The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 4 February 22, 2017

ATTORNEY-CLIENT PRIVILEGE

Protecting Attorney-Client Privilege and Attorney Work Product While Cooperating with the Government: Strategies to Minimize Risks During Cooperation (Part Two of Three)

By Eric J. Gorman and Brooke A. Winterhalter
Skadden, Arps, Slate, Meagher & Flom LLP

Following a cybersecurity breach, companies often will initiate an internal investigation, contact law enforcement, and begin to cooperate with the government. Cybersecurity internal investigations typically focus on identifying and targeting individual wrongdoers, as well as learning of and redressing any internal deficiencies. Attorneys frequently conduct these internal investigations. Thus, attorney-client privileged communications and attorney work product often arise. Guarding the privilege and work product protection, accordingly, are important objectives for investigating companies.

The privilege and, to a lesser extent, the work product doctrine generally require confidentiality. Cooperating with law enforcement, however, often necessitates disclosure. This tension between confidentiality and disclosure raises important strategic questions for companies as they set out to engage with law enforcement while simultaneously preserving their legal protections over internal investigations.

This second installment in the three-part privilege series analyzes these issues, and identifies certain steps that companies may wish to take to try to minimize the risk, and/or extent, of a waiver of the privilege or work product protection while cooperating with the government. The first installment discussed how companies can establish the attorney-client privilege and attorney work product protection in an internal investigation. The third installment will discuss strategies for shielding privileged investigation files that were shared with the government from discovery in collateral litigation involving third parties.

Negotiating an Appropriate Scope of Information-Sharing

As a first step in cooperating with the government, companies can attempt to reach agreement with the government agencies involved about what the cooperation should entail. The DOJ, among other entities, strongly encourages companies that experience a cybersecurity breach to report the incident to law enforcement. In that context, such a company is more likely to be viewed as a victim of a crime, rather than a target of a federal criminal investigation.[1] That may provide such companies more latitude to negotiate with the DOJ, FBI, and other law enforcement agencies over the appropriate scope of documents and information to be shared. As will be discussed later, it also may help establish a basis for a cooperating company to argue that attorney work product it shares with the government (if any) remains protected because of a common interest between the company and law enforcement with respect to the materials and information in question.

Nevertheless, other government agencies, such as the FTC, tend to focus their resources on enforcement actions against the companies themselves because, for instance, companies allegedly failed to adequately protect consumers' personal data. The FTC has indicated that it often asks companies for documents and information such as audits, risk assessments, and privacy policies, as well as explanations of the incident, how the company responded, and what consumer harms may result.[2] Other agencies reviewing a cybersecurity incident, such as the FCC and SEC, may make other requests relating to their respective enforcement objectives.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 4 February 22, 2017

The types of information a company may need to share in the wake of a cybersecurity breach should be discussed with the respective government agencies that become involved. That discussion should address, among other things, limitations on production and information-sharing requirements in accordance with the attorney-client privilege and attorney work product doctrine. The DOJ and SEC, for instance, disclaim any requirement that cooperating companies waive and share attorney-client privileged communications or attorney work product. Although the FTC and FCC have not published formal policies echoing these DOJ and SEC prohibitions, the FTC and FCC are nevertheless equally subject to the privilege and work product legal restrictions, which exist as a matter of law and are independent of particular agencies' statements (or silence) about not seeking waivers. Accordingly, companies that cooperate with the government in the wake of a cybersecurity incident should be able to invoke the attorney-client privilege and attorney work product legal protections when necessary.

Sticking to the Facts

In general, law enforcement entities and government agencies working with a company to investigate a cyber incident ask the company to disclose relevant facts. This reflects the policies adopted by the DOJ and SEC, which focus cooperation efforts on sharing facts, and do not require a waiver of privilege or work product protection as a condition for obtaining cooperation credit.

