applicable Works Council) raise preservation concerns given timing and logistics.

Appropriate scoping and data minimization are clearly important aspects of limiting data protection implications. Interviewing subject matter experts and identified custodians helps to ensure that Company strikes the right balance. In fact, it may come to light that named custodians do not, in fact, have relevant data and can be removed from the Legal Hold.

This Model Guideline language also acknowledges that not all Works Councils nor Company DPOs may find consent and transparency sufficient. In these matters, the In-House litigator, In-House eDiscovery attorney, relevant Company DPO, and Works Council should consult to find a mutually agreeable solution and—importantly—weigh the costs and benefits of not complying with U.S. eDiscovery obligations. It is advisable in most cases (and especially in cases in which the custodian denies consent) to consult with the subject matter experts and custodians to determine whether there is substantively duplicative data that has lesser data protection concerns.

While the Model Guideline suggests that consent and transparency be included in the Legal Hold Notice, it is also an acceptable practice for this to be included in a separate communication with the data custodians. Regardless of which document this communication resides in, it should include contact information for any potential follow-up questions.

This Model Guideline proposes that the Company provide the Data Subject with the opportunity, at his or her request, to conduct a privacy review. This raises the potential for misuse of the privacy review (e.g., the data custodian using the privacy review and redaction process to hide his or her own malfeasance rather than culling legitimately private information (such as medical data)). If there is reason to suspect this, the applicable Company DPO, Works Council, In-House litigator, In-House

eDiscovery counsel, and In-House Human Resources counsel should consult on an appropriate action.

Finally, the conclusion of a matter provides an important data protection step often overlooked by In-House and Outside counsel. Company should consider including the steps described in this Model Guideline in any applicable case closeout checklist.

5. Post-Preservation Process and Data Protection Safeguards:

Model Guideline Language

The eDiscovery process requires additional data protection safeguards beyond the preservation stage (i.e., collection, processing, hosting, transfer, review, and possible production). The process outlined below provides a framework for Company to comply with its discovery obligations with appropriate non-U.S. data protection safeguards.

a. Initial Case Assessment on Data Protection Implications

Each matter may involve data from a number of jurisdictions for which applicable Data Protection Laws need to be considered.[44] Therefore, at the outset of each matter, In-House counsel and a member of the eDiscovery Team should consult to identify the country scope for identified data collections (i.e., the countries where information is located) and appropriate data

44. *See* International Litigation Principles, *supra* note 36, Principle 1 ("With regard to data that is subject to preservation, disclosure, or discovery, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.").

protection safeguards, including potential cross-border data restrictions.

In some circumstances, Company may be required to consult the local DPA or the Company Works Council, and even take into account criminal statutes (e.g., Swiss Penal Code Articles 271 and 273), blocking statutes (e.g., France and Switzerland), or industry specific restrictions (e.g., banking secrecy laws).

Moreover, whether notification or approval of a DPA is required depends upon the local Data Protection Law and certain factors, including: the mechanism chosen for legitimizing the transfer of Protected Data to the United States; whether it concerns a single or repeated transfer; and the amount of data to be transferred. On one end of the spectrum, for example in Belgium or the UK, DPA approval may not be required, provided that the receiving party (e.g., eDiscovery service provider or Retained counsel) is either Privacy Shield certified or has executed Standard Contractual Clauses. However, further onward transfers to third-parties (e.g., opposing party or the court) may require other safeguards like a protective order with appropriate data protection language. On the other end of the spectrum, for example in France or Spain, DPA notification or approval may be required.

If the data has already been transferred to a recipient in the U.S., onward transfer to a third-party recipient in the U.S. (usually the opposing party in U.S. Litigation) is legitimate through a "stipulative court order" (or presumably a protective order), specifically addressing certain data protection criteria (e.g., confidentiality, security, access, restricted use, and distribution). In such cases, the onward transfer requires neither formal approval from nor notification to the DPA. However, the exporting party should be prepared to provide a copy of the protective order in the event of an audit by the DPA. Protective

orders alone, however, may not be an adequate basis for the initial transfer of data to the U.S.

The eDiscovery Team should also determine whether it is appropriate to provide post-preservation notice and/or consent to current and former non-U.S. employees who are data custodians as the eDiscovery process continues. As described above, former employees provide consent as part of the off-boarding procedure. In instances in which it becomes known that a former employee has not consented, Company will take reasonable steps to contact the data custodian using last known contact information. If Company is unable to do so, the eDiscovery Team should consult the Company DPO, In-House counsel, and any other applicable data protection authority such as the Works Council (in Germany) or the CNIL (in France). Again, it is unreasonable to obtain consent from Data Subjects as opposed to data custodians and, thus, Company should undertake other appropriate safeguards in furtherance of International Litigation Principle 3.

