Asserting and Preserving Privilege in Cyber Crises

When a data breach or security incident happens at a company, there can be significant exposure and risks to the company, including risks of litigation, regulatory investigations, reputational harm, and disruption to operations. Given these potential risks, a security incident is often a crisis that requires coordination and communication among many stakeholders, including legal counsel. It is critical to ensure that privileged and protected documents and communications maintain such privilege and protections. This white paper provides an overview of two doctrines in the United States that can protect communications with counsel and documents created during the response to a security incident: attorney-client privilege and attorney work-product protection.[1] This paper also addresses the use of the CYGNVS platform as related to privilege. It should not be viewed as an endorsement or promotion of this or any other similar platform.

A. Attorney-Client Privilege

Federal Rule of Evidence 502 defines attorney-client privilege as "the protection that applicable law provides for confidential attorney-client communications."[2] While the exact formulation of the attorney-client privilege varies by jurisdiction, it generally protects a confidential communication between attorney and client if that communication was made for the purpose of obtaining or providing legal advice to the client.[3] In diversity actions, state law determines the existence and scope of the attorney-client privilege.[4]

Attorney-client privilege applies to current corporate employees and legal counsel for the predominant purpose of the company obtaining legal advice.[5] It also generally extends to independent contractors who are the "functional equivalent" of an employee.[6] For the privilege to apply to communications with in-house counsel (as opposed to outside counsel), some courts require an additional showing that communications were made for a legal rather than business purpose.[7] The privilege can extend to

---

[1] *See* Fed. R. Evid. 501-02 (describing privilege doctrines); *see also* Fed. R. Civ. P. 26(b)(1) (setting out the "scope of discovery . . . as follows: Parties may obtain discovery regarding any *nonprivileged* matter that is relevant to any party's claim or defense and proportional to the needs of the case." (emphasis added)).

[2] Fed. R. Evid. 502(g)(1).

[3] *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 757 (D.C. Cir. 2014).

[4] *Gray v. Bicknell*, 86 F.3d 1472, 1482 (8th Cir.1996).

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

[6] *In re Bieter Co.*, 16 F.3d 929 (8th Cir. 1994).

[7] The issue of the proper scope of attorney-client privilege for communications involving both legal and non-legal advice is currently before the Supreme Court in *In re Grand Jury*, C.A. No. 21-1397.

communications involving counsel-retained experts where counsel relies on experts to provide legal advice.[8] However, the attorney-client privilege does not shield facts from discovery, even if transmitted in communications between attorney and client—only privileged communications themselves are protected.[9]

Courts have generally held that the party asserting the privilege bears the burden to show that the privilege applies, but some courts disagree on how to allocate the burden to establish whether waiver has occurred.[10] While attorney-client privilege can be waived by disclosure to a third party, exceptions exist for agents of either the client or the lawyer that facilitate communications between them, such as cloud services, and agents of the lawyer who facilitate the representation.[11] Neither of those exceptions apply, however, unless the client or attorney communicating the privileged information reasonably believes that no third parties other than the agent will learn the contents of the communication.[12] For example, reliance on cloud services for purposes of communication generally will not waive attorney-client privilege where the cloud service provider employs industry-standard security measures, because such security measures provide a basis to reasonably believe that the contents of such communications are secure from third parties.

B. Attorney Work-Product Protection

Federal Rule of Evidence 502 defines work-product protection as "the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial."[13] Courts have held that the mere fact that litigation has occurred does not justify work product immunity per se; rather, the work product

---

[8] *United States v. Kovel*, 296 F.2d 918, 922-23 (2d Cir. 1961).

[9] *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1238 (D. Or. 2017).

