IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/Commentary_on_Application_of_Attorney-Client_Privilege_and_Work-Product_Protection_to_Documents_and_Communications_Generated_in_the_Cybersecurity_Context

wgs

The Sedona Conference

Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context

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

April 2019
Public Comment Version
Submit comments by June 25, 2019, to
comments@sedonaconference.org

The Sedona Conference®

The Sedona Conference Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context

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

APRIL 2019 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editor-in-Chief
Douglas H. Meal

Contributing Editors
David Thomas Cohen
Jami Mills Vibbert
Brian Ray

Steering Committee Liaison
Alfred J. Saikali

Staff Editors
David Lumia
Michael Pomarico

Preface

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

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

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

In addition to the drafters, this non-partisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of the *Commentary* were the subject of the dialogue. On behalf of The Sedona Conference, we thank all of them for their contributions.

Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by June 25, 2019, to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

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

Craig Weinlein
Executive Director
The Sedona Conference
April 2019

Table of Contents

A. Purpose and Target Audience 1
B. General Governing Principles 3
1. The Attorney-Client Privilege 3
2. Work-Product Protection Law 6
3. Waiver 8
C. Application of Attorney-Client Privilege and Work-Product Protection Principles to Cybersecurity Information 9
1. Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work-Product Protection to Pre-Incident CI 10
a. Types of Pre-Incident CI 10
i. Technical Inventories, Configuration Reviews, Vulnerability Scans, and Penetration Tests 10
ii. Security-Risk Assessments, Outside Audits, and Remediation Efforts 11
iii. Policies and Procedures 12
iv. Tabletop Exercises 13
v. Internal Audit Reports 13
vi. Reports of the Security Team or Board-Level Committees 13
b. Attorney-Client Privilege 14
i. Involvement of a Lawyer 14
ii. For the Predominant Purpose of Obtaining Legal Advice from the Lawyer 14
iii. Among or Within Privileged Persons 17
iv. Reasonable Expectation the Communication Will Be Kept Confidential 19
c. Work-Product Protection 19
2. Legal Evaluation and Practice Guidelines as to Application of Attorney-Client Privilege and Work-Product Protection to Post-Incident CI 19
a. Examples of Post-Incident CI 20

i. Forensic Investigations—Documents and Reports 20
ii. Post-Incident Security Assessments....20
iii. Remediation Efforts and Crisis Management 20
b. Application of Attorney-Client Privilege to Post-Incident CI....21
i. For the Predominant Purpose of Obtaining Legal Advice from a Lawyer 21
ii. Among or Within Privileged Persons 23
c. Application of Work-Product Protection to Post-Incident CI 26
i. Because of Anticipated Litigation 26
ii. Substantial Need 30
3. Waiver of Attorney-Client Privilege and Work-Product Protection as to CI....31
a. Disclosures to Direct or Indirect Contract Parties....32
b. Disclosures to Internal Company Employees....32
c. Disclosures to Law Enforcement 33
d. Disclosures to Information Sharing Organizations....33
e. Common Interest, Joint Defense, and Joint Representation....34
f. Subject-Matter Waiver 35
D. The Path Forward....36
1. A Critical Assessment of the Existing Regime....36
a. Perverse Incentives Created by the Existing Regime....38
b. The Disadvantages of Involving Counsel in Creating CI....40
c. The Disadvantages of Depriving Law Enforcement of Access to Privileged/Protected CI 41
d. To What Extent the Current Regime Promotes Relevant Interests 41
e. The Unique Importance of Cybersecurity and Cybercrime....43
2. Reform Proposals....43

a. Absolute Stand-Alone Cybersecurity Privilege Rejected 44

b. Proposed Qualified Stand-Alone Cybersecurity Privilege 45

c. Selective Waiver for Criminal Cybersecurity Investigations 51

i. Statutory Models 53

ii. Statutory Selective Waiver Proposal and Explanation 54

E. CONCLUSION 58

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

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

A. PURPOSE AND TARGET AUDIENCE

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

Such documents and communications are often highly relevant to litigation or regulatory investigations over a breach because they pertain to issues such as (1) whether the organization's cybersecuri-

ty practices, or its oversight of third parties' (e.g., vendors') cybersecurity practices, complied with any applicable legal requirements; (2) whether the organization made deceptive statements regarding its cybersecurity practices so as to support misrepresentation-based claims; and/or (3) whether the organization provided legally sufficient notice to external parties regarding the breach. Accordingly, such documents and communications are likely to be helpful to plaintiffs and regulators in trying to prove their claims in any litigation or regulatory investigations, and potentially damaging to the breached organization's legal defenses to such claims. As a result, the breached organization may desire to shield such documents and communications from discovery under the attorney-client privilege or as protected trial preparation "work product" (such protection being referred to both colloquially and in this *Commentary* as "work-product protection"), whereas plaintiffs and regulators may desire to overcome any such assertion of attorney-client privilege or work-product protection.

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

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

---

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

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

3 The *Commentary* focuses on attorney-client privilege and work-product protection law, as opposed to other privileges and protections that might potentially apply to CI, but recognizes that other privileges and protections may potentially be applicable to CI and/or may have underlying policy rationales that bear upon the propriety of according attorney-client privilege and/or work-product protection to CI. In addition, while private lawsuits and regulatory investigations regarding cybersecurity breaches occur inside and outside of the United States, and accordingly, data security lawyers have an interest in both the U.S. and the non-U.S. legal standards governing attorney-client privi-

forward by providing practitioners (faced with advocating for and against the discoverability of CI), judges (faced with rendering decisions on its discoverability), and legislators (seeking to create law on its discoverability) with an assessment of the arguments for and against having the discoverability of CI be determined under general principles of attorney-client privilege and work-product protection law, as opposed to modifying those principles in the context of CI to create more or less protection of CI from discovery than otherwise would be provided under the attorney-client privilege and the work-product protection. Finally, the *Commentary* considers various proposals for adapting existing attorney-client privilege and work-product protection law, or developing entirely new protections, in the CI context. To this end, the *Commentary* calls for enacting a qualified—but not an absolute—stand-alone cybersecurity privilege under which CI would enjoy some measure of protection against discoverability, whether or not lawyers were sufficiently involved in its creation to qualify the CI in question for the attorney-client privilege and/or the work-product protection. The *Commentary* also calls for state and federal law to recognize a "selective waiver" doctrine that provides a data holder's disclosure of CI to law enforcement would not waive any privilege that might otherwise be claimed in future civil litigation.

B. GENERAL GOVERNING PRINCIPLES

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

1. The Attorney-Client Privilege

The attorney-client privilege generally protects a communication made in confidence for the "predominant purpose" of obtaining legal advice from a lawyer.[4] The privilege protects communications, but it does not permit a party to resist disclosure of the facts underlying the communications. Its "purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."[5]

---

lege and work-product protection claims that might be made as to CI, the *Commentary* focuses solely on the U.S. legal standards. In so doing, the *Commentary* primarily focuses on *federal* rules and case law, while identifying noteworthy state-law trends or decisions as applicable or necessary, and thus primarily examines the work-product protection afforded under Federal Rule of Civil Procedure 26(b)(3) as well as the attorney-client privilege as elaborated under Federal Rule of Evidence 501 by reference to federal and state common law.

[4] *In re* County of Erie, 473 F.3d 413, 419–20 (2d Cir. 2007); United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961). Courts sometimes alternatively use the phrase "primary purpose" or "dominant purpose" in this context, acknowledging that it has the same meaning as "predominant purpose." *See, e.g.*, County of Erie, 473 F.3d at 420.

[5] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

In the corporate context, confidential communications between corporate employees and counsel for the predominant purpose of assisting counsel in rendering legal advice to the company are protected by the attorney-client privilege.[6] Courts generally have held under both federal common law and state law[7] that this includes not just communications with actual employees, but also with independent contractors who are the "functional equivalent" of an employee.[8] Because in-house counsel may play multiple roles in a corporation, *some* courts applying either federal common law or state law have imposed additional scrutiny to assertions of privilege involving communications with in-house counsel, requiring in-house counsel to make a "clear showing" that communications were made for a legal, rather than a business, purpose.[9]

Communications between "privileged persons" *may* include those between employees, in-house counsel or outside counsel, and any of the company's subsidiaries or affiliates and any combination of them. These could be communications: (1) from employees to counsel; (2) from counsel to employees; (3) between counsel; (4) between employees or their functional equivalents;[10] or (5) with qualified agents of counsel or the client (e.g., employees or counsel of an agent, confidential litigation consultants, or informal consulting experts).[11] The nature and scope of the privilege varies state-by-state and is not uniform as a matter of federal common law, with certain states and federal courts limiting the extent and/or existence of any claim of privilege, for example, between non-lawyer employees, or with functional equivalents and/or affiliated entities.

Courts have generally held under both federal common law and state law that, for the attorney-client privilege to apply, the dominant or predominant purpose of the communication itself must have been to solicit or render legal advice.[12] The majority of courts today employ a "functionality" or "subject-matter" test that extends the attorney-client privilege to include a company lawyer's com-

---

6 *Id.* at 396.

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

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

9 *See, e.g., In re* Vioxx Prod. Liab. Litig., 501 F. Supp.2d 789, 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.").

10 2 David M. Greenwald, Robert R. Stauffer & Erin R. Schrantz, Testimonial Privileges § 1:31 (2012).

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

12 *See In re* County of Erie, 473 F.3d 413. 420 (2d Cir. 2007) ("We consider whether the predominant purpose of the communication is to render or solicit legal advice.") (applying federal law); 1 THE AMERICAN LAW INSTITUTE, RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 72 cmt. c (2000) ("A client must consult the lawyer for the purpose of obtaining legal assistance and not predominantly for another purpose.").

munications with any corporate employee so long as the communication relates to the subject matter for which the company is seeking legal representation.[13] At least one state (California) is more protective, providing that communications will be deemed to present a prima facie claim of attorney-client privilege so long as obtaining advice was the predominant purpose of the *relationship* between the client and counsel.[14]

Courts have generally held under both federal common law and state law that the attorney-client privilege can extend to communications involving counsel-retained experts where the expert is necessarily included for the purpose of assisting the attorney in providing legal advice. Specifically, under what is often referred to as the *Kovel* doctrine, the attorney-client privilege will extend to the work and communications of third-party experts if the expert was hired "for the purpose of obtaining [confidential] legal advice from the lawyer."[15] In *Kovel*, the attorney hired an accountant to assist him in understanding his client's tax position, and the communications at issue were between the client and the accountant. The court analogized the accountant to a translator, whose assistance in overcoming a language barrier would not destroy the privilege. Where the requirements for this exception are met, i.e., where the expert's presence in the communication is necessary for counsel's provision of legal advice, courts have held that the privilege may extend not only to communications between counsel and the expert, but also to communications between the expert and the client directly.[16]

---

[13] THE AMERICAN LAW INSTITUTE, *supra* note 12, at § 73 (2000). Note: Some states continue to employ the more restrictive "control group" test, which designates only upper-level management as clients of the corporate counsel. *See, e.g.,* Alaska (*see* Manumitted Cos. v. Tesoro Alaska Co., 2006 U.S. Dist. LEXIS 57658, at *7 (D. Alaska Aug. 16, 2006)); Illinois (*see* Consolidation Coal Co. v. Bucyrus-Erie Co., 432 N.E.2d 250 (1982); Sterling Fin. Mgmt., L.P. v. UBS PaineWebber, Inc., 782 N.E.2d 895, 900 (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 (1981).