As part of case management, the eDiscovery Team should document steps taken to safeguard data protection.[45]

b. Collection, Hosting, Review, and Production

Data minimization is also an effective data protection safeguard at the collection phase.[46] In-House counsel and an eDiscovery Team member should consult regarding search

45. *See* International Litigation Principles, *supra* note 36, Principle 5 ("A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.").

46. *See* International Litigation Principles, *supra* note 36, Principle 3 regarding data minimization.

terms and time period. Adhering to the U.S. principle of proportionality[47] furthers this safeguard by limiting the overall scope of discovery.[48]

The use of an internal analysis and hosting tool housed and managed in-country or in-region is an effective data protection safeguard. This minimizes the need for cross-border transfer of Protected Data and reduces data security risks. Obviously, there are many circumstances in which it is not practical or feasible for non-U.S. Protected Data to remain on Company's internal tool (e.g., data transfer to Outside counsel or remote access to the internal tool provided to Outside counsel or eDiscovery service provider outside the region). In these circumstances, the eDiscovery Team should consult, as applicable, the Company DPO, Works Council, and/or local data protection authority, and implement additional safeguards (e.g., Privacy Shield certification, execution of Standard Contractual Clauses, inclusion of data protection language in the engagement letter, assurance of secure authentication for access to a limited and identified list of individuals, and prohibition of batch print function).

It may be appropriate for Outside counsel to seek an agreement with Opposing counsel or seek to obtain a court order permitting phased productions to provide Company additional time to implement appropriate safeguards for non-U.S. Protected Data. If production of non-U.S. data is required but presents a conflict with non-U.S. Data Protection Laws, a protective order limiting dissemination and preservation duration

47. *See* FED. R. CIV. P. 26(b)(2)(C) and 26(g)(1)(B)(iii).

48. The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 14 SEDONA CONF. J. 155 (2013), provides additional guidance on this principle.

of the Protected Data may be an appropriate safeguard.[49] Redactions and/or anonymizations may also be appropriate safeguards, although they may not be practical or permitted in certain circumstances.

c. Case Closure and Data Disposal

Ensuring proper disposal of data at the conclusion of a matter is an effective data protection safeguard.[50] The eDiscovery Team should consult with In-House counsel to determine whether it would be appropriate and feasible to obtain certifications of destruction (or other means of confirmation) from Outside counsel, vendors, and Opposing counsel.

Comment

Section a., Initial Case Assessment on Data Protection Implications, of this Model Guideline focuses on specific data protection regulations. This, clearly, is ripe for modification depending on the Company's specific circumstances. However, the Company should be careful to not merely delete potential inapplicable regulations but should instead consult with the Company's counsel to address whether additional specific data protection regulations (whether they be country- or industry-specific) should be addressed here. The Company should also

---

49. *See* International Litigation Principles, *supra* note 36, Principle 4 ("Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.").

50. *See* International Litigation Principles, *supra* note 36, Principle 6 ("Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.").

consider whether internal policies on data handling impacts certain data protection regulations; for example, permitting private use of a Company's email system may affect other regulations, e.g., the German Telecommunications Act.

This Model Guideline also suggests that the eDiscovery Team document steps taken to safeguard data protection. Regardless of which functional entity the Company tasks with this responsibility, it should be clearly defined to help ensure that a potential demonstration of steps taken is centrally located. The level of detail may appropriately vary company-by-company.

Regarding the hosting and management of the hosting tool, it is important to consider the jurisdictions of who has access and/or permissions to grant access. A hosting tool physically located within the region may be better than being physically hosted in the U.S., but it provides greatly reduced protection if it is managed and/or accessible to U.S.-based personnel. It may also be appropriate to inform document reviewers of country- or region-specific Data Protection Laws that may affect the review and also implement additional safeguards. For example, if search terms return a clearly private email, it may be appropriate to delete it from the review platform rather than merely coding the document as non-responsive.

Again, the conclusion of a matter provides an important data protection step often over looked by In-House and Outside counsel. Company should consider including the steps described in this Model Guideline in any applicable case closeout checklist.

