The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 3 February 8, 2017

ATTORNEY-CLIENT PRIVILEGE

Protecting Attorney-Client Privilege and Attorney Work Product While Cooperating With the Government: Establishing Privilege and Work Product in an Investigation (Part One of Three)

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

Companies that experience a cybersecurity incident often cooperate with law enforcement, and simultaneously conduct internal investigations to learn what happened and strengthen defenses against potential future attacks. These internal investigations are often conducted by attorneys, which means that attorney-client privileged communications and attorney work product frequently arise. Guarding the privilege and work product protection, accordingly, are often important objectives for such companies. The privilege and, to a lesser extent, the work product doctrine generally require confidentiality; however, cooperating with law enforcement often necessitates disclosure. This conundrum can be confounding.

This three-part series examines the interplay between the attorney-client privilege and attorney work product protection, on the one hand, and cooperation with the government on the other. This first article in the series addresses how and when the attorney-client privilege and attorney work product protection are created during internal investigations, and steps that can be taken to establish and maintain those protections. The second article will analyze what investigation materials can be shared with the government without implicating the privilege or attorney work product protection, and what steps can be taken to help protect privileged materials and attorney work product if they are shared, intentionally or otherwise, with the government. The third article will provide an overview of when and how privileged or protected investigation materials that have been shared with the government can be protected from discovery in collateral litigation.

See also *"Attorney-Consultant Privilege? Key Considerations for Invoking the Kovel Doctrine (Part One of Two)"* (Nov. 16, 2016); *Part Two* (Nov. 30, 2016).

Government Reporting and Cooperation Policies

To understand the privilege and work product protections in the context of internal investigations, it helps to start with the regulatory environment. The government in general offers incentives to parties that report cybersecurity incidents and cooperate with law enforcement efforts. For example, certain government bodies, including state governments, require disclosures related to data breaches and other cybersecurity incidents.

When a cybersecurity incident occurs, a company may make disclosures to one government entity for reporting and remediation purposes (such as the DOJ), while also facing a potential enforcement action from another (such as the FTC, the SEC or a state attorney general). The government values cooperation in both contexts. Cooperation credit can include, among other things, avoidance or deferral of enforcement actions, and reduced charges and sanctions.

Cooperation entails a number of things. The FTC, for instance, considers whether a company reported a breach to the appropriate law enforcement agencies, and cooperated with them to reduce the harm from the breach.[1] The SEC, for its part, states in the SEC Enforcement Manual that cooperation includes providing the government with all information relevant to the potential underlying violations, as well as the company's remedial efforts. Information a party is required to provide while cooperating thus could include, inter alia, (1) summaries or explanations of particular transactions, fact patterns and issues; (2) summaries of witness statements and answers; and (3) original source documents relating to the conduct at issue.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 3 February 8, 2017

Notably absent from the list of what the government expects, however, is a waiver of the attorney-client privilege or attorney work product protection. The government's stated rule of not requiring a waiver charts the beginning of a course for cooperating parties to follow as they engage with the government, while still maintaining the attorney-client privilege and attorney work product protection. Following that course, however, can at times require significant nuance. For example, there may be questions about whether a communication or document is in fact protected – e.g., because of ambiguities or disputes about the provenance or nature of the document or communication. Indeed, when a claim of privilege or work product protection is more gray than black or white, the practical issues of how to cooperate with the government while still maintaining the privilege or protection (to the extent they apply) can be challenging.

The Attorney-Client Privilege and Work Product Protection in Internal Investigations

To establish and guard the attorney-client privilege and attorney work product doctrine in an internal investigation, it is important first to understand what communications and materials are covered. In general, once a company decides to investigate a potential matter and engage counsel, counsel will begin to gather relevant source documents (some of which may be privileged) and to create documents such as summaries and analyses (many of which may be protected by the privilege or attorney work product doctrine, provided the company takes the necessary steps to obtain such protections).

Attorney-Client Privilege

In general, the attorney-client privilege applies to confidential communications between the company and its attorneys in connection with seeking or providing legal advice. Legal advice lies at the heart of the attorney-client privilege. As a rule, communications or documents that convey or describe legal advice or that request or provide information, such as factual background, necessary to render legal advice are protected by the attorney-client privilege. By contrast, communications – even between an attorney and client – that do not convey or contribute to the provision of legal advice are unlikely to be privileged. Moreover, the attorney-client privilege typically does not protect the facts at issue in an investigation, although it often will protect communications with counsel about those facts.

