Challenges Maintaining Attorney-Client Privilege in Anti-Corruption Enforcement Actions

Moderator:
Laura Perkins, Partner, Hughes Hubbard & Reed

Speakers:
Edward Kang, Partner, Alston & Bird
Richard Grime, Partner, Gibson Dunn
Obiamaka Madubuko, Shareholder, Greenberg Traurig
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

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. 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. Other agencies reviewing a cybersecurity incident, such as the FCC and SEC, may make other requests relating to their respective enforcement objectives.
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.”

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. 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.” 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” – 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. According to 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,” 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. 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
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.

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

...
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
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. 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.


[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.


[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.
Attorney-client privileged communications and attorney work product arise in the course of most if not all corporate internal investigations involving lawyers. Guarding the privilege and work-product protection are often important objectives for investigating companies as investigations proceed. This is particularly true for companies that conduct investigations while cooperating with the government on issues related to the FCPA. The privilege, and to a lesser extent the work-product doctrine, generally require confidentiality. Cooperation with the government, by contrast, often necessitates disclosure. This conundrum can be confounding.

This three-part series seeks to unwind that conundrum by closely examining the interplay between the attorney-client privilege and attorney-work-product protection, on the one hand, and cooperation with the government on the other. It provides an overview of factors for investigating companies and their counsel to consider as they navigate and balance the (sometimes) competing requirements of privilege/work product and cooperation in an FCPA investigation.

This first part 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 part will analyze what types of investigation materials can be shared with the government in an internal investigation without implicating the privilege or attorney-work-product protections, and what steps can be taken to protect privileged materials and attorney work product if they are shared with the government. The third and final part will provide an overview of when and how investigation materials that are privileged or protected by the work-product doctrine, and have been shared with the government, can sometimes be protected from discovery in collateral litigation.

**DOJ and SEC 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 DOJ and SEC, which are responsible for enforcing the FCPA, offer powerful cooperation incentives to companies that internally investigate and remediate alleged violations of the FCPA and share the facts they learn with the government.

In furtherance of their enforcement efforts, which have significantly increased in recent years, the DOJ and SEC offer cooperation credit – in the form of deferred or declined prosecution and reduced financial penalties, among other things – to companies that work with the government to report and remediate violations of the FCPA. Under the DOJ’s FCPA Pilot Program, for instance, a company may receive a declination of prosecution, up to a 50 percent reduction in criminal fines and the avoidance of an appointed compliance monitor, in exchange for self-disclosure, cooperation and remediation as defined by the Pilot Program.

For more on the DOJ’s 2016 Pilot Program, see “Going Deep on the Fraud Section’s FCPA Pilot Program” (Apr. 20, 2016); “How Will the Fraud Section’s Pilot Program Change Voluntary Self-Reporting?” (May 4, 2016); and “Earning Cooperation Credit Under the Fraud Section’s FCPA Pilot Program” (May 18, 2016).
To establish and guard the attorney-client privilege and 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 FCPA matter, 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 and/or attorney-work-product doctrine, provided the company takes the necessary steps to obtain such protections).

**The 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 alleged misconduct; confidential interviews with company employees (subject to Upjohn procedures, described further below); and confidential communications with experts retained to assist the attorneys, such as forensic accountants.
The 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, including a potential FCPA action, satisfies the “in anticipation of litigation” requirement. Thus, many investigation files created during an FCPA investigation by counsel, or at counsel’s direction, are likely to constitute work product.

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. 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 the protection of fact work product is subject to certain exceptions that do not apply to opinion work product. Whether an attorney’s work product constitutes fact or opinion depends on the content of the work product and requires a document-specific analysis.

For example, according to the Clemens case, which considered witness interview memoranda created during an investigation, 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. 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 considered 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, for instance 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 advice without a legal component, then such advice may not be deemed privileged.

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

In the United States, 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 is jurisdiction-specific and should be evaluated by locally-licensed attorneys.
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 ensure that confidentiality is protected. 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, investigating companies 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.⁴

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.

Non-Attorney Investigators

To the extent that non-legal professionals, such as forensic accountants 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. Such professionals are often directed by counsel, and at a minimum should coordinate closely with counsel, to remain within the privilege and work-product protections.