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

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

[16] *See* Umpqua Bank v. First Am. Title Ins. Co., 2011 WL 997212, at *7 (E.D. Cal. Mar. 17, 2011) (communications between client and counsel-retained expert protected where for the purpose of furthering legal advice); *see also In re*

For communications among company employees (or the functional equivalents of employees) that do not include counsel or counsel-retained experts, the inquiry is highly fact-dependent, and generally turns on the intent of the creator of the communications.[17]

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

2. Work-Product Protection Law

In U.S. federal court, the work-product doctrine is governed by Fed. R. Civ. P. 26(b)(3)(A), which provides that "a party may not discover documents and tangible things that are prepared *in anticipation of litigation* or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)."[18] To satisfy the "anticipation of litigation" test, a document must be prepared after a point at which the company "anticipated" that litigation would be filed against it. Courts applying the rule have differed somewhat in their formulation of the test for determining when an as-yet-uncommenced litigation is sufficiently "anticipated" to make work-product protection potentially applicable. They agree, however, that the prospect of that future litigation must be more than speculative.[19]

Evidence that courts have looked to in determining whether litigation was "anticipated" include evidence that a prospective plaintiff intended to make a claim;[20] hiring of outside counsel;[21] dissemina-

---

OM Group Sec. Litig., 226 F.R.D. 579, 588-89 (N.D. Ohio 2005) (same); *In re* Grand Jury Subpoenas Dated March 24, 2003, 265 F. Supp. 2d 321, 331-32 (S.D.N.Y. 2003) (same).

17 *E.g.,* Williams v. Sprint/United Mgmt. Co., 238 F.R.D. 633, 639–40 (D. Kan. 2006) (sustaining privilege as to drafts that ultimately were not shared with counsel, because they nonetheless "constituted communications made for the purpose of obtaining legal advice").

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

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

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

tion of a "litigation hold" or preservation notice;[22] and putting a potential adversary on notice, either directly or through public disclosure, of facts that reasonably could be expected to result in the adversary initiating litigation.[23]

In addition to showing that litigation was anticipated, the proponent of the work-product protection must also show that the document was prepared "in anticipation of" the anticipated litigation, and not for some other purpose. Most circuits decide this aspect of work-product protection by applying the "because of" test, asking if the document was prepared "because of" the prospect of the litigation in question[24] In regard to "dual purpose" documents that serve both business and litigation purposes, the "because of" test is often characterized as a "but for" test: "[w]here a document was created because of anticipated litigation, and would not have been prepared in substantially similar form *but for* the prospect of that litigation, it falls within Rule 26(b)(3)."[25] The Fifth Circuit applies the more restrictive "primary purpose" test, requiring that "the primary motivating purpose . . . was to aid in possible future litigation."[26]

Materials otherwise qualifying for work-product protection may be discovered under certain circumstances where a party "shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means."[27] But, "[i]f the court orders discovery of those materials, it must protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation."[28]

---

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

22 *See* Major Tours, Inc. v. Colorel, 2009 WL 2413631 (D.N.J. Aug. 4, 2009) (collecting authorities that deem litigation hold notices subject to work-product protection).

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

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

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

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

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

28 Fed. R. Civ. P. 26(b)(3)(B).

3. Waiver

The attorney-client privilege or the work-product protection may in certain circumstances be waived as to a document or communication that would otherwise be protected from discovery under one or both doctrines. The attorney-client privilege is more easily waived than the work-product protection. For instance, disclosure of an otherwise attorney-client privileged document or communication to any third party generally results in waiver of the privilege (subject to limited exceptions, such as for disclosures to a third-party having a common interest or who is the functional equivalent of an employee), whereas disclosure of a work-product protected document to a third party generally does not waive the protection unless the disclosure is to an adversary or a conduit to an adversary.[29] Courts have also indicated that disclosure of an attorney-client privileged communication within a company may waive that privilege if the disclosure is made to an employee who did not "need to know" of the document or communication.[30] Moreover, language in some decisions could be read to suggest that in jurisdictions that employ a "control group" test for attorney-client privilege, disclosures of attorney-client privileged communications to internal employees outside the "control group" may waive the privilege as well.[31]

Disclosure of attorney-client privileged or work-product protected documents or communications to a third party may result in waiver of the privilege or protection for the documents or communications not only as against that third party, but also as against other third parties. While at least one court has held that a "selective waiver" theory may protect a party who discloses information to a governmental entity from losing either the attorney-client privilege or the work-product protection as to that information as against other entities,[32] many courts have rejected this theory.[33] Some courts have allowed disclosure to law enforcement or regulators under some circumstances without

---

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

[30] *See, e.g.,* Verschoth v. Time Warner, Inc., 2001 WL 286763 at *3 (S.D.N.Y. Mar. 22, 2001) (company "lost any privilege with respect to" legal advice when that advice was conveyed to worker who did not need to know that advice).

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

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

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

waiving the attorney-client and work-product protections, provided that the company entered into a confidentiality or protective order containing appropriate non-waiver and other provisions.[34]

In addition, disclosure of attorney-client privileged and/or work-product protected information may operate not only as a waiver of the disclosed information as to others, but also as a waiver of attorney-client privilege and/or work-product protection as to any related *undisclosed* information, both as to the recipient of the disclosed information and as to others. Such subject-matter waivers historically were not recognized in the work-product protection context (with some exceptions),[35] but were typically recognized in the attorney-client privilege context.[36] Today, Federal Rule of Evidence 502, which became effective in 2008, consolidates treatment of the scope of waiver of the attorney-client privilege and work-product protection into a single regime when the disclosure is made in a federal proceeding or to a federal office or agency.[37] Under Rule 502, when such a disclosure waives the attorney-client privilege or work-product protection, the waiver extends to undisclosed information only if "the waiver is intentional, the disclosed and undisclosed communications or information concern the same subject matter, and they ought in fairness to be considered together."[38]

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

Taking the general principles of privilege and protection law and applying them to the CI context becomes more complex. The question of whether the attorney-client privilege and work-product protection apply to CI generally arises when a company is faced with litigation or an investigation following a security incident. During this post-incident litigation or investigation, many types of CI may be sought by a regulator or private plaintiff concerning actions taken by the company prior to and after the security incident. These types of CI may be relevant to show the organization's security posture pre-incident, the causes of the incident, and the efficacy of the response.

---

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

[35] *See, e.g.,* Pittman v. Frazer, 129 F.3d 983, 988 (8th Cir. 1997); 1 DAVID M. GREENWALD ET AL., *supra* note 10 § 2:32 (3d ed. 2015).

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

[37] Chick-fil-A v. ExxonMobil Corp., 2009 WL 3763032 (S.D. Fla. Nov. 10, 2009).

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

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

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

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

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

a. Types of Pre-Incident CI

Some of the potential pre-incident CI that may be sought in a post-incident situation include the following.

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

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

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

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

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

Similarly, while these technical inventories, configuration reviews, vulnerability scans, and penetration tests may be part of an organization's larger risk assessment process done at the behest of counsel, those activities often do not involve counsel.

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

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

employees, and sometimes these are people-based, such as the need to increase training or compliance.

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

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

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

In addition to security assessments, organizations will sometimes hire outside vendors to perform compliance audits, such as audits to assess for compliance with the Payment Card Industry Data Security Standard (PCI DSS). Again, these are often done without legal counsel's advice, in order to obtain independent certification of PCI compliance. Following up on these assessments, companies will often engage outside security vendors and/or legal counsel to assist in remediation of any gaps identified in the security assessment process.

iii. Policies and Procedures

Many aspects of a well-run and reasonable cybersecurity system are documented in IT, management, or employee policies or procedures. This could include policies and procedures directed at one specific security control. For example, an access-control policy would dictate how to determine who has access to what, document these permissions, and describe the process for terminating such access, granting additional access, or changing access. Accompanying forms may provide documentation of these decisions, and accompanying procedures would describe how to implement the specific access controls associated with each decision. Another example could be a mobile-device policy regarding how to handle company-owned or "bring your own" mobile devices. The policy could also be one that concerns incident response, privacy and cybersecurity generally, or acceptable use. Some state and federal laws require that organizations maintain a written information security policy, and many other standards indicate that such written policies are a requirement of reasonable cybersecurity.

While the legal team (in-house or outside) will typically be involved in drafting and revising the policies required by state and federal law, that may not be the case with respect to more technology-focused procedures, or technical configuration procedures, such as the type of encryption to use at

rest or in transit. During post-incident proceedings, both IT-focused and legal policies and procedures may be relevant and sought. In addition, drafts of those same policies and procedures may be requested. Decisions made during the drafting process may indicate risk-based approaches that can be questioned in hindsight.

iv. Tabletop Exercises

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

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

v. Internal Audit Reports

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

vi. Reports of the Security Team or Board-Level Committees

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

In addition, this category includes reports given to the board or board committees responsible for overseeing cybersecurity, as well as meeting minutes or other documentation of the board or board committee itself.

Each of the above categories of documents usually involves some assessment of the organization's information security posture. All will produce evidence of what the organization knew and when, and likely will result in the organization making decisions about what, if any, actions it will or will not take to reduce compliance gaps and identified risks. Below, this Part of the *Commentary* explores

how the attorney-client privilege and work-product protection may apply to these general categories of CI, and what factors might be determinative in whether the protection attaches, recognizing that most determinations will be highly fact-specific.

b. Attorney-Client Privilege

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

i. Involvement of a Lawyer

As discussed above, for documents and communications to be privileged, a lawyer must be involved in the circumstances surrounding the generation of the communication. If an attorney is not involved, under the general legal principles governing attorney-client privilege, the CI will not be considered privileged. Thus, referring back to the categories of CI listed above, any technical inventories, configuration reviews, vulnerability scans, or penetration tests that are done by an internal or outside security vendor or expert and not done to assist an attorney will not be privileged. The same is true for security-risk assessments, outside or internal audits, tabletop exercises, and reports of the security team or the board of directors.

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

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

Courts examining whether the communication is predominantly for the purpose of providing or soliciting legal (as opposed to business) advice will focus on several indicators. Courts will examine the content of the communications to determine whether they contain or ask for legal analysis or whether they primarily concern the growth and development of profit.[39] In the context of pre-incident CI, the question of whether certain communications were made or documents created for the predominant purpose of obtaining or giving legal advice is difficult. With respect to technical inventories, configuration reviews, vulnerability scans, and penetration tests, these documents often are part of an organization's ongoing IT operations. For example, an inventory of devices, software,

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

or locations of personal information is often part of the IT department's inventory control, which is a business function.[40] An organization may also measure response times for identifying, containing, and remediating security incidents to measure the quality and efficacy of its security team or to maintain its normal operations. This would also not be considered privileged, even if an attorney relied upon such information in conducting a security-risk assessment, prioritizing legal risk, or in drafting a report for the board of directors.

However, if this CI was created for the purpose of a legally driven or mandated security assessment, audit, or report, such underlying documents may be privileged. One can readily envision the need for such a legal analysis for any type of organization handling sensitive information; this is especially true given the broad-ranging cybersecurity activities over which the Federal Trade Commission (FTC)[41] has taken enforcement actions, including, for example, protection of passwords or adequacy of operating system security on smartphones. Other laws and regulations governing specific industries or enacted in certain states have express security requirements or require organizations to have "reasonable" or "adequate" security. These requirements include overarching statements regarding the comprehensiveness of the program, the existence of policies and procedures, training requirements, and the effectiveness of the security program. Lawyers may need to give advice regarding whether the company's security requirements comply with these laws and regulations, which often are opaquely drafted. Similarly, many laws and regulations require organizations to oversee the security of their vendors, so legal analysis of such vendor oversight will be necessary. Counsel may also need to be involved regarding compliance with commercial contracts requiring one party to "provide reasonable security measures" for the other party's confidential information or to engage in "adequate security measures."

In other contexts, courts will generally find that documents not primarily concerned with business or marketing decisions, but rather primarily related to legal concerns (including legal risk and potential litigation or regulatory enforcement) are privileged.[42] Given the complex legal landscape and varying cybersecurity standards applicable to organizations, to the extent a lawyer engaged in a security-risk assessment or audit focused on prioritizing security controls based on legal risks or compliance with legal requirements, as opposed to business decisions, courts may well find this pre-incident CI primarily related to legal concerns and risk and therefore privileged.