Privileged investigation materials may include, among other things, confidential communications with attorneys regarding the facts, circumstances and nature of an incident; confidential interviews with company employees (subject to Upjohn procedures, described further below); and confidential communications with experts, such as cybersecurity firms, that are retained to assist investigating counsel.

A related concern is which entity owns and controls the privilege – i.e., which entity is the client of the investigating attorney. In a cybersecurity investigation, the client might be the company, or the board of directors, or a committee of the board, or some other entity. Clearly understanding which entity is the client, and if possible documenting it (for instance, in an engagement letter), can help individuals working on an investigation delineate and maintain the necessary boundaries required by the privilege. But just as important is the converse: which people and entities are not the client. Carelessness about who is inside and outside the scope of privilege can quickly result in a waiver.

Attorney Work Product Doctrine

The attorney work product doctrine protects documents and other materials prepared in anticipation of litigation by the company or its representatives, including attorneys and consultants. Various courts have held that an internal investigation conducted in anticipation of a government

enforcement action satisfies the "in anticipation of litigation" requirement. Thus, many files created during an internal investigation by counsel, or at counsel's direction, are likely to constitute work product.

Attorney work product is divided into two categories: opinion work product and fact work product. Opinion work product consists of materials reflecting an attorney's mental impressions, opinions and strategies, and is subject to a high level of protection.[2] Fact work product includes materials such as an attorney's compilation of facts learned during an internal investigation and is also protected by the work product doctrine, although this protection is subject to certain exceptions that do not apply to opinion work product.[3]

Whether an attorney's work product constitutes fact or opinion depends on its content and requires a document-specific analysis. In *United States v. Clemens*, for example, the district court in Washington, D.C. considered witness interview memoranda created during an investigation and ruled that the nature of work product turns on whether it contains either (1) relevant and non-privileged facts, such as statements that could properly be called a witness's own words; or (2) an attorney's mental impressions, conclusions, opinions or legal theories – statements that are attributable to the attorney, rather than a witness.[4]

Seen through that lens, interview memoranda generally constitute opinion work product when the questions are prepared by an attorney and the memoranda contain the attorney's mental impressions from the interview. However, interview memoranda that reflect mere transcripts of an interview and are reviewed and signed by the witness are more likely to be deemed fact work product.

Establishing the Privilege and Work Product Protection in Internal Investigations

Engage Counsel

To ensure the attorney-client privilege and attorney work product protection apply to the maximum extent possible, investigating companies should consider engaging counsel early in the investigation process – ideally, at the point of determining whether to investigate. Indeed, it may be important for an investigating company to protect deliberations about whether, and how, to investigate; such protections may not be readily available if the deliberations do not involve legal counsel and legal advice. By ensuring that attorneys at least guide and oversee, and if possible conduct, the investigation, companies can maximize the privilege and work product protections available under the law.

To that end, the company and its counsel can memorialize that legal advice and representation is being sought and provided, including by documenting this point in an engagement letter if outside counsel is involved. But, as noted above, the privilege only attaches to communications that convey legal advice; if the lawyer is engaged in a non-legal activity, such as providing business advice without a legal component, then such advice may not be deemed privileged.

For more on establishing privilege and work product in a cybersecurity investigation see also *"Preserving Privilege Before and After a Cybersecurity Incident (Part One of Two)"* (Jun. 17, 2015); *Part Two* (Jul. 1, 2015).

In-House Counsel; Non-U.S. Jurisdictions

In the U.S., both in-house and external counsel may be the "attorney" for purposes of the attorney-client privilege and attorney work product protection. Certain other countries, however, appear to limit the availability of these protections to outside, as opposed to in-house, counsel. Still other countries do not appear to recognize the attorney-client privilege or work product protection at all. Questions regarding the applicability of the

attorney-client privilege and work product doctrine in foreign countries are jurisdiction-specific and should be evaluated by locally-licensed attorneys.