Non-attorney investigators who act without the involvement of legal counsel may find that their work is at risk of exposure. Non-lawyers – such as business people, accountants, auditors, 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, audit, 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 may not be immediately apparent, but if they neglect to involve legal counsel early on their work may 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 these can present risks that could be avoided by simply engaging and involving counsel straightaway.

For more on extensions of the attorney-client privilege, see “Attorney-Consultant Privilege? Key Considerations for Using the Kovel Doctrine (Part One of Two)” (Dec. 21, 2016); Part Two (Jan. 18, 2017).
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 witness, 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.”[5] Certain states have rejected the Upjohn approach, however, and subscribe to other standards for defining the extent of the privilege, such as the control-group test.[6]

For more information on international investigations, see “Handling the Challenges of Overseas Anti-Corruption Investigations: Forensic Accountants, Government Expectations, Translators, Upjohn Warnings, Privilege Issues and Recording Interviews” (May 1, 2013).

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 if the facts at issue are not available from another source, the party seeking discovery of the fact work product shows a substantial need for it, and the fact work product is relevant to the party’s claims.[7]

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, and/or issues, and deliberately discloses such material to others who 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.[8] In In re Leslie Fay Cos. Sec. Litig., the Southern District of New York similarly held that a company’s use of an attorney’s report to support a dismissal motion constituted an implied waiver as to documents underlying that report.[9]

Inadvertent Waivers

Inadvertent waivers may occur if, for example, privileged communications or work product are unintentionally produced to a third party, without adequate procedures to limit accidental production, and are not promptly recovered after the producing
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.

For more information on privilege and international investigations, see "Preserving the Attorney-Client Privilege in Cross-Border Internal Investigations" (Jun. 26, 2013).
Eric J. Gorman is a litigation partner based in Skadden’s Chicago office. He has conducted a substantial number of corporate internal investigations and represented companies and their boards in government investigations involving the SEC and DOJ. 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] 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.”).
[2] 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 . . . but . . . 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.”).
[11] 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.
More and more Latin American companies are conducting FCPA internal investigations when faced with allegations that employees or business partners have engaged in corrupt acts, as discussed by FCPAméricas here. This includes taking appropriate steps, such as issuing document preservation "holds," conducting internal investigation interviews and considering voluntary disclosures.
disclosure-considerations/) to enforcement authorities. Latin American companies subject to U.S. law enforcement are also learning the importance of preserving the attorney-client privilege when conducting investigations.

**The Attorney-Client Privilege.** The attorney-client privilege is a U.S. evidentiary privilege that allows a client – either a company or an individual – to seek legal advice from a lawyer in confidence. The purpose of the privilege is to encourage free and open discussions between a client and the client's attorney, which in turn promotes adherence to the law. The privilege applies when a client – either a company or an individual – communicates – either orally or in writing – with a lawyer – either inside or outside counsel – in confidence, for the purpose of obtaining legal advice. If the privilege is established, and so long as the communications are not disclosed to anyone else, neither the client nor the lawyer will be required to disclose these private communications to third parties.

**The Importance of Preserving Privilege in Internal Investigations.** Making sure investigations are privileged is important because it allows clients and their lawyers to discuss problems, to reach conclusions or other findings, to discuss alternative solutions and to make informed decisions based on the findings – without fear of disclosure to outside parties. This helps protect the accuracy and integrity of the review. This protection is especially important in the context of FCPA investigations, given the potential that third parties, including the U.S. government, company shareholders and other stakeholders, could seek access to highly sensitive information produced in a review. The findings of corruption investigations, by their very nature, have the potential to be harmful to a company's interests. The review might reveal that the company has violated the FCPA, the activity is criminal in nature and wrongdoing is widespread, which the company wants to remedy. Alternatively, the review might reveal that there are some questionable practices and some employees who believe the company's conduct is worse than it actually is. Without control over that information, companies can be left highly exposed and unable to choose the appropriate path to resolve the problems.

Because there is no way of predicting the outcome of the review when it begins, taking affirmative steps from the outset to preserve privilege is critical. It gives the company the ability to assess its problems and the alternatives facing it without the pressure that someone else will seek to use the information for his or her personal gain or to embarrass the company. If the review and the advice are privileged, company representatives can engage in frank discussions with its lawyers and can take the time to consider the company's options. This is particularly important if the company eventually decides to produce information to the government or the public.