---

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

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

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

Similarly, internal audit reports drafted to provide insight to counsel, when counsel provides revisions and comments and uses the reports to provide advice to the organization, often are considered privileged.[43] However, the court held in *In re Premera Blue Cross Customer Data Security Breach Litigation (Premera II)* that internal data-security reports prepared before any breach had been discovered (as part of normal business functions), for the purpose of enabling the company to assess the state of its technology and security, were not privileged—even if counsel supervised the audits and later used them for legal advice.[44] But *Premera II* also held that if the draft report or emails about the draft were sent to counsel seeking legal advice, those documents would be protected.[45] In other legal contexts, such as securities litigation, reports from counsel to boards of directors, committees, subcommittees, and senior executives are largely considered the provision of legal advice and subject to privilege protection.[46] Courts would likely treat the cybersecurity context no differently. If a security report to the board of directors is by an attorney and incorporates a security team report, the report may be considered privileged, whereas a security team report without the attorney analysis likely will not be considered privileged. In this pre-incident CI context, this could include not only reports on legal risk, but also reports to the board concerning disclosures to the Securities and Exchange Commission (SEC) in connection with security-related incidents and cybersecurity risk in general. The reports of the board itself are likely not privileged, unless the board hires counsel to represent it in the preparation of the report.[47]

With respect to policies and procedures, generally, attorney-client privilege will apply to protect preliminary drafts of policies and procedures that contain legal advice and attorney opinions;[48] for example, if the policy or procedure contains comments to omit or add certain language for legal reasons. However, privilege will typically not apply to the final versions of policies and procedures—merely because they were drafted by in-house or outside counsel as the final versions constitute business communications, not legal advice communications.[49] These general principles appear as applicable to CI policies and procedures as to those that are created in other contexts.

In addition to the involvement of an attorney and whether the pre-incident CI was reviewed and revised or created to assess legal risk or otherwise assist in the provision of legal advice, the creator of the communication may have some impact on whether a court will determine whether the communication was made predominantly for the purpose of seeking legal advice. But "the mere fact that a

---

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

44 2019 WL 464963, at *7 (D. Or. Feb. 6, 2019).

45 *Id.* at *8.

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

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

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

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

document is created by a non-attorney is not dispositive of the privilege question, so long as the communication of the document to counsel was confidential and for the primary purpose of seeking legal advice."[50] Thus, whether the communicator is an attorney, or a member of the security team, or otherwise from the business, should not affect the ultimate decision of whether privilege applies, as long as the communication was made predominantly for the purpose of seeking legal advice. However, some courts apply additional scrutiny to communications between in-house (as opposed to outside) counsel and corporate employees to determine whether such communications were made predominantly for a legal as opposed to a business purpose.[51] By contrast, under the general tenets of attorney-client privilege, communications from "outside counsel are presumed to be made for the purpose of providing legal advice."[52] Thus, communications from in-house counsel may be less likely to be considered privileged, particularly with respect to security assessments, audits, and reports that have a dual purpose.

iii. Among or Within Privileged Persons

To be privileged, the communication must also be among or within privileged persons. To the extent an employee of the client sent or received the communication, the employee must qualify as part of the client under either the subject-matter or control-group tests described in Part B above. If not—for instance, because the communication was by a front-line IT analyst outside of the "control group" in a control-group jurisdiction—the privilege generally will not apply.[53]

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

In 1961, the U.S. Court of Appeals for the Second Circuit decided *United States v. Kovel*,[54] in which it considered whether communications with an accountant prevented attorney-client privilege protec-

---

[50] United States v. ISS Marine Servs., Inc., 905 F. Supp.2d 121, 128–29 (D.D.C. 2012) (citing *In re* Grand Jury (Attorney–Client Privilege), 527 F.3d 200, 201 (D.C. Cir. 2008) ("Attorney-client privilege applies to a document a client transfers to his attorney 'for the purpose of obtaining legal advice.'" (quoting Fisher v. United States, 425 U.S. 391, 404–5 (1976)))).

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

[52] *Id.* (emphasis omitted).

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

[54] 296 F.2d 918 (2d Cir. 1961).

tion. *Kovel* held that if the accountant (or other third party) was necessary to "interpret" a client's "complicated tax story to the lawyer" to enable the lawyer to represent the client, the accountant did not destroy the privilege between the lawyer and his client. Courts following *Kovel* have extended the doctrine to allow the attorney-client privilege to cover communications to and from other, non-accountant third-party experts and consultants in some circumstances as long as the communications were necessary to assist the lawyer in communicating with the client. Typically, communications with experts in the course of an engagement will not be considered privileged if (1) the communications were not necessary to assist the attorney in understanding communications from the client or (2) the consultant's expertise was used to make a business decision, rather than to assist the lawyers in communicating legal advice.[55]

The attorney-client privilege may also extend to third parties acting as agents of the client, rather than as an agent of the lawyer as under *Kovel*, although it is more limited. The functional-equivalent doctrine will apply when a third party is retained by a company and is intended to, and does, function as an employee.[56] To determine whether such a third party functions as an employee, courts will look to whether the third party was an integrated member of the company, whether he or she played a significant role in the company, and whether he or she was intimately involved in the creation, development, and implementation of information at issue in the privilege determination and/or the relevant project.[57]

If a third party creates pre-incident CI, then it is possible that technical inventories, configuration reviews, penetration tests, and other pre-incident CI may be considered privileged if they were created for the purpose of aiding counsel in providing an assessment or report to the client. In a decision concerning post-incident CI, *Genesco Inc. v. Visa, Inc.*, the court found that an assessment performed on the client's behalf, which suggested remediation measures, was privileged because the expert was "retained . . . to provide consulting and technical services so as to assist counsel in rendering legal advice."[58] While this concerned post-incident CI, the logic appears to apply equally to pre-incident CI.

---

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

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

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

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

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

iv. Reasonable Expectation the Communication Will Be Kept Confidential

As noted in Part B above, to be privileged, the communication must have been made in confidence, i.e., with the intent that it be kept confidential. If CI is created for the purpose of being shared with a third party outside the circle of privileged persons—for instance, a description of IT inventory prepared for distribution to an assessor not working for the company's counsel—the communication will not have the requisite confidentiality, and the privilege will not attach.[59] Once a communication is privileged, the question of whether further disclosure of the communication would destroy the privilege is an issue of waiver, addressed in subsection 3 below.

c. Work-Product Protection

As discussed in Part B, the work-product protection doctrine applies only to documents created "in anticipation of litigation." Although the application of this doctrine varies somewhat across states and jurisdictions, the requirement for a real threat of litigation, rather than the idea that sometime in the distant future there might be litigation, will typically result in no work-product protection for the above types of pre-incident CI. It is unlikely, therefore, that any of the pre-incident CI discussed above would be protected by the work-product doctrine.

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

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

---

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

a. Examples of Post-Incident CI

i. Forensic Investigations—Documents and Reports

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

ii. Post-Incident Security Assessments

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

iii. Remediation Efforts and Crisis Management[60]

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

* * *

As discussed below, in trying to determine whether or not documents falling in the above categories should be considered attorney-client privileged and/or work-product protected, and what practices may affect that determination, a few cases involving post-incident CI provide some guidance. In the world of post-incident CI, courts faced with privilege and protection issues have been attempting to apply general legal principles to these unique sets of documents. These fact-intensive decisions (as with most attorney-client privilege and work-product protection cases) will turn on a court's decision

---

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

as to whether or not the communication was made to solicit or render legal advice or in anticipation of litigation.

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

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

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

As with pre-incident CI, whether the predominant purpose of the CI in question was to provide legal advice, as opposed to serving a business purpose, is likely to become a prevalent fight in whether certain post-incident CI is privileged. This may be the case when in-house counsel is communicating internally with the organization directly following the incident. For example, questions may arise regarding whether the in-house counsel is merely trying to remedy the breach or is providing legal advice concerning how to manage breach notifications or legal risk. The communications may have a dual purpose to both assist in breach remediation *and* breach notification management or legal risk analysis, in which case the courts will determine the predominant purpose of the communications.

In *In re Target Corp. Customer Data Security Breach Litigation*, the court examined whether various types of post-CI information were protected by the attorney-client privilege.[61] The court analyzed whether the privilege applied to CI relating to a data-breach task force established by Target in response to the data breach.[62] Plaintiffs' counsel argued that the communications and documents were not protected by the attorney-client privilege because "'Target would have had to investigate and fix the data breach regardless of any litigation, to appease its customers and ensure continued sales, discover its vulnerabilities, and protect itself against future breaches.'"[63] Target argued that those communications and documents were protected because the task force was established at the request of its law-

---

[61] 2015 WL 6777384 (D. Minn. Oct. 23, 2015).

[62] *Id.* at *1.

[63] *Id.* (quoting Pls.' Letter Br. 3-4).

yers (both in-house and retained) to educate counsel about the breach and allow counsel to provide Target legal advice.[64] While the court did not specifically weigh the business and legal purpose of various CI, it did determine that some internal communications were privileged, while others were not, by discussing the purpose of the communications. Specifically, the court found that internal communications from Target's CEO to the Board of Directors were not privileged because they did not "involve any confidential communications between attorney and client, contain requests for or discussion necessary to obtain legal advice, nor include the provision of legal advice."[65] Conversely, the court did find that other communications with and documents created by the task force were privileged, as Target had demonstrated that the task force "was focused not on remediation of the breach, . . . but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice."[66] The court also found other email communications between in-house counsel and other Target employees privileged because they were made for the purpose of obtaining legal advice.[67] Evident in the court's determination is a consideration specifically regarding whether the communications and documents were created for the predominant purpose of providing or obtaining legal advice.

The District of Oregon, in *In re Premera Blue Cross Customer Data Security Breach Litigation (Premera I)*,[68] had opportunity to do the same. Similar to the court in *Target*, the *Premera* court engaged in a detailed analysis of whether CI was created for the primary purpose of informing counsel so that counsel could provide legal advice. The court evaluated the purpose behind CI created by non-attorneys that "incorporated" advice of counsel but were not sent to counsel, and CI created by employees "supervised" by counsel.[69] The court examined whether the CI was prepared primarily to assist counsel in providing legal advice, or whether the CI was prepared by the business to fulfill a business function, or required to be prepared by the business in response to the data breach, such as press releases, media interactions, and notices to consumers.[70] Generally, the court found that this CI was created for business purposes, not legal ones.[71] However, attorney redlines or edits communicating legal advice would be covered by the attorney-client privilege.[72]

Subsequently, in *Premera II*, the District of Oregon assessed the application of the attorney-client privilege to CI that was sent to and from counsel, as well as CI prepared at the request of counsel.

---

64 *Id.*

65 *Id.* at *2.

66 *Id.* at *3.

67 *Id.*

68 296 F. Supp.3d 1230 (D. Or. 2017).

69 *Id.* at 1240–47.

70 *Id.*

71 *Id.*

72 *Id.* at 1242, 1250.

The court stated that in order to qualify for the attorney-client privilege, emails sent to and from counsel about matters such as press coverage, notices to consumers, and remediation must request or provide legal advice (as opposed to containing merely a factual discussion), or they must contain facts transmitted to counsel so that counsel can provide adequate legal representation.[73] The court further stated that draft documents (e.g., draft notices) prepared by attorneys, at the request of attorneys, or by company employees or vendors and sent to or from attorneys for legal advice relating to the drafts are likely subject to the attorney-client privilege.[74] However, in the court's view, a draft document that is prepared for a business purpose and merely sent to an attorney for the attorney's file or information, or is distributed among company employees or to third-party vendors for general discussion with an attorney merely copied, is not privileged merely because an attorney received it.[75] The court further held that Premera's "investigation into the breach was conducted primarily for a business purpose."[76] But if an attorney took the information from these documents and drafted a different document in preparation for litigation, and/or received emails or draft reports seeking the attorney's advice, those documents would be protected.[77] And the court allowed that CI relating to Premera's later actions in response to the breach may also be privileged: "Other than the initial business steps of remediation, notifying customers, and making public statements, which Premera would have had to do regardless, the later actions by Premera were likely guided by advice of counsel and concerns about potential liability."[78]

ii. Among or Within Privileged Persons

Courts conduct a similar analysis with respect to CI created by third parties. In *Genesco*,[79] Genesco brought suit against Visa in response to Visa's attempt to assess more than $13 million in fines and assessments for Genesco's alleged failure to comply with Visa's cybersecurity standards. Visa had assessed the fines and assessments in response to a breach of Genesco's network that exposed credit card data.[80] Genesco retained a forensic investigator, Stroz Friedberg, to provide consulting and technical services to Genesco's in-house and outside counsel regarding the breach and its own cybersecurity posture, as well as with respect to a report issued by a forensic investigator authorized by the Payment Card Industry Security Standards Council, Trustwave International Security and Compliance (Trustwave).[81] Genesco provided evidence that it retained Stroz Friedberg, through outside

---

[73] 2019 WL 464963, at *2.