6. Conclusion:

This Guideline should be implemented with due respect for Data Protection Laws and under a standard of reasonableness and good faith. Doing so will minimize any potential conflict arising between Company's U.S. eDiscovery and non-U.S.

data protection obligations.[51] If there is doubt as to what action would be appropriate, the Company DPO, In-House counsel, and the eDiscovery Team should be consulted.

51. *See* International Litigation Principles, *supra* note 36, Principles 1–2.

Frequently Asked Questions (FAQ)

Model Language to be customized by Company

This FAQ addresses issues that may arise when implementing the Guideline. The purpose of this FAQ is to provide awareness of the complexity of electronic data protection in a cross-border environment. The FAQ offers points to consider; it does not provide definitive answers, and may not apply to every situation. You should consult the eDiscovery Team before proceeding.

This FAQ will be updated from time to time as additional questions are asked. It has been designed to avoid duplication of the Group Data Protection Guideline and FAQ (available ***here***) as much as possible.

1. Introductory Questions

1.1 Who should read this FAQ?

The intended audience is those working in conjunction with the eDiscovery Team and whose role involves the transfer of non-U.S. data across international borders, typically for the purposes of U.S. litigation or other judicial proceedings.

1.2 Why is electronic data protection important?

Company is legally required to protect personal data and respect applicable privacy rights across all of its global operations. Data Protection Laws vary across jurisdictions; breach of the local laws can be met with financial penalties, regulatory sanctions, or criminal prosecutions. In addition, failure to process personal data according to established data protection principles could result in reputational damage to the brand and diminished consumer confidence.

1.3 Where can I find the Guideline?

It can be found on the Company's Intranet ***here***.

1.4 What is the role of the eDiscovery Team?

The eDiscovery Team assists in ensuring consistent compliance with Company's eDiscovery and data protection obligations. The eDiscovery Team does this in part by coordinating the involvement of appropriate subject matter experts. Depending on the situation, this may include Group Legal, Data Protection Officers, Outside counsel, and Company's Works Councils. Failure to consult the eDiscovery Team when processing non-U.S. personal data for legal proceedings in the U.S. could result in negative consequences for you and/or Company.

1.5 What are some basic principles of which I should be aware?

The Guideline incorporates, where appropriate, the International Litigation Principles.[52] Although the International Litigation Principles are advisory and do not carry the force of law, they provide guidance to public and private parties, counsel, data protection authorities, and the judiciary regarding the management of conflicts that may arise when there is an obligation in one jurisdiction to preserve or produce information from a second jurisdiction, and the laws of the second jurisdiction limit the preservation, processing, or transfer of such information.

You should familiarize yourself with the principles in the Guideline. They explain the importance of being aware of your obligations and working towards solutions that demonstrate

52. International Litigation Principles, *supra* note 36.

good faith, reasonableness, and due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.

2. Key Questions

2.1 Does the Guideline prohibit the cross-border transfer of personal data?

No. There is no blanket prohibition on cross-border transfers of personal data. The Guideline recognizes that certain countries require that appropriate safeguards be implemented prior to the transfer of personal data. You should consult the eDiscovery Team before transferring any data across international borders.

2.2 What is Personal Data?

Personal data is any data containing information that (i) can be used to identify a Data Subject to whom such data relates, or (ii) is or might be directly or indirectly linked to an identifiable Data Subject. If there is any doubt as to whether data is personal, you should consult the local Company Data Protection Officer and the eDiscovery Team for guidance.

Some examples of personal data (non-exhaustive list) include the following: name, date of birth, gender, home address, home phone numbers, personal mobile phone numbers, an employee's CV information or talent profile, national identifiers, client identification numbers, and bank account or credit card numbers.

The Group Data Protection Guideline (available ***here***) provides additional information.

2.3 Does the use of personal data in legal proceedings supersede data protection obligations?

No, data protection safeguards must still be adhered to, although the need to submit personal data may be justified due to the fact that there is a legal proceeding. The eDiscovery Team and local Company Data Protection Officer should be consulted on specific matters.

2.4 What is the Email Archive?

The Email Archive is a storage system for some or all emails sent or received by Company email accounts for a [length of time] period. Additional information about the Archive can be found on the Company's Intranet ***here***.

2.5 What are "blocking statutes"?

Blocking statutes are laws designed to restrict the disclosure of personal data and other covered information to foreign jurisdictions. For example, a U.S. court may order the disclosure of personal data of a French employee with such data being located in France, creating a potential conflict of U.S. law (requiring the production) and French law (prohibiting the production). Similar restrictions exist in Switzerland. Accordingly, data transfers potentially subject to blocking statutes require a case-by-case assessment and you should consult the eDiscovery Team and local Company Data Protection Officer for guidance.