[10] *See, e.g.*, *In re Keeper of Records (Grand Jury Subpoena Addressed to XYZ Corp.)*, 348 F.3d 16, 22 (1st Cir. 2003) ("[T]he party who invokes the privilege bears the burden of establishing that it applies to the communications at issue and that it has not been waived."); *In re VISX, Inc.*, 18 Fed. App'x 821, 823 (Fed. Cir. 2001) ("The privilege holder . . . has the burden of convincing the district court that it has not waived the privilege."); *United States v. Jones*, 696 F.2d 1069, 1072 (4th Cir. 1982) ("The proponent must establish not only that an attorney-client relationship existed, but also that the particular communications at issue are privileged and that the privilege was not waived."); *Weil v. Inv./Indicators, Research & Mgmt., Inc.*, 647 F.2d 18, 25 (9th Cir. 1981) ("As with all evidentiary privileges, the burden of proving that the attorney-client privilege applies rests not with the party contesting the privilege, but with the party asserting it. One of the elements that the asserting party must prove is that it has not waived the privilege.") (internal citation omitted); *In re Horowitz*, 482 F.2d 72, 82 (2d Cir. 1973) (holding that proponent of privilege had not met burden of showing that documents were kept in a manner consistent with intent to maintain confidentiality); *but see, e.g.*, *Sampson v. Sch. Dist. of Lancaster*, 262 F.R.D. 469, 478 (E.D. Pa. 2008) ("As the party challenging the privileged communication, Plaintiff bears the burden of showing that Defendants waived the privilege."); *Texaco, Inc. v. La. Land & Exploration Co.*, 805 F. Supp. 385, 387 (M.D. La. 1992) ("Once a claim of privilege has been established, then the burden of proof shifts to the party seeking discovery to prove any applicable exception to the privilege.").

[11] Restatement (Third) of the Law Governing Lawyers § 70.

[12] *Id.* § 71.

[13] Fed. R. Evid. 502(g)(2).

must be prepared *because of* the prospect of litigation, and the court must determine that "the driving force behind the preparation of each requested document" in resolving the question of work product immunity.[14] If the work product would have been created in essentially similar form irrespective of the litigation, then the work product doctrine would not apply.[15] Unlike the attorney client privilege, the work product doctrine is generally governed, even in diversity cases, by federal law.[16]

The party asserting work product doctrine bears the burden of demonstrating the applicability of the doctrine, and courts generally disfavor assertions of evidentiary privileges because they shield evidence from the truth-seeking process.[17]

---

[14] *Nat. Union Fire Ins. Co. v. Murray Sheet Metal Co.*, 967 F.2d 980, 984 (4th Cir. 1992); *In re Experian Data Breach Litig.*, 2017 WL 4325583, at *1 (C.D. Cal. May 18, 2017).

[15] *RLI Ins. Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007); *In re Premera Blue Cross Customer Data Sec. Litig.*, 296 F. Supp. 3d 1230 (D. Or. 2017) (explaining that, where materials are prepared for "dual purposes", courts must view the totality of the circumstances and determine whether the document would have been created in substantially similar form but for the prospect of litigation.); *In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 2019 WL 7592343 (E.D. Va. Dec. 19, 2019) (holding that defendants failed to show forensic report would not have been completed in substantially similar form but for the prospect of litigation and granting the motion to compel.).

[16] *United Coal Cos. v. Powell Constr.*, 839 F.2d 958, 966 (3d Cir. 1988) (unlike the attorney client privilege, the work product doctrine is governed, even in diversity cases, by federal law); *Coregis Ins. Co. v. Law Offices of Carole F. Kafrissen, P.C.* 57 Fed. Appx. 58, 60 (3d Cir. 2003) (federal - not state - standard applied in determining scope of work product privilege in diversity case); *In re Powerhouse Licensing, LLC*, 441 F. 3d 467, 472 (6th Cir. 2006) ("In a diversity case, the court applies federal law to resolve work product claims and state law to resolve attorney-client claims."); *Baker v. Gen. Motors Corp.*, 209 F.3d 1051, 1053 (8th Cir. 2000) (federal courts apply state law to resolve attorney client privilege issues and federal law to resolve work product issues in diversity cases); *Frontier Ref. Inc. v. Gorman-Rupp Co.*, 136 F.3d 695, 702 n.10 (10th Cir. 1998) ("[u]nlike the attorney client privilege, the work product [doctrine] is governed, even in diversity cases, by a uniform federal standard embodied in Fed. R. Civ. P. 26(b)(3)."); *Allied Irish Banks v. Bank of America, NA.*, 240 F.R.D. 96, 105 (S.D.N.Y. 2007) ("While state law governs the question of attorney-client privilege in a diversity action, federal law governs the applicability of the work product doctrine."); *Schipp v. Gen. Motors Corp.*, 457 F. Supp. 2d 917, 923 (E.D. Ark. 2006) ("In a diversity case, the Court applies federal law to resolve work product claims."); *Bank of the West v. Valley Nat. Bank of Ariz.*, 132 F.R.D. 250 (N.D. Cal. 1990) (in diversity action, California law would govern resolution of issues arising out of plaintiff's invocation of attorney client privilege whereas work product issues would be resolved under federal law); *Nicholas v. Bituminous Cas. Corp.*, 235 F.R.D. 325, 329 n. 2 (N.D. W.Va. 2006) ("In a diversity case, federal courts apply federal law to resolve work-product privilege claims and state law to resolve attorney-client privilege claims."); *Maertin v. Armstrong World Industries, Inc.*, 172 F.R.D. 143, 147 (D.N.J. 1997) ("[T]he work product privilege is governed, even in diversity cases, by uniform federal law..."); *S.D. Warren Co. v. E. Elect. Corp.*, 201 F.R.D. 280, 281 (D. Me. 2001) (federal courts apply federal law when addressing the work product doctrine, even in diversity cases lacking any federal question); 8 Wright, Miller & Marcus, Federal Practice and Procedure: Civil 2d. § 2023 (2d ed. 1994) ("At least since the adoption of Rule 26(b)(3) in 1970, it has been clear that in federal court the question whether material is protected as work product is governed by federal law even if the case is in court solely on grounds of diversity of citizenship.").