[74] *Id.*

[75] *Id.*

[76] *Id.* at *7.

[77] *Id.* at *7-8.

[78] *Id.*

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

[80] *Id.*

[81] *Id.* at 169.

counsel, specifically to conduct an investigation, under privilege, following the earlier investigation by Trustwave, to assist Genesco's attorneys in providing it legal advice.[82]

In these circumstances, the court, relying on *Kovel*, found that the documents and communications generated by the forensic expert were protected by the attorney-client privilege because the expert was "retained by counsel for the purpose of providing legal advice."[83] The court noted that the privilege extended to Stroz Friedberg because the firm "assisted counsel in his investigation."[84] The court also found, separately, but relying on its earlier ruling, that the privilege applied to documents and communications with IBM, which was retained to provide advice concerning remediation, because it was also hired to assist counsel in rendering legal advice to Genesco.[85]

The court also addressed the privilege issues associated with third-party consultants in the *Target* case.[86] In that case, Target had hired a consultant firm to conduct two investigations following its breach. One investigation was conducted by Target's outside counsel, which hired the expert to provide the attorneys information about the breach and how to defend Target; the other investigation was conducted by the consultant firm "on behalf of several credit card brands" to assist in determining how the breach happened and how to remediate.[87] While the two investigations were being conducted by the same outside technical firm, the consultant set up two separate teams that did not communicate with one another.[88] At issue in the action was whether the documents created by and communications with the consultant team hired by outside counsel would remain privileged and protected from disclosure.[89]

The court found that the documents associated with the team of experts retained by outside counsel were protected by the attorney-client privilege because the investigation "was focused not on remediation of the breach, . . . but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice."[90]

---

82 *Id.* at 180-81.

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

84 *Id.*

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

86 *In re* Target Corp. Customer Data Security Breach Litigation, 2015 WL 6777384 (D. Minn. Oct. 23, 2015).

87 *Id.*

88 *Id.*

89 *Id.*

90 *Id.* at *3.

Similarly, the *Premera* decisions evaluated whether CI created by a third-party public relations firm[91] to inform counsel and by a third-party forensic investigator prior to and after the discovery of the breach was protected by the attorney-client privilege.[92] Relying on the primary purpose of the third party, the *Premera I* court generally found that CI created by an attorney-hired public relations firm following the breach (and communications between the firm and Premera) was not privileged. The court relied on the business nature and function of the public relations firm and denied the ability of companies to cloak CI in privilege merely by claiming such CI was created on behalf of an attorney or under the supervision of an attorney. Likewise, the court in *Premera II* held that merely sending such CI to counsel did not make it privileged.[93] The court held in *Premera I and II*, however, that if communications were sent to or from counsel seeking or providing actual legal advice, such as about possible legal consequences of proposed text or an action being contemplated by Premera, then such communications would be privileged.[94]

In connection with the third-party forensic investigator, two sets of CI were at issue: (1) CI created by the investigator prior to discovery of the breach, when the investigator had been hired by the company; and (2) CI, including at least one forensic report, created by the investigator after the discovery of the breach, after being hired by counsel, and after entering into a new and separate statement of work.[95] The court summarily rejected the notion that simply because the forensic investigator was hired by counsel after discovery of the breach, documents and communications relating to that investigator would necessarily be covered by the attorney-client privilege.[96] Largely relying on the fact that the company had initially hired the forensic investigator for business purposes prior to discovery of the breach, the court found that Premera would have "the burden of showing that [the forensic investigator] changed the nature of its investigation at the instruction of outside counsel and that [the forensic investigator's] scope of work and purpose became different in anticipation of litigation versus the business purpose [the forensic investigator] was performing when it was engaged by Premera before the involvement of outside counsel."[97] The court held, however, that if there were specific documents or portions of documents relating to the investigator that were prepared for the purpose of communicating with an attorney for the provision of legal advice, those particular documents could be withheld as attorney-client privileged.[98]

---

91 The court conducted a similar analysis with respect to eDiscovery and other vendors hired by Premera. *In re* Premera Blue Cross Customer Data Security Breach Litig., 296 F. Supp.3d 1230, 1240–47 (D. Or. 2017) [hereinafter *Premera I*].

92 *Id.*

93 In re Premera Blue Cross Customer Data Security Breach Litigation, 2019 WL 464963, at *4 (D. Or. Feb. 6, 2019) [hereinafter Premera II].

94 *Premera I,* 296 F. Supp.3d at 1240-47; *Premera II*, 2019 WL 464963, at *2-3.

95 *Id.*

96 *Id.*

97 *Id.*

98 *Id.*

Based upon the *Target*, *Genesco*, and *Premera I* and *II* decisions, it appears courts that face attorney-client privilege claims as to post-incident CI will employ the generally applicable principle of focusing on the predominant purpose of the CI in question to make such privilege determinations—that is, whether the documents and communications were created or solicited predominantly for the purpose of aiding the lawyer in providing legal advice, including not only those created by forensic experts, but also by non-forensic investigator experts like public relations consultants.[99]

In this regard, courts will likely look to who retained the service provider as evidence of the purpose of, and hence whether to apply the privilege to, the CI at issue. Courts may be more likely to find a service provider was retained to assist a lawyer in providing legal advice if such provider was retained by counsel, as both the *Target* and *Genesco* courts noted that the expert was retained by counsel in making the determination that the CI at issue was privileged. While not noted by the court in *Target* and *Genesco*, courts may also look to the agreement with the expert regarding the extent to which documents/communications generated as part of the engagement will be kept confidential, the extent to which the lawyer actually relied upon the report and documents of the provider, and the extent to which the lawyer supervised the outside consultant.[100]

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

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

i. Because of Anticipated Litigation

Courts dealing with work-product protection claims that are made as to post-incident CI have examined carefully whether the post-incident CI in question was created "because of" anticipated litigation, as is required for work-product protection. For example, the *Target* court found that communications from Target's CEO to the Board of Directors did not qualify for work-product protection because nothing showed that the update to the Board was made *because of* any anticipated litigation.[101] However, as with respect to the application of the attorney-client privilege in that case, the court

---

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

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

[101] *In re* Target Corp. Customer Data Security Breach Litig., 2015 WL 6777384, at *3 (D. Minn. Oct. 23, 2015).

found that the documents created by and communications with the data-breach task force were protected by the work-product doctrine.[102] The court found those documents were created to "prepare to defend the company in litigation that was already pending and was reasonably expected to follow."[103]

A California federal court has similarly examined whether post-incident CI was prepared "because of" anticipated litigation in *In re Experian Data Breach Litigation*.[104] That court found that the question is whether the totality of the circumstances suggests that the document "'was created because of anticipated litigation, and would not have been created in substantially similar form but for the prospect of that litigation.'"[105] The court examined whether a report drafted by an outside forensic investigator was drafted "because of" anticipated litigation, focusing on whether the report was more relevant to the internal investigation and remediation of the incident, or to the defense of the litigation.[106] In making its determination, the court relied in part on the fact that the full report was shared only with the legal team (as opposed to the entire incident response team).[107] The court reasoned that the report would have been given in full to the incident response team if it "was more relevant to Experian's internal investigation or remediation efforts, as opposed to being relevant to defense of this litigation."[108]

In *Genesco*, the court also examined whether documents created by and communications with third-party experts were protected by the work-product doctrine.[109] Citing *United States v. Nobles*, the court found this post-incident CI squarely within the doctrine because the investigator was counsel's agent and was working under counsel's direction to prepare for litigation.[110]

Similarly, in *Premera I*, the court stated that if the CI at issue (drafts and CI created by employees and third parties following the breach, including press releases, notices, etc.) had a dual purpose, that CI would be protected by the work-product doctrine if the CI was created "because of" the prospect of litigation.[111] The court rejected the notion that the CI at issue was necessarily created because of litigation, rather than for business reasons, simply because the business functions at issue were directed

---

[102] *Id.*

[103] *Id.*

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

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

[106] *Id.* at 3-4.

[107] *Id.*

[108] *Id.*

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

[110] *Id.* at 191.

[111] Premera I, 296 F. Supp.3d 1230, 1240-47 (D. Or. 2017).

by attorneys.[112] Rather, the court held that in order to establish that a particular document is subject to work-product protection, Premera must show that the document was prepared specifically because of anticipated litigation.[113] Likewise, with respect to the third-party investigator, the court relied on the fact that the investigator had not changed its scope or purpose at the direction of outside counsel in finding that Premera had not yet established that the CI relating to the investigator was created because of the anticipated litigation.[114] However, the court noted that if there were specific documents relating to the investigator that were created because of anticipated litigation, Premera could properly withhold them as subject to the work-product protection.

In *Premera II*, the court held that narratives drafted to help prepare responses to regulatory inquiries were entitled to work-product protection insofar as they were prepared for the regulatory inquiry and not a general business purpose.[115] It also held that draft notices and scripts prepared by counsel because of anticipated litigation were protected.[116] However, it stated that a timeline prepared by in-house counsel relating to remediation would not be protected if Premera did not demonstrate that the timeline would have been prepared in substantially different format absent anticipated litigation or regulatory investigations.[117]

Whether post-incident CI is protected by the work-product doctrine may also include an examination of when the documents or information were generated. Often, internal IT or security teams may create documents and engage in communications while trying to determine whether a breach occurred. If no lawyer is engaged in these communications or consulted and no regulatory investigation or litigation has been contemplated up to that point, courts may be less likely to find that these early documents were created in anticipation of litigation. If a company is contemplating that a security incident may result in an investigation or litigation, and has open lines of communication between first-line responders on the IT or security team and the relevant in-house or external counsel in connection with that contemplated investigation or litigation, the work-product protection is more likely to apply.

A court's determination regarding whether litigation was reasonably anticipated may rely either on language directly in a retainer agreement (as in *Genesco*)[118] or because litigation, though not yet com-

---

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] Premera II, 2019 WL 464963, at *7 (D. Or. Feb. 6, 2019).

[116] *Id.* at *6.

[117] *Id.* at *7.

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

menced, has at least been threatened. Courts may also rely on the issuance of a litigation hold, the retention of outside counsel, or documentation that litigation or an investigation may be forthcoming.[119]

Analogous case law—such as the line of decisions concerning how the work-product protection's "anticipation of litigation" requirement applies to a situation in which a company suspects a defect in its product and investigates regarding the defect, its scope, and remedial action—further underscores that courts likely will carefully distinguish between documents prepared because of anticipated litigation and documents prepared for business purposes. For example, in *Adams v. Gateway, Inc.*, concerns about problems with its computers led Gateway to launch an internal investigation headed by an attorney and labeled a "legal investigation."[120] The attorney interfaced with engineers and other technical personnel as part of the investigation, and Gateway attempted to claim that several of the documents related to the investigation were work-product protected on that basis.[121] The court disagreed, finding that while Gateway may have become aware of product performance issues as a result of a litigation, "the investigation had at its core the diagnosis and resolution of potential problems" and was motivated by "Gateway's self-interest as a retailer of computer products."[122] In determining whether specific documents were work-product protected, the court found some of the documents showed "concrete litigation-related preparation" and attorney instructions, whereas others showed "technical efforts and results," not revealing or responsive to litigation concerns.[123] Thus, the court ordered the production of the latter documents.[124]

---

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

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

[121] *Id.* at *5–6.