Non-Attorney Investigators

To the extent non-legal professionals, such as cybersecurity consultants or other specialists, are needed to conduct a thorough investigation, the privilege and work product protection can in certain circumstances be extended to cover them. It can be helpful (though not necessarily required) in extending the privilege and work product protection to such non-legal professionals if investigating counsel, rather than the company itself, engages them.[5] Such professionals are often directed by counsel, and at a minimum should coordinate closely with counsel, to remain within the privilege and work product protection.

See *"Target Privilege Decision Delivers Guidance for Post-Data Breach Internal Investigations"* (Nov. 11, 2015).

Conversely, non-lawyers – such as IT specialists, business people, compliance professionals, human resources personnel, and others – who undertake an investigation without the involvement and advice of legal counsel generally will have fewer, and weaker, grounds to protect their processes, deliberations, and findings. Such a situation can arise when, for example, IT, compliance, or human resources personnel identify a potential issue in the course of their work and try to assess it. The need for legal advice and involvement in this scenario may not be immediately apparent, especially to a non-lawyer, but if a company neglects to involve legal counsel early on then its investigation work could later be deemed outside the scope of the privilege and work product protection. Privilege and work product shield legal advice and legal strategy. If attorneys are engaged later, they might be able to argue retroactively to apply the privilege and work product doctrine to the earlier work of the non-lawyers, but such an argument could be challenging. As such, scenarios like this can present risks that could be avoided by simply engaging and involving counsel straightaway.

Establishing and Maintaining Confidentiality

People involved in an investigation should be made to understand that the investigation – and especially communications with counsel, and counsel's deliberations and work product – are confidential. There are a number of steps that can be taken to help ensure confidentiality. These steps can help a company establish, in the face of a challenge, that the work and communications of investigating counsel and other professionals are protected to the maximum extent under the law.

Limit Disclosure to Necessary Personnel

To establish and maintain the privilege, an investigating company should ensure that privileged communications are shared, and intended to be shared, only among appropriate personnel at the company, the company's counsel, and consultants retained to assist counsel in providing legal advice. Some courts deem documents that are intended to be shared with the government, or another third party, as not privileged.[6]

Clearly Mark Documents as Privileged and/or Attorney Work Product

Appropriate documents and communications should be marked as attorney-client privileged and/or attorney work product. Marking a document as such may help identify it and thus avoid an inadvertent production if it is in fact privileged or work product material. However, the mere marking of a document or communication as "attorney-client privileged" or "attorney work product" does not make it so. Application of the privilege or protection depends on the content of the communication or document, and the related facts and circumstances.

Assert the Privilege Early and Consistently

The privilege and work product protection should be asserted when applicable, including in response to government requests or other inquiries, and these assertions should be documented.

Give Upjohn Warnings

Investigating companies and their attorneys should deliver Upjohn warnings to witnesses during investigation interviews, including explaining that

1. Witness interviews are confidential and subject to the attorney-client privilege – which is held by the company rather than the interviewee;
2. The investigating attorneys represent the company and not the interviewee; and
3. The company may waive the privilege if it chooses, without notice to or consent of the interviewee, and disclose some or all of the contents of the interview to others, including the government.

In *Upjohn*, the Supreme Court held that the attorney-client privilege extends not only to communications between attorneys and senior corporate decision-makers, but also to interviews between attorneys and corporate employees where such communications are "at the direction of corporate superiors in order to secure legal advice from counsel."[7] Certain states have rejected the Upjohn approach, and subscribe to other standards for defining the extent of the privilege, such as the control-group test.[8] For purposes of federal enforcement actions, however, Upjohn controls.

Waiver Principles

Once established, the attorney-client privilege and work product protections apply unless and until they are waived. As a general matter, waivers may be intentional, implied or inadvertent. In addition to waiver, courts may order the discovery of fact work product (but not opinion work product) if (1) the facts at issue are not available from another source, (2) the party seeking discovery of the fact work product shows a substantial need for it, and (3) the fact work product is relevant to the party's claims. [9]

Waivers in the investigation context can occur in several ways:

Intentional Waivers

An intentional waiver can occur, at least in a limited way, if a company voluntarily decides to waive the privilege or work product protection over particular communications, documents or issues, and deliberately discloses such material to others – including law enforcement – that are outside the scope of the privilege. Intentional waivers should be carefully considered in advance, and if possible, the scope of any such waiver should be clearly defined and agreed to beforehand with the receiving party to limit the risk of a broader subject matter waiver. Subject matter waivers will be addressed in more detail in a subsequent installment of this series.

