The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 5 March 8, 2017

ATTORNEY-CLIENT PRIVILEGE

Protecting Attorney-Client Privilege and Attorney Work Product While Cooperating With the Government: Implications for Collateral Litigation (Part Three of Three)

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

When a company conducts an internal investigation and cooperates with the government, there can sometimes be collateral litigation that in one way or another concerns the issues under investigation. Such litigation – which can be in addition to government regulatory enforcement actions – may involve the company itself as a party, or it may be limited to third parties. Moreover, it can be criminal or civil in nature, and may include, among other things, prosecutions of individuals or entities that are implicated in alleged misconduct; putative class actions arising out of failure to protect against security breaches; shareholder derivative claims; and other privacy and consumer protection litigation.[1]

If litigation does arise, and it appears to overlap in some way with issues that are or were under review in an internal investigation, the plaintiffs, prosecutors or defendants in the litigation sometimes may seek discovery of the company's internal investigation files. To support their discovery efforts, litigants may try to argue, among other things, that the privilege and work product protection were waived, perhaps as a result of the company's cooperation with the government.

Parts one and two of this series addressed ways for investigating companies to establish and preserve the attorney-client privilege and attorney work product protection during internal investigations and government cooperation. This third installment analyzes strategies and legal arguments that companies may wish to consider as they seek to shield investigation materials shared with the government from third-party discovery requests in collateral litigation.

The Risks of Collateral Litigation

The Northern District of California's recently issued discovery order in the Bio-Rad case demonstrates the litigation risk to investigating companies.[2] There, the plaintiff, Bio-Rad's former general counsel, filed retaliatory discharge claims against his former employer, alleging that he had been wrongfully terminated for raising potential violations of the Foreign Corrupt Practices Act ("FCPA") with Bio-Rad's Audit Committee. The ex-general counsel claimed that he had identified and raised these potential violations while the company was conducting an internal FCPA investigation, and that he was subsequently terminated, allegedly in retaliation for flagging these issues. In its defense, the company cited its internal investigation and related findings, explaining that the investigation did not identify evidence of corrupt practices, as the company had reported to the government. Plaintiff argued that the company waived any privilege and work product protection over its related FCPA investigation files by, inter alia, disclosing them to the government as part of its cooperation.[3] The district court agreed, ruling that the company's disclosures to the DOJ and SEC amounted to a waiver. (The court also cited the company's reliance on some of those materials in its defense in the lawsuit, including filing certain materials in unredacted form with the court, revealing privileged communications in publicly filed declarations, and sharing certain materials with the Department of Labor during an earlier stage of the dispute.)

The case law on protecting investigation files is mixed, but investigating companies can assert a number of different arguments in collateral litigation, in an effort to defend the attorney-client privilege and attorney

work product protection over investigation materials. The courts have developed a variety of analytical approaches for addressing these arguments, which have yielded different – and sometimes conflicting – results.

Notwithstanding the uncertainty in the case law, the existing jurisprudence suggests that investigating companies can avoid a waiver by sharing facts, as opposed to privileged communications or attorney work product, with the government, and can at least somewhat reduce (though not eliminate) the risk of a waiver when privileged communications or attorney work product are shared by executing and utilizing a confidentiality agreement with the government; identifying and relying on a common interest, if one exists, with the government; and if a waiver is intended, or likely, defining its scope in a way that is clear, defensible and designed to avoid a broader waiver.

Sharing Facts Minimizes the Risk of Waiver

The more purely factual a cooperating company's disclosures to the government are, the stronger its defenses against a potential waiver claim are likely to be, if collateral litigation arises. As explained in part two, law enforcement agencies including the DOJ/FBI and state and local bodies strongly encourage companies that are victims of cybersecurity attacks to timely share information with the government in an effort to identify and punish wrongdoers, minimize damage, and limit additional attacks. To the extent other government agencies (for example, the FTC) become involved, the government generally expects companies that cooperate to fully disclose the facts underlying alleged violations. Although certain agencies that may become involved in cybersecurity issues do not appear to have specific guidance on the issue of waiver, both the DOJ and SEC have spoken on the issue, and neither agency requires companies to waive the attorney-client privilege or attorney work product protection in order to receive cooperation credit. More fundamentally, and as part two explains, the attorney-client privilege and attorney work product protection exist as a matter of law and can be asserted regardless of any particular agency's position, or silence, on the matter.