2.6 What is a Works Council or Workers' Council?

A Workers' Council (sometimes also referred to as a Works Council) is an organization representing employees at a local or firm level. Workers' councils have been established in, for example, Germany, France, and the Netherlands. You

should consult the eDiscovery Team prior to processing personal data of Company employees from the countries that have established such Councils.

2.7 What constitutes a cross-border "transfer" of personal data?

The cross-border "transfer" of personal data may include disclosure of personal data to a recipient employed or contractually bound by a third party in a different country, even if such recipient is within the same organization. Making this information accessible remotely is also considered a "transfer." Similarly, allowing the recipient to process the personal data by, among other things, collecting, recording, accessing, using, storing, altering, retrieving, or consulting (reading) the data constitutes a "transfer." If you have any doubts as to what may constitute a transfer, you should consult the eDiscovery Team.

2.8 In my case, Outside counsel conducts cross-border productions of personal electronic data. Should I still consult the eDiscovery Team?

Yes. While many outside law firms have good cross-border data transfer processes, ultimate responsibility remains with Company. Further, Outside counsel may not be sufficiently familiar with local data protection restrictions or have a comprehensive understanding of the physical location of information environments and data storage facilities of the Company. Accordingly, you should consult the eDiscovery Team to ensure compliance with internal policies and applicable laws and to maintain appropriate communication with internal stakeholders.

2.9 A European employee of Company consented for his or her personal electronic data to be used in a U.S. proceeding. Should I still consult the eDiscovery Team?

Yes. While employee consent is sufficient in many instances, there are still regulations regarding the nature and form of employee consent. For instance, in some European jurisdictions the validity of employee consent may be questioned on the basis that it may not have been given voluntarily. Also, Company may need to undertake additional steps in light of, for example, blocking statutes and the Swiss Penal Code.

2.10 A European employee wants to see the documents that are to be or have been produced by Company in a U.S. proceeding. Does he/she have such a right?

Potentially, European (and other) Data Protection Laws provide the Data Subject certain rights of access to their personal data processed by Company. However, there may be legal restrictions on allowing access to the personal data of other parties. If you are confronted with a Data Subject access request, you should consult local Company Data Protection Officers and the eDiscovery Team to ensure compliance with internal policies and applicable law and to maintain appropriate communication with internal stakeholders.

2.11 Does European employee personal data have to be redacted?

In the case of a civil litigation, employee and other personal data contained in business documents to be disclosed usually do not have to be redacted. There may be cases where redactions are required or appropriate (e.g., in certain investigations of potentially criminal conduct by foreign authorities). However, even if no redactions have to be made, internal

and sometimes external data protection safeguards should be considered with regard to business documents that contain personal data of persons from Europe or other countries with applicable Data Protection Laws. You should consult the eDiscovery Team on these issues and make sure that Outside counsel considers them early on in the process.

2.12 Are special arrangements required with Outside counsel?

In the event that Company retains non-European Outside counsel to handle personal data that is subject to European (or other) Data Protection Laws, special arrangements with Outside counsel will usually be necessary (e.g., including a data protection clause in the engagement letter or having Outside counsel sign the EU model clauses for cross border data transfers).

Outside counsel must be instructed properly on data protection issues and made aware of the restrictions (not only including data protection and privacy laws in the narrow sense, but also issues related to blocking statutes, business secrets, and labor laws, because violation of these restrictions may result in criminal liability). You should consult the eDiscovery Team on these issues.

Creating awareness with Outside counsel early on is important not only to ensure compliance with data protection and privacy laws, but also to ensure that counsel will represent Company adequately in dealing with opposing parties and authorities (e.g., in the meet-and-confer phase provided for by U.S. civil procedure law).

3. Country-Specific Questions

3.1 My U.S. legal proceeding involves only U.S. employees. Does this FAQ apply?

This FAQ addresses the cross-border transfer of non-U.S. data, not the use of U.S. data in U.S. legal proceedings. U.S. laws and regulations on data protection and data transfers differ significantly from Data Protection Laws and regulations in Europe, Asia, Latin & South America, and other regions.

Nevertheless, you should still consult the eDiscovery Team. There is no such thing as an "eDiscovery case;" every litigation and arbitration involves eDiscovery. The eDiscovery Team, as Company's subject matter experts, is here to assist and ensure consistent compliance with Company's eDiscovery obligations.