The distinction between facts, on the one hand, and privilege and attorney work product, on the other, has long been recognized in the law. In Upjohn Co. v. United States, for instance, the Supreme Court noted that "[t]he privilege only protects disclosure of communications; it does not protect disclosure of the underlying facts by those who communicated with the attorney. . . . A fact is one thing and a communication concerning that fact is an entirely different thing."[3]

Viewed in this light, the analysis seems simple: facts – which are all the government generally says it wants – are not privileged or protected by the work product doctrine, so disclosing facts to the government should not threaten the privilege or work product protection. Insofar as it goes, that analysis is correct. But that analysis may not go far enough in some cases.

When Complexity Confounds Sticking to the Facts

Disentwining Facts From the Investigation Process

Facts do not emerge, unbidden, from the ether. And they are not transplanted into the consciousness of government lawyers and other personnel without some intermediary. That intermediary is often a lawyer for the investigating company, or a consultant retained by the lawyer or the company. Moreover, facts that are learned, identified and transmitted to the government by lawyers for an investigating company are a product of the legal process that elicited them – which may include privileged communications with clients, as well as attorney analysis (i.e., work product).

If the facts can be readily separated from privileged communications and attorney work product, as Upjohn suggests, the basic proposition should apply that disclosing facts – which are neither privileged nor attorney work product – should not imperil the legal protections afforded to the investigating company. But in other cases, it may be more difficult to extract pure facts from the privileged communications and attorney work product that attend an investigation, and report those facts without revealing, expressly or implicitly, protected aspects of the underlying investigation process. And even apart from the investigation process itself, there may be ambiguity in "the facts," which could intrude into the privilege or work product doctrine. For instance, there could be uncertainty or a dispute about the facts; questions about the facts' significance, if any; and questions about which facts are relevant and should be disclosed. When such questions arise, the government's binary formulation of facts vs. privilege/work product may prove insufficient. Such situations may call for a variety of measures,

described later in this article, on the part of investigating companies to protect the attorney-client privilege and attorney work product.

Special Considerations Regarding Fact Work Product

In addition to facts, a government agency may request documents that companies or their counsel create, such as chronologies of events. The SEC specifically mentions chronologies as among the documents it might seek from a cooperating company. Depending on a chronology's content and the circumstances of its creation (e.g., whether it is created by counsel, or under counsel's supervision), a chronology could be considered fact work product. (The different types of work product are explained in part one of this series.)

In general, facts become fact work product when they are prepared by attorneys in a particular form.[4] Whereas the facts contained in attorney documents are not shielded by the work product doctrine, the attorney documents themselves generally are. Fact work product, as a rule, includes tangible materials prepared or collected by counsel in connection with an anticipated litigation. It can consist of items such as (among other things) handwritten notes, electronic recordings, diagrams and sketches, financial analyses, and photographs.

The DOJ and SEC are clear that, in asking cooperating companies to provide the facts, they do not request such companies to provide "non-factual or 'core' attorney-client communications or work product."[5] Framed in this way, the government's restriction seems focused on privilege and opinion work product: both agencies describe the "non-factual or core attorney work product" they expressly do not seek as "for example, an attorney's mental impressions or legal theories"[6] – in other words, what the courts categorize as opinion work product.

But the work product doctrine does not shield only opinion work product. It also protects fact work product, though with an exception that does not burden opinion work product.[7] According to Fed. R. Civ. P. 26(b)(3)(A), "[o]rdinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation," although such materials can be subject to discovery if "the 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."

Disclosure Might Lead to Waiver

Complicating matters further, certain courts have held that disclosures of attorney work product waive the protection. For example, in Westinghouse Electric Corp. v. Republic of Philippines, the Third Circuit ruled that Westinghouse's disclosure of attorney work product to the DOJ and SEC while cooperating waived the protection over the disclosed documents, thereby exposing those documents to the company's adversaries in civil litigation.[8] Other courts have held the reverse. This split, and its implications, will be discussed in Part Three of this series.