[122] *Id.* at *4.

[123] *Id.* at *17.

[124] *Id.* at *34, *38. Similarly, in Janicker by Janicker v. George Washington Univ., the District Court of Washington, D.C., found that "[i]f in connection with an accident or an event, a business entity in the ordinary course of business conducts an investigation for its own purposes, the resulting investigative report is producible in civil pretrial discovery." 94 F.R.D. 648, 650 (D.D.C. 1982). The court found that the report was "prepared in the ordinary course of business with the primary motivation being to determine what steps could be taken to prevent any repetition of such a tragedy to protect other resident college students and the University's standing in the college community and in recruiting students to attend the institution in the future." *Id.* For additional examples in the defective products' context, *see, e.g.*, Soeder v. Gen. Dynamic Corp., 90 F.R.D. 253, 255 (D. Nev. 1980) (granting plaintiffs' motion to compel in-house report regarding aircraft accident on grounds that "given the equally reasonable desire of Defendant to improve its aircraft products, to protect future pilots and passengers of its aircraft, to guard against adverse publicity in connection with such aircraft crashes, and to promote its own economic interests by improving its prospect for future contracts for the production of said aircraft, it can hardly be said that Defendant's 'in-house' report is not prepared in the ordinary course of business"); Bradley v. Melroe Co., 141 F.R.D. 1 (D.D.C. 1992) (ordering production of files related to incidents involving product); Scott Paper Co. v. Ceilcote Co., Inc., 103 F.R.D. 591, 595–96 (D. Me. 1984) (recognizing the "important but subtle distinction between reports prepared in response to

Other case law evaluating whether an internal investigation or an internal audit qualifies for work-product protection indicates that courts are not likely to find post-incident CI work-product protected merely because counsel involved in a litigation generated or received the CI in question.[125] This may be more true to the extent it involves in-house counsel, as opposed to outside counsel.[126] Courts may be more likely to afford work-product protection to an internal investigation with a dual purpose if the litigation purpose is clear from the particular documents at issue, such as the legal ramifications of the investigation's findings.[127]

Given the case law in both the CI and non-CI scenarios, courts seem likely to scrutinize whether documents claimed to be work-product protected were prepared in anticipation of litigation or an investigation. Such scrutiny may include an examination as to whether counsel had a significant enough role in the preparation of a document as to suggest that it was created "because of" and/or for the "primary purpose of" aiding litigation, and/or whether it would not have been prepared in substantially the same form but for the litigation. If portions of documents were created in anticipation of litigation and others were not, segregation of these portions may also affect a court's decision.[128]

ii. Substantial Need

As discussed in Part B, work-product protection is not absolute, and courts may order documents and information covered by the work-product protection produced if the requesting party can show

---

an unfortunate event, that might well lead to litigation, and materials prepared as an aid to litigation" and finding that documents had business purpose of maintaining relationship with plaintiff and avoiding litigation).

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

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

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

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

a substantial need for the information. The court in the *Target* case specifically addressed whether the work-product protection could be overcome by the "substantial need" exception, but found that plaintiffs did not have a substantial need to discover the work product being withheld because Target had "produced documents and other tangible things, including forensic images, from which Plaintiffs can learn how the data breach occurred and about Target's response to the breach."[129]

The court also addressed the substantial-need issue in *Experian*. In that case, plaintiffs argued that Experian's third-party expert had access to live servers that plaintiffs did not have access to, and therefore plaintiffs had a substantial need to access the work-product protected information.[130] Because Experian refuted that claim and plaintiffs could "get those exact server images and hire their own expert to perform the work," plaintiffs did not meet the substantial-need exception to the work-product protection.[131]

These cases indicate that courts may be less likely to find work-product protection over post-incident CI in instances in which only one investigation occurred into the causes of and responses to a data breach, unless the party seeking to apply the protection can prove that the opposing party has sufficient information regarding the breach, its investigation, and the response to the breach.

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

Even if a court finds that the attorney-client privilege and/or work-product protection apply to certain CI, it may determine that the company has waived the privilege or protection as to that CI. This could be because the company disclosed the CI to a third party—which could include disclosure to: (1) a regulator (the FTC, the SEC, state attorneys' general, Office for Civil Rights (OCR), etc.) pursuant to statute, an investigative demand, or voluntarily; (2) contract parties whose data or systems may have been impacted during an incident; (3) law enforcement to assist in the investigation seeking to apprehend the criminal attacker; (4) an information sharing organization; (5) an insurance carrier; (6) an affiliated entity; or (7) other parties involved in the same or similar litigation. A court could even potentially find waiver because company personnel disclosed the CI to others within the company.[132]

---

[129] *Id.*

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

[131] *Id.*

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

a. Disclosures to Direct or Indirect Contract Parties

In *Genesco,* the court relied on *In re TJX Cos. Retail Sec. Breach Litig.*[133] in determining that the company's disclosure of brief portions of the counsel-retained forensic expert's report to Visa and the assistance of the forensic expert in creating an annotated response to Visa's forensic report did not constitute a waiver of the attorney-client privilege and work-product protection as to other documents of the forensic expert.[134] And in *Premera II*, the court suggested that whether disclosure of a document to a third-party vendor created a waiver would depend on whether the vendor is providing a "legal" as opposed to "business" service.[135] While neither *Genesco, TJX,* nor *Premera II* clearly distinguished between the test for waiver of the attorney-client privilege and the test for waiver of the work-product doctrine, these tests are in fact very different, with the attorney-client privilege generally being much more readily subject to waiver.[136] That being the case, there may be circumstances in which disclosure of CI to one person will waive the attorney-client privilege, but not the work-product protection, as to that CI in regard to other persons.

b. Disclosures to Internal Company Employees

One example of a situation where such differing results could arise is the disclosure of an attorney-client privileged and work-product protected forensic report, cybersecurity assessment, or other CI to internal company employees. While such a disclosure would *not* result in a waiver of the work-product protection unless a court were to somehow conclude that the employee recipient was likely to turn the report over to an adversary, the disclosure might result in waiver of the attorney-client privilege if the employee recipients did not "need to know" the information in the CI (e.g., where there was no need for the employee to provide feedback to the attorney on the report to facilitate the attorney's legal advice)[137] and/or the recipient employees were outside of the company's "control group."[138] Under either test, courts will likely scrutinize the employee recipients to determine whether their receipt of, for instance, an attorney-client privileged data-breach forensic report results in waiver of the privilege. For example, though an IT analyst may rank far lower on the company hierarchy than a vice president of sales, the IT analyst's role and knowledge may be critical for enabling the company's attorneys to provide legal advice. If so, sharing the forensic report with the IT analyst

---

[133] 246 F.R.D. 389 (D. Mass. 2007).

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

[135] Premera II, 2019 WL 464963, at *9 (D. Or. Feb. 6, 2019).

[136] *See* Part B.3 *supra*.

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

[138] *See* Part B.3 *supra*.

is unlikely to waive the attorney-client privilege under the widely used subject-matter test. However, insofar as the IT analyst is not considered part of the company's control group, sharing the report may waive the privilege in a control-group jurisdiction like Illinois.

c. Disclosures to Law Enforcement

Courts may also eventually need to determine whether, when, and to what extent, protected CI loses its protection by reason of being disclosed to law enforcement in connection with its investigation seeking to apprehend the perpetrator of the incident or to a regulator during its investigation of the breached entity's possible role in the incident. As noted in Part B above, at least one court has held that a "selective waiver" theory may protect a party who discloses information to a governmental entity from losing the attorney-client privilege or work-product protection as to that information as against other entities.[139] However, many courts have rejected this theory, despite the public policy benefits of such a position.[140] Some courts have allowed disclosure to law enforcement or regulators under some circumstances without waiving the attorney-client and work-product protections, provided that the company entered into a confidentiality or protective order containing appropriate non-waiver and other provisions.[141] Thus, while it may not be effective to prevent waiver, depending on the court at issue and the circumstances of the disclosure, inclusion of non-waiver and confidentiality provisions or agreements in any disclosure of CI to the government may at least increase the likelihood that a court will not find that such disclosure waived, as against other persons, any attorney-client privilege and/or work-product protection to which the disclosed CI might otherwise have been entitled.

d. Disclosures to Information Sharing Organizations

Information sharing of certain aspects of an incident or other vulnerabilities may also be protected via the Cybersecurity Information Sharing Act (CISA) of 2015. CISA provides protections to encourage sharing cyber threat indicators and defensive measures with the federal government, state

---

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

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

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

and local governments, and other companies and private entities. Relevant here, CISA provides that the sharing of information pursuant to CISA does not waive as to other persons any attorney-client privilege or work-production protection to which the information may have been entitled and also protects information shared from Freedom of Information Act (FOIA) disclosure.[142]

e. Common Interest, Joint Defense, and Joint Representation

Whether the sharing of CI with insurance providers, third parties whose systems or data may be involved in the incident, and/or affiliated entities waives any attorney-client privilege or work-product protection that may otherwise have applied to such CI as against other persons may revolve around a court's determination as to whether the parties have a common interest. If the CI in question otherwise qualifies for protection under the attorney-client privilege or work-product doctrine, courts will typically find that a party sharing information with a person or entity in pursuit of a common legal goal or concerning a matter of mutual legal concern did not waive the privilege/protection by sharing the information.[143] Sharing of CI with third parties may qualify for the joint defense privilege if the contracting parties have a common legal goal, such as to prepare for defense of claims anticipated to be asserted against both entities by consumers or regulators. However, if one of the two parties believes the other is responsible for the incident and the disclosure occurs within the context of a discussion of who is at fault, a common legal goal will not be present. The common interest doctrine may also shield communications between affiliated companies, although a prominent appellate decision held that the so-called "joint representation doctrine"—which prevents waiver of communications between clients who share a common attorney—is a better fit for situations where a single attorney or group of attorneys represent multiple corporate affiliates.[144] A fact-intensive determination will dictate whether a common interest exists between an insured and its insurer, as courts do not recognize a blanket privilege between insureds and insurers.[145] Similarly, where the two parties are in other sorts of privity, their contractual relationship may assist or work against a common-interest claim, depending on the nature of the contract and the relationship between the parties.

The court in *Premera I* had the occasion to review whether the disclosure of CI to third parties who were not defendants in the same litigation, but in similar litigations, was shielded by the common-

---

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

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

[144] *In re* Teleglobe Commc'ns Corp., 493 F.3d 345, 370 (3d Cir. 2007) ("Courts typically offer versions of three arguments for not construing the sharing of communications with the corporate family as a waiver: (1) the members of the corporate family comprise one client; (2) the members of the corporate family are joint clients; and (3) the members of the corporate family are in a community of interest with one another. Of these three rationales, we believe only the second withstands scrutiny.") (internal citations omitted).

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

interest doctrine.[146] Noting that generally joint-defense or common-interest parties are subject to the same litigation, the court found that entities in similar litigation to which Premera had disclosed documents would share a sufficient common interest if they were subject to the same data breach, but otherwise would not.[147]

f. Subject-Matter Waiver

Finally, in a situation where disclosure of attorney-client privileged and/or work-product protected CI operates as a waiver of the privilege and/or protection afforded to the *disclosed* CI, the question may then arise whether such disclosure also operates as a waiver of the privilege and/or protection as to related *undisclosed* CI, both as to others and as to the recipient of the disclosed CI. Under the general principles discussed in Part B.3 above, whether there is such a "subject-matter waiver" may turn on both the identity of the recipient (e.g., federal government versus private party) and the circumstances surrounding the disclosure.