3.2 I'm transferring personal data out of Switzerland. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

Switzerland is not within the EU, and although Swiss data protection law is comparable to the Data Protection Laws within the EU, there are differences (as there are certain differences also within the EU). For example, Switzerland has a different definition of what constitutes "personal data," as it also includes personal data about legal entities, not just individuals.

In addition, the Swiss Penal Code may be implicated depending on whether the disclosure of personal data is "forced" (in other words, performed upon the direct order of a non-Swiss governmental entity (e.g., a U.S. court, foreign regulator) with sanctions in case of non-compliance) or "unforced" (in other

words, performed voluntarily in furtherance of a legal obligation).[53] The Swiss Penal Code may also be implicated if business or manufacturing secrets of other Swiss third parties are at issue when Company knows that the business or manufacturing third party desires to keep the secret.[54]

3.3 I'm transferring personal data out of Germany. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

Germany has enacted its own Data Protection Laws (based on the principles of the EU Directive). Germany has also established a Workers' Council, which, depending on the circumstances, may need to be consulted prior to the transfer of data. Furthermore, German law provides for detailed requirements with regard to contracts governing cases in which companies instruct third parties to process personal data on their behalf.

3.4 I'm transferring personal data out of France. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

---

53. SCHWEIZERISCHES ZIVILGESETZBUCH [StGB], [SWISS PENAL CODE] Dec. 21, 1937, SR 311.0, art. 271.

54. SCHWEIZERISCHES ZIVILGESETZBUCH [StGB], [SWISS PENAL CODE] Dec. 21, 1937, SR 311.0, art. 273.

France has enacted its own Data Protection Laws (based on the principles of the EU Directive). France has also established a Workers' Council, which, depending on the circumstances, may need to be consulted prior to the transfer of data. Depending on the circumstances, French Outside counsel and regulatory bodies may need to be consulted prior to the transfer of electronic data.

3.5 I'm transferring personal data out of Italy. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring. Italy has enacted its own data privacy laws (based on the principles of the EU Directive).

3.6 I'm transferring personal data out of the Netherlands. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

The Netherlands has enacted its own data privacy laws (based on the principles of the EU Directive). The Netherlands has also established a Workers' Council, which, depending on the circumstances, may need to be consulted prior to the transfer of data.

3.7 I'm transferring personal data out of the United Kingdom. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

The United Kingdom has enacted its own Data Protection Laws (based on the principles of the EU Directive). Transfer of personal data to any other country, even one with stricter data protection and privacy requirements, must be considered on a case-by-case basis.

APPENDIX B: TEMPLATE CROSS-BORDER DISCOVERY MANAGEMENT FORM FOR IN-HOUSE EDISCOVERY TEAMS

What it is: A checklist of common tasks, which tracks activities, roles, and responsibilities a company may consider when faced with a new U.S. matter that requires preservation and collection of data from offices outside of the U.S.[55]

Who it is for: Primarily In-House counsel; although, it may be shared with key stakeholders, such as Outside counsel and law department management.

Why it is important: Helps In-House counsel quickly triage a new matter as well as document a reasonable process and reduce risk of miscommunication.

How to use it: May be customized for the client and the matter; fill it out as each phase approaches; circulate it to key stakeholders to confirm understanding and buy-in.

---

55. The Template Cross-Border Discovery Management Form has been converted to grayscale and reformatted for purposes of printing in *The Sedona Conference Journal*. To view this Form in color and its orginal format, *see* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, Appendix B, at B-2, THE SEDONA CONFERENCE (Sept. 2015 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Practical%20In-House%20Approaches%20for%20Cross-Border%20Discovery%20and%20Data%20Protection.