[17] *Solis v. Food Employers Labor Relations Ass'n*, 644 F.3d 221, 232 (4th Cir. 2011); *In re Grand Jury Proceedings*, 727 F.2d 1352, 1355 (4th Cir. 1984); *RLI Ins. Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007).

C. Recent Case Law

Over the past couple years, some courts have found the work product doctrine and attorney-client privilege did not apply to forensic reports and materials prepared in the wake of a data breach, a departure from prior decisions. The seminal case was *In re Capital One Customer Data Security Breach Litigation*, E.D. Va., No. 1:19-md-02915, U.S., in which defendant Capital One Financial Corp. ("Capital One") was ordered to produce a forensic report in a lawsuit arising from Capital One's 2019 data breach. In rejecting Capital One's claim that the report was privileged under the work product doctrine, the judge agreed there was "no question" that its third party forensic vendor drafted its forensic report at a time when Capital One faced the prospect of litigation. But the court held that the report did not warrant work product privilege because it "would have been prepared in substantially similar form" in any event, even without the prospect of that litigation. In arriving at this conclusion, the court focused on the combined weight of several facts:

- Capital One had a "long-standing relationship" with its forensic vendor
- Capital One had a pre-existing scope of work ("SOW") with its forensic vendor to perform essentially the same services that were performed in preparing the subject report.
- The forensic vendor's service was considered a business-critical expense to Capital One as a financial institution, and not a legal expense at the time the vendor was paid its retainer fee.

The court acknowledged as "significant evidence" that the forensic vendor's work was performed at the direction of outside counsel and that the final report was initially delivered to outside counsel. However, it emphasized that there was no statement or supporting evidence offered by the defendant to support finding that Capital One would not have called upon the forensic vendor to perform its services and prepare a written report, as contemplated in the SOW that predated the data breach. Although the forensic vendor was not performing an ongoing investigation at the time of the breach or its subsequent discovery, the vendor was nevertheless then obligated to perform 285 hours of service for Capital One in 2019. Ultimately, the court found Capital One did not carry its burden "of showing that [the forensic vendor's] scope of work under the Letter Agreement with outside counsel was any different than the scope of work for incident response services set forth in the existing SOW and that it would not have been performed without the prospect of litigation."[18]

In a subsequent case, a federal district court questioned whether a forensic report could be subject to attorney-client privilege.[19] The defendant, who had suffered a data breach, argued that the forensic report at issue was privileged because it was prepared at the

[18] *In re Cap. One Customer Data Security Breach Litig.*, E.D. Va., No. 1:19-md-02915, U.S., at 11-12.

[19] *Wengui v. Clark Hill, PLC*, C.A. No. 19-3195 (D.D.C. Jan. 12, 2021).

direction of counsel for the sole purpose of assisting the law firm in gathering information necessary to render timely legal advice. Although courts had in the past held materials made in the course of a separate investigation track led by a defendant's legal counsel as privileged,[20] the court concluded in this case that there was insufficient evidence on record to support the defendant's two-track story. Specifically, the court flagged the absence of any sworn statement averring that a separate investigation was conducted to learn how the breach happened and facilitate an appropriate response. It further pointed in justifying its conclusion to the facts that (1) the defendant's report was shared for non-legal purposes with a broad audience including in-house leadership, the IT team, and the FBI and (2) the firm charged with performing forensic work was engaged for immediate "incident response" and began its work as the attack was thought to still be ongoing, with its report containing pages of specific remediation advice.[21]

D. How CYGNVS Is Designed to Help Protect Privilege

CYGNVS, a guided cyber crisis response platform strives to empower organizations to stay connected and in control as they prepare for and respond to any cyber crisis. The CYGNVS platform is designed to help navigate through uploading critical documents and contracts, creating a tailored response plan, and assigning tasks to team members. Through dynamic tenancy technology, the platform has controls to grant access solely to employees involved in the incident and provide access control to external parties. This will allow the organization to establish various levels of permission for each participant.