Orienting a victim or cooperating company's interactions with the government around these principles – focusing on facts, and limiting (or avoiding altogether) the sharing of privileged communications and/or attorney work product – can help reduce opportunities for a third-party litigant to later claim that a company waived the privilege and/or work product protection by sharing information with the government. Indeed, if a third-party litigant cannot identify specific disclosures of privileged communications or attorney work product to the government (or others outside the company-counsel ambit), it will be unlikely to succeed in arguing that the investigating company waived the attorney-client privilege or the attorney work product protection. And because neither the privilege nor the work product protection applies to facts, standing alone, the disclosure of such facts should not endanger either protection.

As discussed in detail in part one, the attorney-client privilege protects communications seeking or rendering legal advice, and the attorney work product doctrine insulates materials created by or at the direction of counsel in anticipation of litigation. Facts may be discussed in communications with counsel, or analyzed in attorney work product, and those discussions and analyses generally are protected under the law. The facts themselves, however, are not. Accordingly, companies may share the facts learned during an investigation (as well as non-privileged documents) with the government without affecting the company's legal protections.[4] Indeed, just as a witness who is deposed, or a company that is subpoenaed, generally cannot refuse to respond with factual information by calling it privileged or work product, a cooperating company does not waive the attorney-client privilege or attorney work product protection by sharing facts with the government.[5]

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 5 March 8, 2017

Other limitations recognized in the law can also help. For instance, because opinion work product receives the highest degree of protection in the courts, sharing only fact work product with the government should not result in a waiver of opinion work product – even on a related matter.[6] Similarly, if a production is compulsory, rather than voluntary, it is less likely to be deemed a waiver.[7] However, certain courts have ruled that a cooperating company's response to an SEC subpoena is voluntary, notwithstanding the existence of the subpoena.[8]

Courts May or May Not Respect Confidentiality and Non-Waiver Agreements

Whether or not an investigating company intends to share privileged communications or attorney work product with the government, a confidentiality agreement should nevertheless be considered. As described in part two, such agreements typically limit disclosure (beyond the government) of investigation materials that the company shares, and provide express non-waiver language in which the government and company agree that production of investigation materials does not waive any applicable legal protections. A confidentiality agreement also may provide clawback protections in the event of an inadvertent disclosure. The government regularly enters into confidentiality agreements with cooperating companies, and in general, these agreements should be effective and enforceable as between the investigating company and the government.

Some courts hold that government confidentiality agreements permit an investigating party to share privileged communications and attorney work product with the government without waiving the privilege and work product protection vis-à-vis other persons or entities.[9] Other courts, however, disagree and hold that disclosure to the government amounts to a waiver, notwithstanding the existence of a confidentiality agreement.[10]

The Theory of Selective Waiver

The legal framework underlying these conflicting outcomes begins with the doctrine of selective, or limited, waiver. As a general matter, parties waive attorney-client privilege by disclosing a privileged communication to a third party, and they waive work product protection by sharing protected attorney material with an adversary. However, in Diversified Indus., Inc. v. Meredith,[11] the Eighth Circuit reasoned that the government occupies a different role than private litigants, and it accordingly created the selective waiver exception. The court thus held that a company's prior disclosure of privileged materials to the government during an internal investigation did not waive the privilege as to other parties.[12] Certain courts have since expanded this doctrine to include attorney work product.