Cross-Border Discovery Management Form [Matter Name & Number]	In-House Case Team	eDiscovery Team	In-House IT Support	Law Firm (merits counsel)	Law Firm (eDiscovery)	Vendor
Identify						
• Identify relevant cross-border data sources						
• Compile a list of custodians and locations						
• Conduct employee interviews to determine relevant data locations						
Research						
• Research applicable laws that apply to the data sources identified						
• Consult guidelines and company policies (e.g. Model Guidelines)						
• Confer with specialized privacy counsel						
Plan						
• Identify and prepare safeguards						
▪ Seek a stipulation or court-mandated protective order						
▪ Draft consent and consider whether it needs to be translated						
• Hold introductory meeting with critical stakeholders						
▪ Communicate a general plan and timeline for data collection						
▪ Discuss the company's policies for cross-border data collections as well as relevant experiences						
▪ Discuss alternate cost models to determine impact on budget						
▪ Assign roles for each major group						
Preserve						
• Prepare a preservation plan with a phased approach						
▪ Issue legal hold notices to U.S. custodians first						
▪ Prepare to issue legal hold notices to non-U.S. custodians along with appropriate safeguards, e.g. consent						
• Define the scope and narrowly tailor both the substantive and custodial scope of data to be preserved outside the U.S.						
▪ Define the relevant time period for the case						
• Scope privacy issues with opposing party or regulator where possible and document any agreement						
Collect						
• Plan for a targeted collection						
▪ Learn about the key stakeholders, key systems, and country customs ahead of time						
• Plan logistics in detail prior to collection efforts						
• Engage vendor support as early as possible for collection and processing as necessary						
▪ Conduct planning sessions with the vendor staff and local IT resources where the collection will take place						
• Set up transparency checkpoints in addition to consent						
▪ Prepare a frequently asked questions document to address employee concerns						
▪ Prepare a detailed collection script						
▪ Document efforts to keep employees informed						
▪ Provide employees with the opportunity to review data and confirm acceptance of transfer, as well as the opportunity to remove personal folders or emails from the collection process						
Process						
• Filter down the data to what is relevant and necessary						
• Learn about key business terms, names, and dates and develop a keyword search list with the goal of eliminating irrelevant information from the data set						
Review						
• Consider whether to perform the review of data in-country						
▪ Consult with local privacy counsel, outside eDiscovery counsel, and vendor to consider available review options						
• Draft document review guidelines for attorneys performing the review						
▪ Include protocols for tagging documents with protected data						
Produce						
• Consider various safeguards for production of protected data, such as producing in an anonymized or redacted format						
• Consider tiered document review, e.g., produce responsive data collected from U.S. custodians first and determine whether further production from non-U.S. custodians is necessary						
Close						
• Prepare an inventory of all locations of the data preserved, collected, or produced during the matter						
• Prepare to release legal holds and return or dispose of the data promptly upon termination of a matter						

(R) Responsible (A) Accountable (S) Supportive (C) Consulted (I) Informed

APPENDIX C: TALKING POINTS INFOGRAPHIC FOR INTERNAL BUSINESS CLIENTS AND EMPLOYEES

What it is: An infographic that provides a basic, visual education about the conflict of law that clients face when collecting data from countries with Data Protection Laws.[56]

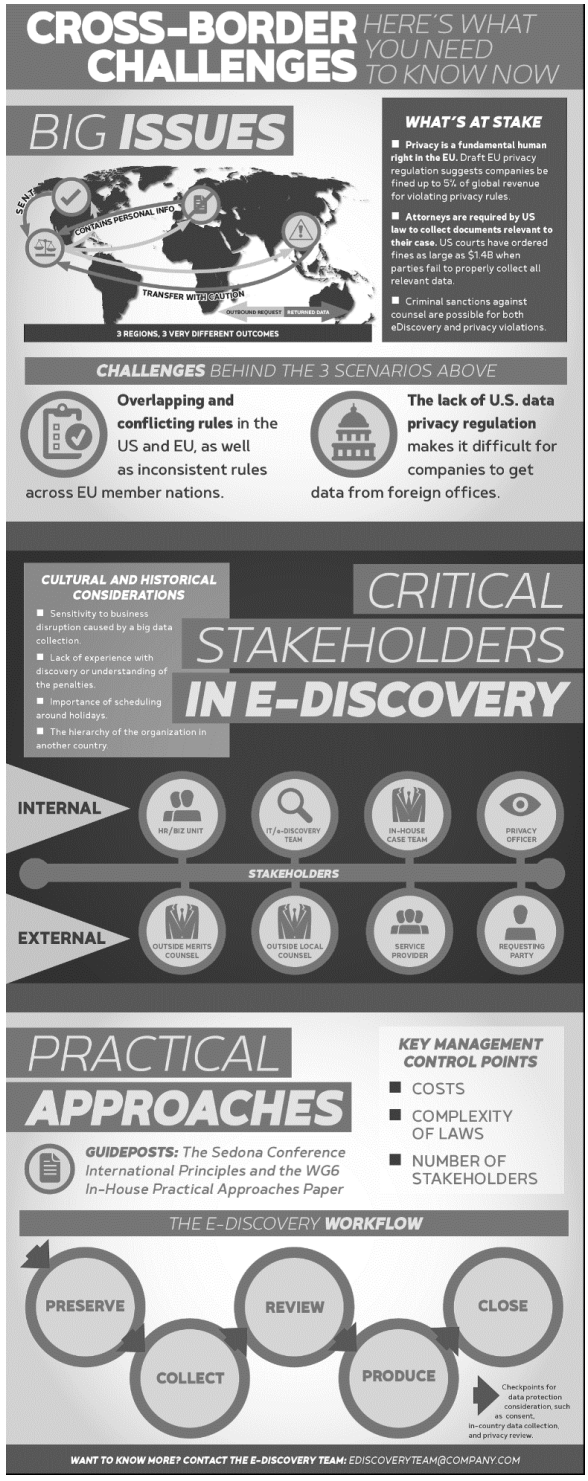
Who it is for: Internal business clients, employees, or legal counsel unfamiliar with the issues or company process.