The court in *Premera I* had occasion to briefly consider whether a disclosure to third parties involved in similar litigation constituted a subject-matter waiver of all related documents. The court indicated that it would have found subject-matter waiver of all communications relating to the same subject matter; however:

> because Premera believed in good faith that it and these entities were subject to the common interest exception to waiver, under the unique circumstances of this case, fairness requires that the waiver of privilege extend only to the communications actually shared among the entities and not to all documents relating to the same subject matter that was addressed in the communications that were shared.[148]

Thus, *Premera* suggests that broad subject-matter waiver may generally apply, stripping protection from otherwise privileged or protected information.

Finally, courts have also indicated that the use of attorney-client privileged information affirmatively or as a defense could also constitute a waiver of the privilege in regard to related privileged CI. In *In re United Shore Financial Services, LLC*, the court found a waiver of the privilege in regard to CI created by an investigator because, according to the court, the defendant had used the conclusion of the investigator as a defense in the litigation.[149]

---

[146] Premera I, 296 F. Supp.3d 1230, 1247-50 (D. Or. 2017).

[147] *Id.*

[148] *Id.* at 1247–49.

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

Considering how courts have and presumably will analyze attorney-client privilege and work-product protection in the CI context, the *Commentary* next seeks to address whether such application of traditional principles adequately promotes the policy rationales in this context.

D. THE PATH FORWARD

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

1. A Critical Assessment of the Existing Regime

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

These varying interests cut in different and sometimes conflicting ways.

- *Data holders*: Typically, data holders will want a legal regime that prevents forced disclosure of CI to its actual or potential adversaries in a litigation or regulatory enforcement

context. Even where it makes sense from a data holder's perspective to share CI with one or more of those adversaries, the data holder will want to make that decision on its own terms, rather than have the law require disclosure.

- *Law enforcement*: The interests of criminal law enforcement tend to favor disclosure of CI, at least to law enforcement. Criminal law enforcement will need some access to CI to find clues about potential wrongdoers, even if criminal law enforcement is much more interested in misconduct by hackers rather than misconduct by data holders.

- *The public*: The interests of the public are as varied as the public itself. To some extent, the public whose information is in the hands of data holders may want access to the data holders' CI, to make better decisions about sharing information with the data holder in the future. On the other hand, to the extent data holders will be better able to protect sensitive information if CI is not exposed, the public itself may be protected by having that CI under wraps.

- *Regulators*: A regulator's interest in enforcing the law will almost always argue in favor of more rather than less access to CI. CI contains critical clues about a data holder's legal compliance, and a regulator is practically working blind if it is unable to view that information.

- *Affected individuals*: Similarly, the interests of individuals whose personal information may have been, or may be vulnerable to being, compromised in a cyberattack will almost always argue in favor of more rather than less access to CI. As CI contains critical clues about a data holder's compliance with any potentially applicable legal regime that imposes a cybersecurity duty in regard to personal information, such individuals will want access to CI to evaluate and pursue claims that the data holder violated that duty.

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

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

The rigid structure of the rules governing the attorney-client privilege, and even the somewhat more flexible approach that recognizes exceptions to work-product protection, however, largely preclude

any balancing of the interest in effective legal representation against the other, similarly significant, interests that cybersecurity litigation implicates. That same rigid structure also ties any expansion or reduction of these protections in the cybersecurity context to a set of concerns that, at best, occasionally and largely incidentally overlap with the important objectives of incentivizing the adoption of robust and resilient cybersecurity measures and protecting all concerned against criminal cyberattacks.

a. Perverse Incentives Created by the Existing Regime

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

Risk assessment activities have substantial operational components, because they are intended to create, test, and improve security policies and practices. Distinguishing between the core operational activities and activities arguably conducted for the purpose of seeking legal guidance is the central factor in determining whether and to what extent attorney-client privilege or work-product protection will apply to any given CI.[150] Moreover, pre-incident risk assessment activities typically are not initiated in response to a specific or reasonably foreseeable threat of litigation, which makes extending work-product protection to them next to impossible.

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

---

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

While the example of risk assessments well illustrates the perverse incentives the existing regime creates regarding the creation of CI, those perverse incentives extend to *any* CI that discloses a company's mental impressions, conclusions, opinions, assessments, evaluations, or theories concerning its cybersecurity posture, a cyberattack on the company, or its actual or potential actions in anticipation of, or in response to, a cyberattack. The more frank and pointed companies are when they generate such CI, the more efficacious their cybersecurity efforts would be expected to be. But the current regime chills companies from generating such frank and pointed CI, because it allows such CI to be discovered and used against the company in question by regulators and private litigants intent on building a case that the company's cybersecurity efforts were legally insufficient.

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

To be sure, this dynamic is arguably not as relevant after a breach. Post-breach CI is frequently generated specifically with the guidance of outside counsel and in anticipation of litigation. Thus, treating the discoverability of post-breach CI under the guise of the influence of lawyers and litigation is at least less unrealistic for post-breach situations. Most of the few cases in this area confirm this assessment: in both the *Target* and *Genesco* cases courts protected almost all the CI at issue from disclosure.[151] *Premera Blue Cross* is a recent important exception to this trend.[152]

But in the post-breach context, a different sort of perverse incentive can become operative. Ideally the rules for disclosure of CI would promote robust cooperation between the victims of criminal cyberattacks and the criminal law enforcement authorities responsible for investigating such crimes and catching the perpetrators. Yet under the limited protections the existing regime affords against disclosure of attorney-client privileged and work-product protected materials to third parties result-

---

[151] *Id.* (denying plaintiffs' motion to compel with respect to all documents except a few post-breach emails updating the Board of Directors on Target's "business related interests . . . in response to the breach"); Genesco, Inc. v. Visa U.S.A., Inc., 302 F.R.D. 168, 194 (2014) (barring discovery of all contested documents except those connected to "remedial measures that Genesco took in response to" the breach). Moreover, to the extent post-incident CI is not protected by the attorney-client privilege or work-product protection, it may nevertheless in many cases be inadmissible as a "subsequent remediation measure" under Federal Rule of Evidence 407 and its state analogs insofar as it relates to the company's efforts to remediate the breach. *See* FED. R. EVID. 407 ("When measures are taken that would have made an earlier injury or harm less likely to occur, evidence of the subsequent measures is not admissible to prove negligence, culpable conduct, a defect in a product or its design, or a need for a warning or instruction."). This aspect of the existing regime arguably reduces or eliminates whatever disincentive companies otherwise might have to take remediation measures in the wake of a data security incident.

[152] Premera I, 296 F. Supp.3d 1230 (D. Or. 2017) (rejecting defendant's assertion that several categories of documents, including a forensic investigator's report, prepared post-breach after outside counsel was hired to investigate, were not protected work product because they served a primarily business purpose).

ing in a waiver of the privilege or protection as to other third parties, cyberattack victims may be reluctant to disclose privileged or protected CI to law enforcement. Such cyberattack victims may justifiably be concerned that such disclosures will waive as to their actual and potential litigation and regulatory adversaries the privilege/protection that the CI otherwise would have enjoyed. To the extent such concerns result in criminal law enforcement authorities being denied access to CI that would have assisted their efforts to bring cyberattack perpetrators to justice (and/or delaying access while the victim figures out a "workaround" to share the CI without waiving the privilege or protection), the current regime will have operated against, rather than in support of, the goal of promoting robust cooperation between those authorities and the victims of the crimes they are investigating.

b. The Disadvantages of Involving Counsel in Creating CI

The distinction courts have drawn in the post-breach context between reports developed under the direction of counsel—especially outside counsel—and those directed by security professionals, likely will apply to pre-incident risk assessments. As a result, a consensus is emerging that to the extent that organizations want to shield CI from being discovered in litigation, they should seek to "cloak" all pre- and post-incident cybersecurity work under privilege and/or work-product protection by retaining outside counsel or using inside counsel to hire and direct these efforts.

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

- *Risk That Work Will Not Be Protected.* Even when counsel that is retained to provide legal advice and/or in anticipation of litigation with regard to a company's cybersecurity conducts or commissions the activities that generated the CI in question, the risk remains that those activities will be viewed by a court as primarily operational rather than legal, and therefore the CI is not protected from disclosure. This risk is heightened in the pre-incident context because, as noted above, the activities that generate CI are not tied to any specific pending or anticipated legal action or investigation. Some have argued that the increasingly pervasive risk of a breach strengthens the case that all security-planning activities are tied to assessing legal and regulatory risks, but no court has yet embraced that view. Moreover, that view undermines a core premise of both the work-product protection and the attorney-client privilege that courts can and should carefully distinguish between operational activities and legal advice and strategy when applying those doctrines. Routinely involving counsel in more data-security-related activities, especially activities with little or no concrete legal dimension, increases the risk that some or all of the CI generated by such activities will not be protected under either doctrine.

- *Increased Cost.* Involving counsel, in particular outside counsel, in generating CI often increases the costs of the activity in question. Retaining outside counsel incurs fees; involving inside counsel redirects resources.

- *Potential Duplication*. Even where an organization involves counsel to strengthen the case for protection of CI, there inevitably will be some duplication between the operational and legal processes. The dual track process that was used in the *Target* litigation is a prime example.

- *Inappropriate Expertise*. Inside and outside counsel may not always be the best qualified to lead many cybersecurity activities. The internal information-technology personnel or an outside security firm is a more appropriate choice to lead the effort in some instances.

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

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

d. To What Extent the Current Regime Promotes Relevant Interests

Predictably, when it comes to protecting (or not protecting) CI from disclosure, the interests of data holders, law enforcement, the public, civil regulators, and individuals affected by a cyberattack cut in different and sometimes opposing ways. For data holders, the current regime may create incentives to avoid creating potentially damaging CI[153] that could be used by a litigation adversary or a regulator to impose liability. Those same risks incentivize structuring information security programs to protect as much information as the current regime allows, even where doing so involves the above-mentioned negatives of incurring the additional cost of retaining counsel, potentially duplicating other information security efforts, and placing leadership of certain information security efforts in the hands of lawyers rather than technologists. At the same time, the relative difficulty of protecting CI created at the pre-breach stage and the still uncertain scope of privilege and work-product protection for even post-breach CI arguably should incentivize robust and proactive security efforts to

[153] For example, often there is a misperception that engaging in a security assessment will be futile at best because it will be too expensive to meaningfully address any security gaps and counterproductive at worst because the assessment itself will provide damaging evidence in potential future litigation. Likewise, some regulators have reported incidents where there is reason to believe that an entity involved in a breach has taken steps to actively avoid documenting the results of a forensic investigation specifically to avoid creating potentially damaging CI.

avoid the heightened risk of liability and minimize the negative effects of disclosure. However, the potential discoverability of CI may discourage companies from conducting assessments of their security posture over and above those that are legally required, and it is arguably unfair for any *legally required* assessments to be used against the company in a litigation or regulatory setting, as is the case in the current regime.

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

Civil regulators and plaintiffs present still different issues. These parties seek to enforce the law against data holders and therefore are both interested in CI and more likely to have requests for CI rebuffed. Companies, however, may have strategic incentives to disclose otherwise protected CI to regulators in the course of an investigation—for instance, in hopes that their cooperation will bring about a lighter sanction.[154] In addition, through pre-lawsuit subpoenas, civil regulators have tools at their disposal to seek CI that are not available to private plaintiffs. Nonetheless, the possibility that a private civil action will accompany an investigation, and the clear risk that disclosure in a regulatory investigation likely will waive privilege and work-product protection, combine to create significant incentives for data holders to resist disclosure of CI to regulators as much as possible.