Rejection of the Theory by Other Courts

Despite the Eighth Circuit's adoption of the selective waiver doctrine, a number of other circuits have rejected the doctrine, holding that a waiver cannot be confined in this way, and that disclosing privileged communications to the government also waives the privilege more generally. Specifically, the First, Third, Fourth, Sixth, Ninth, and D.C. Circuits have rejected the selective waiver doctrine in the context of the attorney-client privilege.[13]

Courts in the Tenth and Federal Circuits have declined to apply the selective waiver doctrine to specific facts, but have not ruled definitively that the selective waiver doctrine is, or is not, legally available.[14] The Fifth and Eleventh Circuits do not appear to have addressed selective waiver, but district courts in those circuits have declined to apply the doctrine to the facts at issue in specific cases before them.[15] As for the Seventh Circuit, it has both appeared to implicitly accept the notion of selective waiver in Dellwood Farms,[16] and stated in Burden-Meeks (which did not acknowledge the selective waiver discussion in Dellwood Farms) that "selective disclosure is not an option."[17] And, as described below, the

Northern District of Illinois in fact later applied the selective waiver doctrine, after Burden-Meeks was decided, to protect an investigation report that was shared with the government pursuant to a confidentiality agreement.

The Second Circuit's Middle-Ground Approach

The Second Circuit has adopted a middle ground. In In re Steinhardt Partners, L.P., that court declined to endorse a per se rule for or against the selective waiver doctrine, and instead held that waiver determinations require a fact-specific analysis that considers any confidentiality agreement or common interest.[18] Accordingly, district courts in the Second Circuit have proceeded to analyze the facts and circumstances in particular cases. In so doing, however, they have at times rendered inconsistent and sometimes contradictory rulings, for example about whether confidentiality agreements are effective at preserving any privilege over communications or attorney work product that is shared with the government.

In one case, for instance, the Southern District of New York held that a disclosure to the government, subject to a confidentiality agreement, of investigation files containing privileged communications and attorney work product did not waive the privilege or work product protection because the agreement included "explicit non-waiver" provisions, which were sufficient to prevent a waiver.[19] In a separate ruling in that case, the court cited the government's stated intention to keep the materials confidential, which is required to maintain privilege, as well as the express non-waiver language in the agreements.[20]

Other district courts in the Second Circuit have reached the opposite conclusion and have found waivers even when a confidentiality agreement was in place. For instance, one court in the SDNY ruled that a voluntary disclosure of attorney work product to the SEC waived the work product protection, notwithstanding a confidentiality agreement.[21] The court disregarded the confidentiality agreement there, describing it as "essentially a fig leaf that permits the producing party to claim, as to third parties, that attorney-client privilege and work product protection are preserved." The court thus ruled that the company's waiver of the privilege and work product protection extended beyond the government to include other parties.[22]

The Effect of Confidentiality Agreements Outside the Second Circuit

Outside the Second Circuit, the Northern District of Illinois ruled in one case that disclosure of outside counsel's report to the SEC during an investigation did not waive the attorney-client privilege or attorney work product protection because the government signed a confidentiality agreement, which included an express non-waiver provision.[23]

Various other courts, however, have ruled that confidentiality language – which is endorsed in the SEC Enforcement Manual and excerpted in certain decisions – requiring the government to maintain the confidentiality of materials it receives, unless disclosure is required by law or would further the government's discharge of its duties, is insufficient to preserve the privilege or work product protection. Such discretion on the part of the government, these courts hold, undercuts the requirement of confidentiality. Yet other courts disagree, and deem government confidentiality agreements containing such language to be effective at preserving privilege and work product.

Still other courts take into account a presumed rationale for company disclosures to the government – i.e., that companies share information with the government for their own benefit, as opposed to assisting the government – and thus find a waiver.[24] But such cases do not necessarily fully acknowledge the government's own need for and interest in such information, as explained in the common interest section below. Complicating matters even further, the waiver analyses in the rulings sometimes neglect to account for and apply the distinct waiver principles

that cover privilege and attorney work product, and at other times provide only limited rationales for the decisions reached.

The Varied Rulings Spell Risk for Companies

This varied legal landscape creates risk for cooperating companies. The selective waiver doctrine applies in the Eighth Circuit. It is sometimes applied in the Second and Seventh Circuits. Certain circuits have not considered it. And in a number of other circuits, the doctrine is not available.