**How to Preserve Privilege.** To establish privilege in an investigation, a company should:

- Use U.S. lawyers, either in-house or external, to initiate, direct and oversee the review. If other providers, like forensic accountants or investigators, participate in the investigation, their work should be conducted under the direction and oversight of lawyers so their findings are privileged as well.
- Take steps to make clear that the investigation is being conducted to obtain legal advice. This includes marking materials as “PRIVILEGED AND CONFIDENTIAL” and informing witnesses of the legal purpose of the investigation, as discussed here (http://fcpameicas.com/english/audits/ensuring-upjohn-sound-miranda/).
- Limit the distribution of investigation-related materials to help protect the confidentiality of the review.
- Do not allow company representatives to discuss the review with anyone who is not involved in the review.
Other Issues of Note. While internal communications with a company’s in-house counsel can be deemed privileged, they can also be subject to challenge. This is because in-house lawyers usually perform dual roles and the line between legal and business advice can be difficult to draw. Third parties might argue that the purpose of a communication was business-related and not legal, thereby leaving vulnerable the company’s assertion of privilege. Because of this, many companies choose to involve outside lawyers as a way to clearly establish privilege.

CCI Recommends:

How to Be a Wildly Effective Compliance Officer: Lea…
Compliance Management: A How-to Guide for Execu…
Compliance: A concise guide to the role of the Compliance Function in…

When structuring internal investigations, companies must also concern themselves with the privilege rules of local jurisdictions. For example, in Brazil’s civil law system, confidentiality between an attorney and a client is treated as an obligation, not a privilege, that cannot be waived by either party with some specific exceptions. Companies must carefully structure their reviews to consider rules like these so that they maximize protections over the findings in all relevant jurisdictions.

The opinions expressed in this post are those of the author in his or her individual capacity and do not necessarily represent the views of anyone else, including the entities with which the author is affiliated, the author’s employers, other contributors, FCPAméricas or its advertisers. The information in the FCPAméricas blog is intended for public discussion and educational purposes only. It is not intended to provide legal advice to its readers and does not create an attorney-client relationship. It does not seek to describe or convey the quality of legal services. FCPAméricas encourages readers to seek qualified legal counsel regarding anti-corruption laws or any other legal issue. FCPAméricas gives permission to link, post, distribute or reference this article for any lawful purpose, provided attribution is made to the author and to FCPAméricas LLC.
Matteson Ellis serves as Special Counsel to the FCPA and International Anti-Corruption practice group of Miller & Chevalier Chartered in Washington, DC. He is also founder and principal of Matteson Ellis Law PLLC, a law firm focusing on FCPA compliance and enforcement. He has extensive experience in a broad range of international anti-corruption areas. Previously, he worked with the anti-corruption and anti-fraud investigations and sanctions proceedings unit at The World Bank.

Mr. Ellis has helped build compliance programs associated with some of the largest FCPA settlements to date; performed internal investigations in more than 20 countries throughout the Americas, Asia, Europe and Africa considered “high corruption risk” by international monitoring organizations; investigated fraud and corruption and supported administrative sanctions and debarment proceedings for The World Bank and The Inter-American Development Bank; and is fluent in Spanish and Portuguese.

Mr. Ellis focuses particularly on the Americas, having spent several years in the region working for a Fortune 50 multinational corporation and a government ethics watchdog group. He regularly speaks on corruption matters throughout the region and is editor of the FCPAméricas Blog.

He has worked with every facet of FCPA enforcement and compliance, including legal analysis, internal investigations, third party due diligence, transactional due diligence, anti-corruption policy drafting, compliance training, compliance audits, corruption risk assessments, voluntary disclosures to the U.S. government and resolutions with the U.S. government. He has conducted anti-corruption enforcement and compliance work in the following sectors: agriculture, construction, defense, energy/oil and gas, engineering, financial services, medical devices, mining, pharmaceuticals, gaming, roads/infrastructure and technology.

Mr. Ellis received his law degree, *cum laude*, from Georgetown University Law Center, his masters in foreign affairs from Georgetown's School of Foreign Service, and his B.A. from Dartmouth College. He co-founded and serves as chairman of the board of The School for Ethics and Global Leadership in Washington, D.C. He is a member of the District of Columbia, Texas, New York, and New Jersey bar associations.