CYGNVS provides levels of control within the platform that grant distinct levels of authority for creating teams, inviting participants to rooms, and adding or removing other participants. Moreover, once in the room, each workstream can be classified as Open or Restricted. The organization can create multiple workstreams to delineate between sensitive information and content that can be shared with the entire group. When the workstream is Open, all the content in the workstream is visible to everyone in the room. Alternatively, when Restricted, each participant in the workstream is classified as an Owner, Contributor, or Viewer, further controlling each users' visibility into the content and their ability to add or edit the information. These features are designed to manage access control and to maintain privilege for both internal and external team members with an audit trail in an effort to simplify reporting to regulators, insurers and shareholders.

---

[20] *See In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522, 2015 WL 6777384, at *2-3 (D. Minn. Oct. 23, 2015).

[21] *Clark Hill*, at 12; *see also In re Rutter's Inc. Data Sec. Breach Litig.*, C.A. No. 1:20-CV-382 (N.D. Penn. July 22, 2021) (finding that the attorney work product doctrine did not apply to a forensic report prepared by Kroll because (1) the report was not prepared with an eye toward litigation and at the time of the engagement, as Rutter's was not sure a data breach had occurred (2) at depositions, Rutter's confirmed it was not anticipating litigation when contracting with Kroll or at the time Rutter's received the report, (3) the report was provided directly to Rutter's, rather than first providing it to outside counsel, and (4) Rutter's paid Kroll directly for their work.).

E. Best Practices to Protect Privilege

Accordingly, companies seeking to assert privilege over the response to security incidents and data breaches under either the attorney-client privilege or attorney work product doctrine should carefully consider how they manage incident response teams and controls around creating documents, such as forensic reports. Some examples of best practices include:

- The incident response team should be advised at the outset that the investigation will be conducted at the direction of counsel for the purpose of counsel providing legal advice in anticipation of litigation.
- All third-party service providers assisting with the response should be engaged by legal counsel through a tri-party SOW.
- Because some courts have required a showing that communications were made for a legal rather than business purpose for the privilege to apply to communications with in-house counsel, companies should consider engaging outside counsel.
- Companies should ensure that any cloud service provider or communication tools used during the incident employs industry-standard security measures to keep communications confidential and secure from third parties.
- Companies should exercise caution when using or sharing any privileged documents (even when sharing internally) to mitigate the risk of a court finding privilege was waived.

Key Contacts

Beth George is a partner at Wilson Sonsini Goodrich & Rosati. *bgeorge@wsgr.com*

Megan Kayo is a partner-elect at Wilson Sonsini Goodrich & Rosati. *mkayo@wsgr.com*

Dan Chase is an associate at Wilson Sonsini Goodrich & Rosati. *dchase@wsgr.com*

CYGNVS Inc. info@cygnvs.com (with respect to the CYGNVS platform)

About Wilson Sonsini Goodrich & Rosati

For more than 60 years, Wilson Sonsini's services and legal disciplines have focused on serving the principal challenges faced by the management and boards of directors of business enterprises. The firm is nationally recognized as a leading provider to growing and established clients seeking legal counsel to complete sophisticated corporate and technology transactions; manage governance and enterprise-scale matters; assist with intellectual property development, protection, and IP-driven transactions; represent them in contested disputes; and/or advise them on antitrust or other regulatory matters. With deep roots in Silicon Valley, Wilson Sonsini has 19 offices in technology and business hubs worldwide. For more information, please visit www.wsgr.com.

About CYGNVS Inc.

CYGNVS is a guided cyber crisis response platform purpose-built to empower organizations to be connected, confident, in control and compliant before, during and after a cyber breach. Backed by a $55 million series A round from Andreessen Horowitz, Stone Point Ventures, and EOS Venture Partners, CYGNVS Inc. is headquartered in California, with offices in Canada, India and Ireland. For more information, visit www.cygnvs.com.