Accordingly, investigating companies should carefully consider the types of information that should be shared with the government, as well as the rewards, and risks, of sharing such information. That analysis can be challenging – especially when the information or materials at issue lie somewhere on the spectrum between the clear-cut cases posited by the government, of facts, at one end, and privilege and "core" work product, at the other.

Basic Steps to Help Avoid a Waiver While Sharing Information with the Government

In light of the above factors, there are certain steps that investigating companies may take to try to minimize risks to the privilege and work product protection as cooperation proceeds.

1) Enter Into a Confidentiality Agreement

One thing companies can do to help protect information they provide to the government – whether privileged or not – is to enter into confidentiality agreements

with the respective government agencies before making disclosures. Confidentiality agreements with the government often (1) limit the government's discretion to disclose materials produced by the company; (2) include non-waiver provisions in which the government agrees that the production of any privileged communication or attorney work product does not result in a waiver; (3) provide that the government will not assert a broader subject-matter waiver based on such disclosures; and (4) include claw-back provisions to address any inadvertent disclosures of privileged material or attorney work product.

The SEC Enforcement Manual, for example, permits the SEC to enter into confidentiality agreements which provide that:

> [T]he staff agrees not to assert that the entity has waived any privileges or attorney work-product protection as to any third party by producing the documents, and agrees not to assert that production resulted in a subject matter waiver. The staff also agrees to maintain the confidentiality of the materials, except to the extent that the staff determines that disclosure is required by law or that disclosure would be in furtherance of the SEC's discharge of its duties and responsibilities.[9]

The DOJ, FTC, and FCC have not published guidance on confidentiality agreements, but DOJ confidentiality agreements, at least, tend to mirror the approach of the SEC.

Courts are split over whether confidentiality agreements with the government are effective vis-a-vis third parties: some enforce them, while others do not. The law governing confidentiality agreements and related waiver arguments will be discussed in greater detail in Part Three of this series.

2) Share Facts Without Disclosing Protected Materials

In addition to entering into a confidentiality agreement, companies can help maintain the privilege and work product protections over their investigations by utilizing, where possible, the government's distinction between facts, on one side, and privileged communications and attorney work product, on the other. To the extent facts can be shared without revealing privileged communications or attorney work product, such an approach should present the least risk to a company's legal protections. As Upjohn notes, facts – standing alone – generally are not privileged, and they are not protected work product, so disclosing them should not threaten those protections.

Moreover, as explained further below, to the extent companies share fact work product with the government, they may want to withhold opinion work product, which is often more sensitive and is highly protected under the law.

3) Separate the Legal Investigation from the Factual Investigation

Finally, companies cooperating with law enforcement entities or government agencies during a cyber investigation may consider segregating investigations into two pieces: (1) an ordinary course of business investigation to uncover the facts; and (2) a privileged investigation led by counsel for the purpose of providing legal advice regarding potential litigation. This approach was recently used by Target Corporation in connection with a cyber incident, and the District of Minnesota ruled that Target's legal investigation was privileged. In re Target Corp. Customer Data Sec. Breach Litig., MDL No. 14-2522 (D. Minn. Oct. 23, 2015), E.C.F. No. 622 (denying motion to compel production of legal task force's documents, including documents created by forensic analysts, because task force's focus was "on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in litigation"). Of course, the potential logistical complications and expense of such dual-track investigations also should be considered, along with the need to maintain a clear wall separating the two.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 4 February 22, 2017

Additional Precautions When Sharing Privileged or Protected Materials

Companies sometimes share privileged communications and attorney work product with the government, even though the government generally disclaims any need for privilege or "core" opinion work product. Such disclosures may be either voluntary or inadvertent.

Voluntary Production

The government generally is willing to accept disclosures of privileged communications or attorney work product if a company chooses to share such materials. Under certain circumstances, companies may deem it in their interests to provide materials to the government notwithstanding legal privilege and work product protection.