Why it is important: Educates stakeholders why it is important to incorporate The International Litigation Principles into the matter handling process, demonstrates the complexity of managing the process as well as the need for appropriate resources, and previews what legal, cultural, and historical considerations may come into play.

How to use it: Can be used as a one-page infographic or as three separate panels for a PowerPoint presentation for stakeholders who may lack experience with the issues.

---

56. The Talking Points Infographic has been converted to grayscale for purposes of printing in *The Sedona Conference Journal*. To view this Infographic in color, *see* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, Appendix C, at C-2, THE SEDONA CONFERENCE (Sept. 2015 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Practical%20In-House%20Approaches%20for%20Cross-Border%20Discovery%20and%20Data%20Protection.


CROSS-BORDER CHALLENGES
HERE'S WHAT YOU NEED TO KNOW NOW
BIG ISSUES
SEND
CONTAINS PERSONAL INFO
TRANSFER WITH CAUTION
OUTBOUND REQUEST
RETURNED DATA
3 REGIONS, 3 VERY DIFFERENT OUTCOMES
WHAT'S AT STAKE
Privacy is a fundamental human right in the EU. Draft EU privacy regulation suggests companies be fined up to 5% of global revenue for violating privacy rules.
Attorneys are required by US law to collect documents relevant to their case. US courts have ordered fines as large as $1.4B when parties fail to properly collect all relevant data.
Criminal sanctions against counsel are possible for both eDiscovery and privacy violations.
CHALLENGES BEHIND THE 3 SCENARIOS ABOVE
Overlapping and conflicting rules in the US and EU, as well as inconsistent rules across EU member nations.
The lack of U.S. data privacy regulation makes it difficult for companies to get data from foreign offices.
CULTURAL AND HISTORICAL CONSIDERATIONS
Sensitivity to business disruption caused by a big data collection.
Lack of experience with discovery or understanding of the penalties.
Importance of scheduling around holidays.
The hierarchy of the organization in another country.
CRITICAL STAKEHOLDERS IN E-DISCOVERY
INTERNAL
HR/BIZ UNIT
IT/e-DISCOVERY TEAM
IN-HOUSE CASE TEAM
PRIVACY OFFICER
STAKEHOLDERS
EXTERNAL
OUTSIDE MERITS COUNSEL
OUTSIDE LOCAL COUNSEL
SERVICE PROVIDER
REQUESTING PARTY
PRACTICAL APPROACHES
GUIDEPOSTS: The Sedona Conference International Principles and the WG6 In-House Practical Approaches Paper
KEY MANAGEMENT CONTROL POINTS
COSTS
COMPLEXITY OF LAWS
NUMBER OF STAKEHOLDERS
THE E-DISCOVERY WORKFLOW
PRESERVE
COLLECT
REVIEW
PRODUCE
CLOSE
Checkpoints for data protection consideration, such as: consent, in-country data collection, and privacy review.
WANT TO KNOW MORE? CONTACT THE E-DISCOVERY TEAM: EDISCOVERYTEAM@COMPANY.COM

APPENDIX D: EXEMPLAR HEAT MAP OF DATA PROTECTION AND DATA PRIVACY REGULATIONS

What it is: Example of a map that depicts an individual company's internal risk profile, color-coded by country.[57] A key feature of the map is an interactive "pop up" menu summarizing key Data Protection Laws, possible transfer mechanisms, key stakeholders, possible next steps, and applicable company policies or documents, like the Model Guideline (Appendix A).