Private plaintiffs lack the pre-litigation tools of civil regulators in seeking disclosure of CI. Such plaintiffs must frequently overcome efforts to demonstrate they lack standing or have failed to state a claim before they can even hope to obtain CI, an issue that is rarely disputed in regulatory contests. As the discussion in Part C explains, if defendants carefully structure post-incident analyses of security incidents, in particular by retaining counsel to direct those processes, they should be able to protect from disclosure much of the CI generated by those post-incident activities. On the flip side, the few decisions analyzing application of attorney-client privilege and work-product protection in this

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

context suggest that courts will carefully distinguish between documents that are intended to assist in providing legal advice and/or preparing for litigation and those that are created for strategic and business purposes. Moreover, most pre-incident documents will be difficult to protect from disclosure, thus giving access to a potentially large amount of CI.

e. The Unique Importance of Cybersecurity and Cybercrime

American businesses and government agencies are under cyberattack twenty-four hours a day, seven days a week from criminal third parties, and the federal government has declared this global cybercrime wave a compelling national security concern, particularly in the area of critical infrastructure. In this context, any regime regarding the discoverability of CI that creates disincentives for companies to engage in behavior that could enhance their network security, or interferes with law enforcement's efforts to catch the third-party criminals, arguably poses particularly significant threats to the national economy and public safety. Under this line of argument, broader protections regarding the discoverability of CI are warranted in the cybersecurity context. At the same time, it is arguably more important in the cybersecurity context than in other public protection contexts for regulators and private litigants to be able to obtain information about companies' documents and communications so that laws governing cybersecurity can be enforced and companies have appropriate incentives to enhance the security of their networks. Under this line of argument, while the current regime's limited protections on the discoverability of a company's documents and communications might be acceptable in the context of enforcing laws as to the physical safety of consumer products, the cleanliness of the environment, and other potential dangers to public health and safety, those limits are not acceptable in the more important context of protecting the public against the economic and intangible (e.g., emotional) injuries people may incur from the misuse of their personal information.

The unique importance of cybersecurity and cybercrime has led some to suggest that the current regime's limited protections, by means of the attorney-client privilege and work-product protection, on the discoverability of a company's documents, while acceptable in some other contexts, should either be broadened or narrowed in the cybersecurity context. In the section that follows, we assess some of the reform proposals that have been advanced for changing the current regime to account for the unique importance of cybersecurity and cybercrime.

2. Reform Proposals

As discussed above, the current regime for determining the discoverability of CI makes the creation of CI more expensive for those who seek to ensure it will be protected from disclosure, and chills companies from creating the sort of CI that would be most efficacious in furthering their cybersecurity efforts. At the same time, in many cases this model puts the creation of such documents in the wrong hands—attorneys know a lot about cybersecurity law, but perhaps not as much about other aspects of cybersecurity. In addition, even where it would be beneficial for law enforcement to view some CI, the current regime makes such disclosure less likely by increasing a data holder's liability exposure when it decides to disclose such information. These disadvantages may pose a greater threat to the public in the cybersecurity context than in other contexts because of the particularly

compelling national interests in protecting the networks of American businesses and government agencies, catching cybercriminals, enforcing cybersecurity laws, and thereby protecting members of the public against injuries from the misuse of their personal information. All of these considerations warrant at least some consideration of whether an alternate regime should potentially govern the discoverability of CI.

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

a. Absolute Stand-Alone Cybersecurity Privilege Rejected

The unique issues that data breaches raise have led some to call for an independent, unqualified cybersecurity privilege as to at least some CI. The basic premise is that cybersecurity investigations raise a similar set of concerns and require the same kind of confidential relationship that privileges in other contexts protect, such as attorney-client, therapist-patient, and others. As discussed below, the unique mix of interests implicated by the increasing and pervasive risk of a data breach provide several persuasive arguments in favor of recognizing a new privilege in this area. But the conflicting nature of the relevant interests also provides counterarguments in favor of the status quo. At minimum, these conflicting interests counsel against making such a privilege unqualified and instead support careful calibration, including significant qualifications permitting disclosure of some otherwise protected CI under the right circumstances.[155]

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

[155] *See, e.g.*, Jeff Kosseff, *The Cybersecurity Privilege*, 12:2 I/S J.L. & POL'Y FOR INFO. SOC'Y 641 (2016). Koseff develops the most extended argument in favor of an independent privilege for cybersecurity investigations. He proposes that courts should recognize a broad, unqualified privilege for all legal cybersecurity activities under Federal Rule of Evidence 502 or that Congress and state legislatures should do so through statute. *Id.* at 298–303.

pelling case for a new privilege that closely tracks the justifications for, and hence the unqualified nature of, other common-law privileges, including the attorney-client privilege.[156]

As an initial matter, the case for an unqualified cybersecurity privilege is premised on the contestable assumption that the risk of disclosure in litigation creates disincentives for entities to develop robust and effective cybersecurity policies and practices. The counter argument assumes the precise opposite: organizations are more likely to expend sufficient resources and take pro-active measures to prevent data breaches because their security planning and implementation processes will be closely scrutinized in litigation if they suffer a breach. Which assumption is correct ultimately is an empirical question, the answer to which almost certainly will shift over time and likely depends on the relative maturity of an organization's cybersecurity posture.

Equally important, an unqualified cybersecurity privilege would take no account of the offsetting policy considerations just identified, including the data owner's interest in recourse for an entity's failure to take legally required security measures, and the risk that a lack of transparency would substantially frustrate the ability of regulators to enforce existing privacy and cybersecurity laws. For these reasons, any realistic proposal for a stand-alone cybersecurity privilege should almost certainly include qualifications on the privilege, including some restrictions on the CI that could qualify for the privilege, as well as some qualification that would permit opposing parties to obtain protected information under certain circumstances.

b. Proposed Qualified Stand-Alone Cybersecurity Privilege

Any stand-alone cybersecurity privilege should include the following features and qualifications:

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

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

---

[156] *Id.*

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

Having said that, a qualified stand-alone privilege that extended to *all* documents and tangible things prepared in anticipation of or in response to a cyberattack would potentially create a presumptive protection from discovery for any and every document concerning a company's cybersecurity efforts. This would include ordinary-course documents such as computer-generated logs and the results of automated vulnerability and anti-virus scans that do not in and of themselves disclose or reflect the *human* analyses, evaluations, and decisions that the current regime arguably chills and/or weakens. Addressing the concerns created by the current regime does not necessitate affording such ordinary-course documents enhanced protection against discovery. Rather, those concerns can be addressed by limiting any such enhanced protection to documents and tangible things that reflect a person's (or its representative's) mental impressions, conclusions, opinions, assessments, evaluations, or theories concerning a cyberattack on that person, or the person's actual or potential actions in anticipation of or response to a cyberattack—in much the same way that Federal Rule 26(b)(3)(B) affords enhanced work-product protection to documents reflecting such mental impressions and the like.

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

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

(2) the person seeking production shows it has substantial need for the materials and cannot, without undue hardship, obtain their substantial equivalent by other means.

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

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

(1) expressly make the claim; and

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

(D) Definitions

(1) "Cybersecurity threat" has the meaning given the term in section 102(5) of the Cybersecurity Information Sharing Act of 2015 (CISA), including the definition of the related term "information system," given in section 102(9) of CISA.[157]

---

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

Section 102 (5) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term "cybersecurity threat" means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Section 102(9) INFORMATION SYSTEM.—The term "information system"—

Any stand-alone cybersecurity privilege modeled on the work-product doctrine need not, in our view, include a more liberal undue-burden/substantial-need exception than the work-product doctrine's version of that exception. To begin with, much of the CI generated by a company will not fall within the above draft rule's limited presumptive protection against disclosure in the first place because it will not disclose a person's mental impressions and the like, and thus will not satisfy the requirements of Paragraph B of the proposed rule. Moreover, while we recognize that some kinds of CI within the draft rule's presumptive protection against disclosure will be essential and difficult to replicate through other evidence, the recent discussion of the undue-burden/substantial-need exception in the *Experian* case illustrates how the equivalent exception under our proposed rule can enable plaintiffs to obtain such CI when necessary.[158] There, the court denied plaintiffs access to the forensic report created by the defendants' outside expert *only* because it recognized that the plaintiffs could readily replicate the report themselves, since the report relied solely on server images that the plaintiffs could obtain in discovery.[159] By contrast, under both the work-product doctrine and the proposed qualified stand-alone cybersecurity privilege, where an organization generates materials that otherwise would be protected by the doctrine/privilege, but an opposing party has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain a substantial equivalent by other means, the party generating the materials could be required to provide that information to the opposing party.

In addition to providing a balanced alternative to an unqualified stand-alone cybersecurity privilege, a qualified stand-alone cybersecurity privilege modeled on the work-product doctrine could result in parties more selectively asserting the blanket protection of attorney-client privilege to pre- and post-breach CI and would provide courts with a more nuanced set of tools to deal with competing arguments over the application of privilege in the cybersecurity context.

Having said all that, while a qualified stand-alone cybersecurity privilege would provide more limited protection than an unqualified privilege modeled on traditional attorney-client privilege principles, and thereby better address the mix of interests implicated in the cybersecurity context, such a privilege would still protect a much greater range of CI from disclosure than does the current regime. The argument in favor of a qualified standalone cybersecurity privilege thus still rests on the contestable proposition that some currently unprotected CI really should be protected, even though it does not qualify for the attorney-client privilege or work-product protection. Ultimately, then, the argument for even a qualified stand-alone cybersecurity privilege depends on whether concerns about cybersecurity and cybercrime are both unique and substantial enough to justify drawing the protec-

---

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

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

[159] *Id.* at 5.

tion/non-protection line differently in the cybersecurity and CI context than where the current regime draws that line in all other contexts.

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

The narrow limitations the proposed privilege would impose on the discoverability of relevant CI in such cases are outweighed by the benefits the privilege would achieve. First, the proposed qualified privilege would enable parties to take robust actions to protect themselves against and respond to third-party cyberattacks with greater (though not absolute) assurance that the CI they generate in the course of those efforts will not be used against them at some point down the road. In our view, affording parties such greater assurance treats the victims of third-party cyberattacks more fairly than does the current regime.

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

In this way, the proposed qualified privilege is analogous to the medical peer-review privilege recognized by the vast majority of U.S. states (although generally not by federal common law), which lessens hospitals and physicians' disincentives to thoroughly investigate medical incidents by shielding reports and other documents of their medical staff committees in connection with such investigations from discovery.[160] We recognize that in *University of Pennsylvania v. EEOC*, the U.S. Supreme Court declined to recognize a qualified common-law privilege against the disclosure of confidential university faculty peer-review materials.[161] We also recognize that several lower federal courts have relied on the Court's reasoning in that decision to refuse to recognize an analogous "self-critical analysis" or "self-evaluative" privilege that would protect confidential, nonfactual deliberative mate-

[160] *See* Leonard et al., The New Wigmore: A Treatise on Evidence § 7.8 (3d ed. 2017).

[161] 493 U.S. 182 (1990).

rial such as opinions or recommendations that result from internal investigations, reviews, or audits conducted by public and private entities.[162]

The limited privilege we propose stands on much different footing than either the faculty peer-review process or the self-critical analysis privilege. The Supreme Court in *University of Pennsylvania* noted that confidentiality is not the norm in all faculty peer-review systems and expressed skepticism that disclosure of faculty peer reviews would actually have a chilling effect on the candidness of such reviews.[163] By contrast, corporations closely safeguard the confidentiality of their candid assessments of their own information security. As noted above, the current regime incentivizes companies to maintain that confidentiality by putting attorneys in charge of their efforts to address being victimized by cyberattacks and/or taking other measures to avoid creating a discoverable record concerning those efforts, thereby raising the risk that those efforts will be less efficacious and/or more costly than they would otherwise have been.

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

Second, we propose that this qualified privilege be established through legislation at the federal and state level, rather than through common law. Courts understandably are reluctant to recognize new common-law privileges and generally cite the high burden for such recognition when rejecting the self-critical analysis privilege.[164] Establishing the privilege through legislation removes those concerns. While it is no simple task to pass legislation, there is growing bipartisan consensus that cybersecurity is a critical national priority that requires new and creative approaches.[165]

---

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

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

[164] *See Lund,* 2017 WL 5891186, at *5.