Federal law encourages companies to share cybersecurity threat information, such as cyber threat indicators and defensive measures, with the federal government. To that end, the Cybersecurity Information Sharing Act of 2015 expressly protects "any applicable privilege provided by law" against waiver if privileged or work product-protected cybersecurity threat information is shared with the government.[10] Thus, if a company discloses cyber threat indicators and defensive measures to the federal government, the attorney-client privilege and attorney work product protection are not waived as a consequence of that disclosure.

Moving beyond cybersecurity threat and response information, the picture is less clear, and the risk of a waiver increases. Accordingly, before voluntarily providing other types of privileged material or attorney work product to the government, companies should (1) make certain that doing so advances an important interest that cannot be attained by sharing only the facts that the government generally says it wants; and (2) ensure that the benefit of providing such material outweighs (a) the risk that the disclosure will be deemed a waiver and (b) the consequences of more widespread disclosure if a waiver is found.

In addition to entering into a confidentiality agreement, as described above, companies that voluntarily decide to disclose privileged or protected files to the government may wish to define the precise scope of the intended waiver – e.g., the subject matter and/or dates of the privilege or work product to be waived – in a statement to or perhaps agreement with the government. This may help avoid, or at least limit, a potential future dispute with the government over the extent (and intent) of the waiver, and also may help establish a clear, defensible limit to the waiver if it is later challenged by a third party. A recent decision from the Southern District of New York illustrates the point. There, a company's voluntary waiver as to certain privileged information, which was expressly defined by the company, was held not to waive the attorney-client privilege over documents that were created after the defined waiver period or that concerned topics that were not directly related to the materials over which protection was waived.[11]

Such clarity can also help lay a foundation for later reliance, if necessary, on Rule 502(a) of the Federal Rules of Evidence. Rule 502(a) provides that in the case of disclosures to federal agencies, a "waiver extends to an undisclosed communication or information in a federal or state proceeding only if: (1) the waiver is intentional; (2) the disclosed and undisclosed communications or information concern the same subject matter; and (3) they ought in fairness to be considered together." Thus, the disclosure of one privileged or protected document to the government should not waive the privilege as to a second document unless the second document relates to the same subject matter as the first and it would be unfair to consider the first document without the second.

Extending this concept beyond disclosures to the federal government, the Southern District of New York recently declined to find a broad subject matter waiver after a

bank shared certain privileged communications with FINRA as part of a post-merger trading inquiry.[12] In that case, the bank's in-house counsel communicated with one of the bank's employees in the course of an internal review, and disclosed those communications to FINRA in response to concerns about possible insider trading. The court ruled that although the disclosure waived privilege over the communications that were shared, there was no broader subject-matter waiver because the disclosure was outside the judicial context, the bank was not a party to the underlying case and nothing in the record indicated that the disclosure was used affirmatively to prejudice either of the parties in the criminal proceeding.

The principles noted above should apply to both privileged communications and attorney work product. But work product also presents additional, unique considerations. For instance, companies that decide to share work product with the government can seek to limit such material to fact work product, as opposed to more sensitive opinion work product. Courts tend to be more protective of opinion work product, and a disclosure of only fact work product generally will not result in a waiver of related opinion work product.

Moreover, companies sharing work product can attempt to articulate a common interest with the government that may help preserve the work product protection vis-a-vis other parties. For instance, a company might be able to cite a common interest between itself and the government in seeking to identify hackers and bolster cyber defenses – the company because it wants to protect the integrity of its data and computer systems, and the government because of its interest in pursuing wrongdoers and maintaining robust communication systems and infrastructure, which are essential to American national and economic security (as the DOJ and FCC, among others, have noted). Again, however, the case law on such claimed common interests is mixed, as will be discussed further in Part Three.

Notwithstanding the range of mechanisms companies may employ to try to avoid, or at least limit the scope of, a waiver, risk remains. The courts have not developed a clear and consistent approach to questions of waiver in the context of sharing information with the government, as Part Three will explain. Accordingly, before voluntarily disclosing attorney-client privileged or work product protected materials to the government, companies should consider the possible impact if a court were to order a more general disclosure of the communication or material in question (and, possibly, related items, in the case of a subject matter waiver) to parties other than the government.