Implied Waivers

An implied waiver can occur if, for example, a privilege holder asserts a claim, such as an advice of counsel defense, that in fairness requires examination of a protected communication. In U.S. v. Bilzerian, for instance, the Second Circuit ruled that a good faith defense, if based on conversations with counsel, constitutes an implied waiver of privilege over such conversations. [10] And in In re Leslie Fay Cos. Sec. Litig., the Southern District of New York similarly held that using an attorney's report to support a dismissal motion constituted an implied waiver as to documents underlying that report.[11]

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 3 February 8, 2017

Inadvertent Waivers

Inadvertent waivers may occur if, for example, privileged communications or work product are unintentionally produced to a third party. Under Federal Rule of Evidence 502(b), an inadvertent disclosure of privileged or protected materials generally 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. A clawback clause, which can be included in a confidentiality agreement with the government, is often among the mechanisms a cooperating party can use in rectifying inadvertent disclosures.

Waiver of Attorney-Client Privilege vs. Waiver of the Work Product Protection

How these waiver principles apply differs between privileged materials and attorney work product. In general, disclosure of privileged materials to a third party (absent a common interest arrangement or agreement) may result in a waiver of the attorney-client privilege as to those materials. Attorney work product is different, however. As a general matter, disclosing attorney work product to a third party only waives the work product protection if that disclosure increases the ability of an adversary to gain access to the work product.[12]

The differing waiver principles governing privilege and work product reflect the distinct purpose that each doctrine serves. The attorney-client privilege encourages full and frank discussion between attorneys and their clients, whereas the attorney work product doctrine protects an attorney's mental impressions and legal strategies from adversaries. Because disclosing work product to a third party, particularly one that is not an adversary, is not necessarily contrary to the doctrine's purpose, such disclosures do not always result in a waiver of the work product protection.

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] Mark Eichorn, *If the FTC Comes to Call*, (May 20, 2015) ("In our eyes, a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach. Therefore, in the course of conducting an investigation, it's likely we'd view that company more favorably than a company that hasn't cooperated.").
[2] Fed. R. Civ. P. 26(b)(3)(B) ("[The court] must protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation.").
[3] Fed. R. Civ. P. 26(b)(3)(A) ("Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation . . . [b]ut . . . those materials may be discovered if: (i) [they are relevant and non-privileged] and (ii) 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.").
[4] 793 F. Supp. 2d 236, 253 (D.D.C. 2011).
[5] *See, e.g., In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522 (D. Minn. Oct. 23, 2015), E.C.F. No. 662 (denying plaintiffs' motion to compel production of documents created by task force, including 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"); *Genesco Inc. v. Visa U.S.A., Inc.*, No. 13-0202 (M.D. Tenn. Jan. 17, 2014), E.C.F. No. 297-1 (attorney-client privilege and work product protection applied to documents created by general counsel and consulting firm hired by general counsel to provide consulting and technical services to counsel in rendering legal advice regarding a cyber intrusion).
[6] *See In re Syncor ERISA Litig.*, 229 F.R.D. 636, 645 (C.D. Cal. 2005) ("[N]either the attorney-client privilege nor the work product doctrine applies to [documents] . . . created with the intent to disclose them to the Government.")
[7] *Upjohn Co. v. United States*, 449 U.S. 383, 394 (1981).
[8] *See, e.g., Consolidation Coal Co. v. Bucyrus-Erie Co.*, 432 N.E.2d 250 (Ill. 1982). In cybersecurity investigations involving state attorneys general from states that do not follow *Upjohn*, the respective state laws of privilege are likely to come into play.
[9] Fed. R. Civ. P. 26(b)(3)(A).
[10] 926 F.2d 1285, 1292 (2d Cir. 1991).
[11] 161 F.R.D. 274, 283 (S.D.N.Y. 1995).
[12] *See, e.g., United States v. Am. Tel. & Tel. Co.*, 642 F.2d 1285, 1299 (D.C. Cir. 1980).
[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.