Mr. Ellis is also author of *The FCPA in Latin America: Common Corruption Risks and Effective Compliance Strategies for the Region*.
Supermarket to the World – The ADM FCPA Enforcement Action

Posted by Thomas Fox - January 6, 2014
Last week, it was announced that the Department of Justice (DOJ) and Securities and Exchange Commission (SEC) had settled an...

G8 Open Data Charter – The Implications for Due Diligence

One of the more substantial outcomes of the recent G8 leaders’ summit was the signing of the Open Data Charter.
Voluntary Disclosures, through the Eyes of FCPA Enforcement

Posted by Matteson Ellis (http://www.corporatecomplianceinsights.com/author/matteson-ellis/) - January 8, 2014
0 (http://www.corporatecomplianceinsights.com/voluntary-disclosures-through-the-eyes-of-fcpa-enforcement/#respond)

When James Cole, U.S. Deputy Attorney General, gave his keynote address at ACI’s 30th International Conference on the FCPA, he...

Ukraine Update: Anti-corruption Legislation Amid the Protests

0 (http://www.corporatecomplianceinsights.com/ukraine-update-anti-corruption-legislation-amid-the-protests/#respond)
The most significant element in the legislation is the introduction of corporate criminal liability for companies whose employees or their...

The Problem with Leniency Agreements in Brazil

Posted by Matteson Ellis - January 24, 2014

One of the most innovative features of Brazil’s new Anti-Bribery Law is Chapter 5, which establishes the possibility of leniency...
PODCASTS

TRACE Podcast: Hong Kong’s ICAC
(http://www.corporatecomplianceinsights.com/trace-podcast-hong-kongs-icac/)
January 31, 2018

TRACE Podcast: Understanding Suspension, Debarment and Blacklisting
(http://www.corporatecomplianceinsights.com/trace-podcast-understanding-suspension-debarment-blacklisting/)
January 24, 2018

TRACE Podcast: Dirty Entanglements: Corruption, Crime and Terrorism
(http://www.corporatecomplianceinsights.com/trace-podcast-dirty-entanglements-corruption-crime-terrorism/)
January 17, 2018

TRACE Podcast: 2017 FCPA Year in Review
(http://www.corporatecomplianceinsights.com/trace-podcast-2017-fcpa-year-review/)
January 10, 2018

Resilient: Jake Wood on Veterans Finding Purpose in Helping Others
(http://www.corporatecomplianceinsights.com/resilient-jake-wood-veterans-finding-purpose-helping-others/)
January 9, 2018

VIDEOS

The Impact of Technology on Enhanced Due Diligence
(http://www.corporatecomplianceinsights.com/impact-technology-enhanced-due-diligence/)
August 3, 2017
U.S. Regulatory Examiners’ 2017 Priorities
(http://www.corporatecomplianceinsights.com/u-s-regulatory-examiners-2017-priorities/)
February 6, 2017

SCOTUS Decides Highly-Anticipated Insider Trading Case
(http://www.corporatecomplianceinsights.com/scotus-decides-highly-anticipated-insider-trading-case/)
December 22, 2016

Promoting & Measuring Bank Culture Reform
(http://www.corporatecomplianceinsights.com/promoting-measuring-bank-culture-reform/)
June 8, 2016

Prepare for a Compliance Job Interview
Free Q&A
(http://www.corporatecomplianceinsights.com/compliance-job-interview-questions-and-answers/)

ABOUT CCI

Corporate Compliance Insights is a professionally designed and managed forum dedicated to online discussion and analysis of corporate compliance, risk assessment, ethics, audit, and corporate governance topics. Additionally, CCI is a focused knowledge-sharing forum designed to educate and encourage informed interaction within the corporate compliance community. CCI is founded by Maurice Gilbert, managing partner of Conselium Executive Search (http://www.conselium.com), the leading global compliance search firm.

A WHOLLY OWNED SUBSIDIARY OF:

(http://www.conselium.com)
We are a participant in the Amazon Services LLC Associates Program, an affiliate advertising program designed to provide a means for us to earn fees by linking to Amazon.com and affiliated sites.

©2017 Corporate Compliance Insights
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. 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. Other agencies reviewing a cybersecurity incident, such as the FCC and SEC, may make other requests relating to their respective enforcement objectives.
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,
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.”

**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. 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.” 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” – 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. 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. 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.
**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. 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.

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. 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. 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.


951 F.2d 1414, 1429–30 (3d Cir. 1991).

SEC Enforcement Manual § 4.3.1.

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.


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.