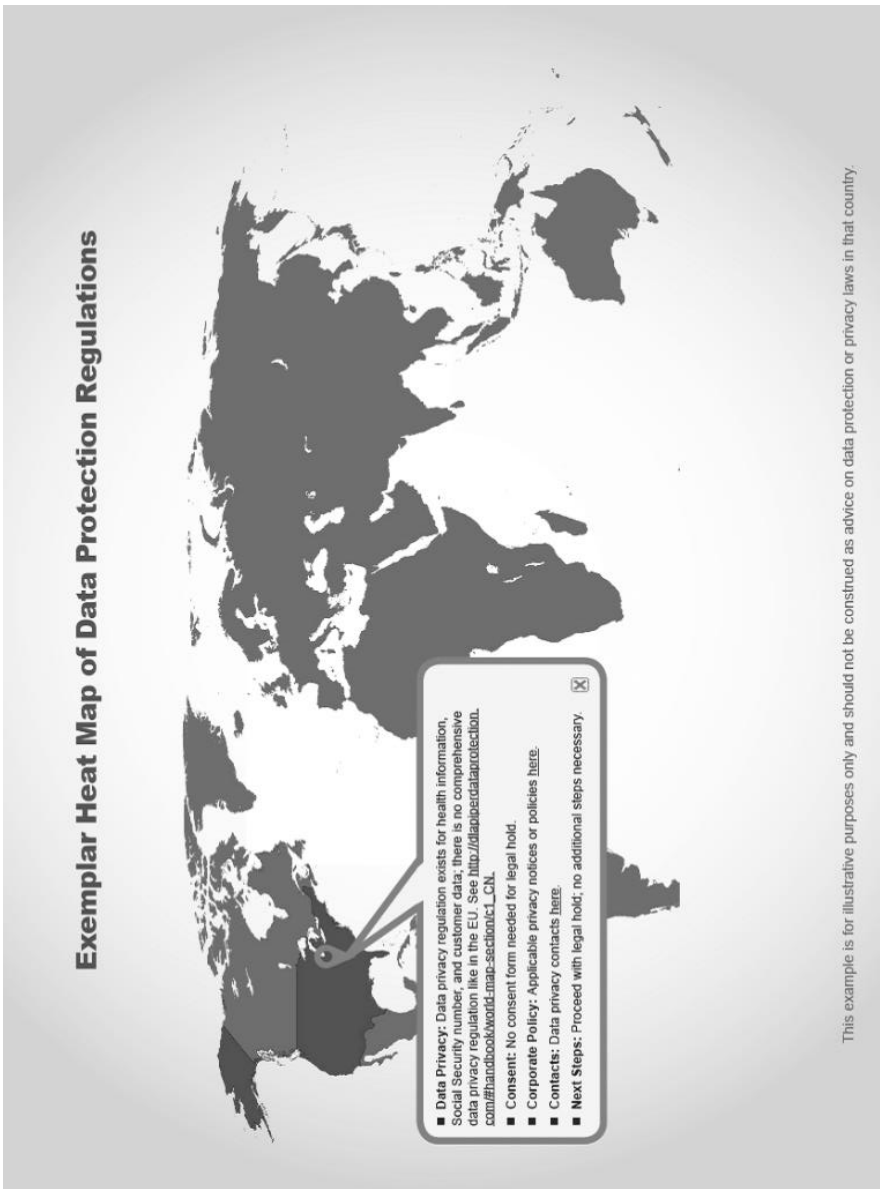
Who it is for: Primarily In-House legal and compliance departments.

Why it is important: Builds speed, efficiency, and consistency in In-House counsel who may need to juggle a number of jurisdictions and considerations for these types of matters.

How to use it: Although the example suggests providing certain data to the user, In-House counsel can customize their internal heat map in any way that helps tackle these types of matters.

---

57. The Exemplar Heat Map has been converted to grayscale for purposes of printing in *The Sedona Conference Journal*. To view this map in color, *see* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, Appendix D, at D-2, THE SEDONA CONFERENCE (Sept. 2015 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Practical%20In-House%20Approaches%20.


Exemplar Heat Map of Data Protection Regulations
Data Privacy: Data privacy regulation exists for health information, Social Security number, and customer data; there is no comprehensive data privacy regulation like in the EU. See http://dlapiperdataprotection.com/#handbook/world-map-section/c1_CN.
Consent: No consent form needed for legal hold.
Corporate Policy: Applicable privacy notices or policies here.
Contacts: Data privacy contacts here.
Next Steps: Proceed with legal hold; no additional steps necessary.
This example is for illustrative purposes only and should not be construed as advice on data protection or privacy laws in that country.

Moving the Law Forward in a Reasoned & Just Way