Inadvertent Production

Especially in large-scale or fast-moving productions, investigating companies might inadvertently produce privileged communications or attorney work product to the government. Such unintentional disclosures can often be remedied if appropriate measures were taken to avoid such disclosures, and a claw-back agreement is in place.

Federal Rule of Evidence 502(b) provides that an inadvertent disclosure of privileged or protected materials does not constitute a waiver if:

1. the disclosure was inadvertent;
2. the company took reasonable steps to prevent the disclosure, and
3. the company took reasonable steps to rectify the error.

To that end, companies producing materials to the government generally conduct a review for privilege and attorney work product. In designing such a review, with an eye towards its reasonableness, companies may wish to consider factors such as the size of the review and production, timing and other constraints and the availability of various technical methods to help identify and filter out privileged communications and attorney work product. In addition, marking appropriate documents as privileged or protected during the investigation may help avoid inadvertent disclosures of privileged or protected materials as the company works together with the government.

Clawback agreements can also help rectify inadvertent productions. Such provisions, which are often included in confidentiality agreements with the government, can be utilized and cited as among the reasonable steps a company takes to limit and recover inadvertent disclosures under Rule 502(b). Taken together with a well-constructed privilege and work product review that is reasonable under the circumstances, such an agreement can help limit potential damage – vis-a-vis the government and third parties – if a document is produced in error.

For more on the attorney-client privilege and work product protection during cybersecurity investigations see "*Attorney-Consultant Privilege? Key Considerations for Invoking the Kovel Doctrine (Part One of Two)*" (Nov. 16, 2016); *Part Two* (Nov. 30, 2016); *"Target Privilege Decision Delivers Guidance for Post-Data Breach Internal Investigations"* (Nov. 11, 2015); and *"Preserving Privilege Before and After a Cybersecurity Incident (Part One of Two)"* (Jun. 17, 2015); *Part Two* (Jul. 1, 2015).

Eric J. Gorman is a litigation partner based in Skadden's Chicago office.[13] *He has conducted a substantial number of corporate internal investigations and represented companies and their boards in government investigations involving the SEC and DOJ. Mr. Gorman has handled investigations in the U.S. and abroad, and has advised boards of directors and senior executive teams in connection with U.S. criminal and regulatory issues. His litigation experience also includes defending against large-scale class actions, and prosecuting and defending transaction-related litigation and other high-value claims.*

Brooke A. Winterhalter is a litigation associate based in Skadden's Chicago office.

[1] See generally, DOJ Cybersecurity Unit, Best Practices for Victim Response and Reporting of Cyber Incidents (Apr. 2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.
[2] Mark Eichorn, Assistant Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, F.T.C., If the FTC Comes to Call (May 20, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call.
[3] 449 U.S. 383, 395–96 (1981).
[4] See In re Convergent Techs. Second Half 1984 Sec. Litig., 122 F.R.D. 555, 558 (N.D. Cal. 1988).
[5] SEC Enforcement Manual § 4.3; U.S. Attorney's Manual § 9-28.710.
[6] U.S. Attorney's Manual § 9-28.720; SEC Enforcement Manual § 4.3.
[7] See Fed. R. Civ. P. 26(b)(3)(A).
[8] 951 F.2d 1414, 1429–30 (3d Cir. 1991).
[9] SEC Enforcement Manual § 4.3.1.
[10] 6 U.S.C. §§ 1504(d)(1). The Act also protects against waiver of intellectual property rights in cybersecurity threat information and defensive measures that are shared.
[11] United States v. Mount Sinai Hosp., 185 F. Supp. 3d 383, 390-93 (S.D.N.Y. 2016).
[12] Memorandum Order, United States v. Stewart, No. 15-cr-00287 (S.D.N.Y. July 22, 2016) E.C.F. No. 141.
[13] This article contains the views of the authors, and does not necessarily represent the views of Skadden, Arps or any one or more of its clients.