[165] States in particular have been very active in seeking to address these issues. Through Nov. 6, 2018, at least 22 states had passed 52 cybersecurity-related bills, and at least 35 states, D.C. and Puerto Rico introduced/considered more than 265 bills or resolutions related to cybersecurity. *See Cybersecurity Legislation 2018,* NATIONAL COUNCIL OF STATE

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

c. Selective Waiver for Criminal Cybersecurity Investigations

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

The arguments in favor of limiting waiver in this situation are not unique to the cybersecurity context. Others have advocated for a version of this protection, often called "selective waiver," for information shared in the course of civil regulatory investigations, and federal law provides a broad protection against privilege and work-product waiver for information shared with banking regulators.[166] Several courts have recognized selective waiver on the basis that it encourages companies to fully investigate potential illegal conduct and to cooperate with regulatory agencies, thus protecting shareholders, customers, and the public.[167]

The majority of courts that have addressed whether to apply selective waiver in civil regulatory investigations, however, have not found either "the rationale of encouraging corporations to seek outside review of allegedly illegal corporate activities, nor that of encouraging them to cooperate with [regulatory] investigations" sufficient to justify the doctrine.[168] Courts that reject the doctrine note that organizations have ample incentive to seek candid advice from legal counsel regardless of whether a government regulator may require it to disclose that advice in an investigation. Moreover,

---

LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx. (last visited Jan. 17, 2019).

166 2 PAUL R. RICE, ET AL., ATTORNEY-CLIENT PRIVILEGE IN THE U.S., LIMITED WAIVER—LOGIC OF LIMITED WAIVER § 9:91 (2018).

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

168 RICE, *supra* note 166.

the benefits an organization obtains from voluntary disclosure, in the form of more lenient sanctions resulting from an investigation, in most cases is sufficient incentive for cooperation with the regulator and not likely to be undermined by the risk of waiver of privilege or work-product protection.[169]

The case for selective waiver for disclosures in the course of a law enforcement investigation into a cybersecurity incident is arguably stronger than for civil regulatory investigations. The public's interest in obtaining complete information following a cybersecurity incident extends beyond ensuring full disclosure of potential legal violations to identifying information regarding potential cyber threats and actors that could help prevent those threats from affecting other organizations, individuals, and data. Compromises of the confidentiality, integrity, or availability of information or systems frequently results from criminal conduct by a third party. Permitting the affected entity to fully disclose information regarding a potential breach to law enforcement authorities without risk of waiving attorney-client privilege or work-product protection in a subsequent civil law suit or regulatory investigation would likely encourage such disclosures. This, in turn, could assist law enforcement in apprehending the criminal actors involved in the incident, thereby preventing that actor from similarly attacking other organizations.[170]

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

---

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

[170] Our collective experience suggests that many organizations either do not engage law enforcement or delay engagement following a data breach for a range of reasons, including concerns about waiver of attorney-client privilege and work-product protection. Our shared intuition is that while that reluctance in most instances is not driven primarily by waiver concerns, eliminating those concerns likely will encourage at least timelier, and possibly greater overall, cooperation and information sharing. Informal discussions with several federal law enforcement personnel actively involved in cybercrime matters confirmed that, in their experience, organizations often are reluctant to share information with law enforcement, and that legal liability concerns, including potential waiver of attorney-client privilege, frequently cause delays in the ability of law enforcement to obtain information.

i. Statutory Models

A statute providing selective waiver of privilege and work-product protection for information disclosed to criminal law enforcement could draw on waiver protections that exist in other contexts. Congress has created statutory limits on the waiver of the attorney-client privilege in two contexts: (1) a broad protection against waiver as to submissions made to banking regulators, and (2) as discussed in part C above, a protection against waiver for specific information shared through the processes prescribed by CISA.[171]

(a) Bank Examiner Waiver Protection

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

> (x) Privileges not affected by disclosure to banking agency or supervisor
>
> (1) In general
>
> The submission by any person of any information to the Bureau of Consumer Financial Protection, any Federal banking agency, State bank supervisor, or foreign banking authority for any purpose in the course of any supervisory or regulatory process of such Bureau, agency, supervisor, or authority shall not be construed as waiving, destroying, or otherwise affecting any privilege such person may claim with respect to such information under Federal or State law as to any person or entity other than such Bureau, agency, supervisor, or authority.[172]

Very few courts have interpreted this provision, and it lacks any significant legislative history. The text leaves open several important questions, including whether the bank examiner can waive an entity's privilege by disclosing the privileged material provided to it and how broadly to interpret "submission[s]," including whether material provided to a regulator during an enforcement action should be treated the same as submissions of more routine information.

Notably, bank regulators take the position that the bank-examiner regime does not merely permit, but requires, banks to disclose privileged information when requested by the regulator, given the compelling public interest in ensuring compliance with banking regulations.[173]

---

[171] Consolidated Appropriations Act, 2016, H.R. 2029, Pub.L. 114–113, Division N, Title I (2015).

[172] 12 U.S.C. § 1828(x).

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

(b) CISA Waiver Protection

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

> Section 1504(d)(1) Information Shared With Or Provided To The Federal Government:
>
> > (1) No waiver of privilege or protection. The provision of cyber threat indicators and defensive measures to the Federal Government under this subchapter shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.[174]

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

ii. Statutory Selective Waiver Proposal and Explanation

We are persuaded that concerns about cybersecurity and cybercrime are sufficient to justify adoption of a "selective waiver" rule in the cybersecurity context that would apply to disclosures made by a cyberattack victim to the criminal law enforcement authorities investigating the attack. A key foundation for this conclusion is our belief that such disclosures do not significantly undermine the policy rationale for finding a waiver of the attorney-client privilege and/or work-product protection in certain circumstances where the privileged/protected material in question is disclosed to a third party. Specifically, a frequently cited reason for such third-party disclosures being deemed to waive the privilege/protection to which the disclosed information otherwise would have been entitled is that the party making the disclosure usually has a self-interested motive in doing so—the self-interest usually being that the disclosing party believes the disclosure will advance its position in the proceeding in which the disclosure is being made.[175] In that circumstance, it is not perceived as "unfair" to find that the disclosure waived the privilege/protection both as to the recipient of the information

---

[174] 6 U.S.C. § 1504.

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

and as to other third parties; and both as to the disclosed information and other related information that otherwise would have qualified for the privilege/protection.[176] As the saying goes, finding a waiver of the privilege/protection in that circumstance is necessary to prevent the disclosing party from using the privilege/protection "both as a sword and a shield."[177] Whatever merit that policy rationale may have in the usual context of a self-interested disclosure of attorney-client privileged or work-product protected material, we do not see such a disclosure as being fairly thought of as "self-interested" when it is made by the victim of a criminal cyberattack to criminal law enforcement authorities investigating that attack, even though the victim may receive some incidental benefits from the disclosure—such as being viewed slightly more favorably by regulators and the public, and/or receiving information from law enforcement to assist the victim's investigation and remediation efforts that the victim otherwise might not have received if it had not cooperated. As a result, we do not see that policy rationale as being significantly undermined by adoption of a "selective waiver" rule in that circumstance. This same rationale does not exist for disclosure in regulatory investigations, where the disclosing party is waiving the privilege specifically to protect its interests.

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

Based on the above thinking, we conclude that whatever limitations such a selective waiver rule would impose on the discoverability of relevant CI in the cybersecurity context are outweighed by the benefits that such a rule would achieve. And we see those benefits as being substantial. Adoption of a selective waiver rule that would apply to disclosures made by a cyberattack victim to criminal law enforcement authorities investigating the attack would result in authorities receiving a greater flow of CI regarding the attack than is currently the case. Moreover, because the CI included in the

---

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

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

increased flow is highly likely to provide detailed insights into the cybersecurity measures the attacked entity had in place, the vulnerabilities in those measures that the attacker exploited, and the data the attacker succeeded in compromising by means of those vulnerabilities, the CI could provide substantial assistance to law enforcement in bringing the perpetrators to justice. Accordingly, we are persuaded that the benefits of a selective waiver rule of this sort are sufficient to justify its adoption, given that such a rule would not in our view impose undue hardship on regulators and private litigants in building and bringing cases against the victims of cyberattacks or provide those victims with any unfair advantage in defending those cases.

We therefore propose adoption of a selective waiver rule in the cybersecurity context containing the following language:

> *Selective waiver for information shared with law enforcement*—The submission by any person of any information to a law enforcement agency for any purpose in connection with a potential or existing criminal investigation or proceeding by the agency regarding the potential or actual unauthorized access, or attempted unauthorized access, to computerized data or systems shall not constitute a waiver of any applicable privilege or protection provided by law or otherwise affect any privilege or protection such person may claim with respect to such information under Federal or State law as to any person or entity.
>
> > "Law enforcement agency" means any government agency that has authority to investigate or prosecute a crime regarding the potential or actual unauthorized access, or attempted unauthorized access, to computerized data or systems.

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

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

What incidents are covered. The operative language describing the incidents covered ("regarding the potential or actual unauthorized access, or attempted unauthorized access, to computerized data or systems") is adapted from similar language in the Computer Fraud and Abuse Act (CFAA).[178] We

[178] 18 U.S.C. § 1030 ((a) Whoever—(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— . . .).

looked to the CFAA as a model for defining the relevant criminal conduct related to data access that would trigger the waiver protection but updated the CFAA's somewhat dated reference to "computers."

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

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

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

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

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

seeking to address their perceived concerns with disclosing or not disclosing otherwise protected CI to the government. A mandatory disclosure regime would focus on the needs of government, seeking to address its perceived concerns with enforcing the law. While the rationale for waiver protection arguably could support mandatory disclosure, doing so would transform a protection intended to create incentives to voluntarily share information with law enforcement into a powerful tool for demanding cooperation in circumstances where there otherwise is neither a legal requirement nor a strong incentive to do so.[179] Our proposed rule, accordingly, is limited to disclosure in connection with a potential or existing criminal investigation and is designed to encourage greater and more timely sharing of information with law enforcement agencies.

Confidentiality agreement with law enforcement. A hallmark of attorney-client privileged or work-product protected documents is that they are developed confidentially and shared as narrowly as possible. One issue sometimes raised in the court decisions discussing the selective-waiver doctrine is whether the doctrine requires that the disclosing party enter into a confidentiality agreement with a regulatory agency to effectively prevent waiver and, if so, what form that agreement should take.[180] Our proposed rule clearly establishes that disclosure to law enforcement in connection with an existing or potential criminal investigation of a potential cybersecurity breach does not waive privilege or work-product protection and therefore no additional measure, including entering into a confidentiality agreement, is necessary to prevent waiver.

E. CONCLUSION

Through the examination of how courts have and presumably will apply traditional attorney-client privilege and work-product protection law to CI, the *Commentary* discusses whether such application will incentivize and protect CI in accordance with the policy considerations accompanying the cybersecurity context. The *Commentary*'s consideration of various proposals explores the tradeoffs between the current regime and a modified one and arrives at suggesting two proposals that would remedy what appear to be issues with the current regime's incentives. As discussed above, a qualified stand-alone privilege could help address the current regime's chilling effect on conducting frank and pointed analyses of (or even undertaking) various cybersecurity measures. Second, because of the significant hazards—including the risk of waiver— for data holders in sharing CI with law enforcement, as well as the public interest in prompt and complete knowledge about cybersecurity incidents, the *Commentary* proposes that state and federal law recognize a "selective waiver" doctrine

---

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

[180] *See*, *e.g.*, *In re* Mutual Funds Inv. Litig., 251 F.R.D. 185 (D. Md. 2008) (discussing *In re* Doe, 662 F.2d 1073 (4th Cir. 1981) and noting that the Fourth Circuit in that decision "explained that waiver of work product protection may occur in circumstances where the attorney 'cannot reasonably expect to limit the future use of the otherwise protected material.'" *Id.* at 1081).

providing that disclosure of CI to law enforcement would not waive any privilege that might otherwise be claimed in future civil litigation. The *Commentary* provides a roadmap to discuss these critical issues facing the discoverability and protection of CI and to provide concrete proposals for how policymakers and courts may wish to use current or new law to align the incentives with policy goals.