Regardless, companies can maximize their chances – to the extent possible – of preserving the attorney-client privilege and attorney work product doctrine over protected materials that are shared with the government by entering into a confidentiality agreement. But in doing so, cooperating companies should recognize the risk, even with such an agreement, of a potential waiver, and weigh that risk against the benefits the company expects to obtain by sharing attorney-client communications or attorney work product with the government in the first place.

Common Interest

Using Common Interest to Preserve Attorney Work Product Protections

The waiver principles that apply to attorney work product differ from those covering the attorney-client privilege. In certain circumstances, as explained in part one, attorney work product may be shared with other parties without waiving the protection if doing so advances a common goal and would not make the materials accessible to adversaries. This standard can be satisfied even if the common interest is not with a specific party in particular litigation.[25] These principles have persuaded certain courts to permit investigating companies to share attorney work product with the government without waiving the protection.[26]

The government's interest in cybersecurity issues is manifest and has been expressed repeatedly. The government has often stated that it places a high priority on cybersecurity, and strongly encourages victim companies to report breaches and share relevant information with law enforcement. The FTC, for instance, has noted that it tends to more favorably regard companies that self-report breaches and cooperate with the government than those that do not.[27] The DOJ has issued extensive guidelines describing best practices for companies before, during, and after a cybersecurity incident, and emphasizes the need to be open with law enforcement.[28] These government interests may be shared, in many respects, by companies.

Companies experiencing a cybersecurity breach also may find common cause with the government in pursuing individuals – including employees – who are implicated in an incident. For instance, the DOJ explained last year in the Yates Memorandum that one of its principal enforcement objectives is to hold individuals accountable for corporate wrongdoing – e.g., senior officers and other employees who are responsible for unlawful conduct. Under certain circumstances, companies arguably may have a common interest with the government in that goal. Companies experiencing a cyber incident also may share an interest with the government in recovering intellectual property, for instance if individual employees stole, or assisted others in stealing, intellectual property in a cyber incident. And, more generally, the Cardinal Health and Wsol decisions note a common interest between investigating companies and the government in rooting out possible problems and ensuring lawful conduct.[29]

Common Interest May Be More Challenging to Assert If the Company Is a Target

The common-interest argument may be more challenging to assert, however, if the company itself is a target of the government agency to which it discloses. In such a case, it can be more difficult to argue that the company and the agency share a common interest and are not adversaries.[30] Indeed,

even if the company is not a target, courts sometimes find that the company could be a target – a potential adversary – and thus deem work product protection waived.[31] Nevertheless, companies that wish to share attorney work product with the government in connection with an investigation should analyze whether any common interests exist that could support such a disclosure.

Carefully Define the Scope of a Possible Waiver

If the investigating company intends to make a waiver, or a waiver is likely to be found, the company can make its disclosures in a way that is designed to limit the scope of the waiver. If the waiver's scope is defined in a factually well-founded and defensible way, it could help lay the groundwork for later reliance on Rule 502(a) of the Federal Rules of Evidence, which governs subject matter waiver, in collateral litigation.

What constitutes the same "subject matter" under Rule 502 is fact-dependent. Courts making this determination assess the substance of the protected materials that were disclosed, and determine the subject matter accordingly.[32] Thus, for example, a factual disclosure that describes a single protected meeting may result in a limited waiver of fact work product related to that meeting. However, an express and general waiver over an investigation as a whole (for instance, by relying on the investigation generally as a defense to liability) may result in a broad waiver of undisclosed materials that were created as part, and in furtherance, of that investigation – though not necessarily other, unrelated, investigations.[33]

Courts also consider the fairness of the waiver in an effort to avoid undue discovery windfalls to particular parties.[34] Thus, the disclosure of one privileged investigation file should only waive the privilege as to another file if the second file relates to the same subject matter and it would be unfair to consider the first document without the second.[35]

Conclusion

Ultimately, companies that internally investigate cybersecurity breaches and cooperate with the U.S. government should be aware that the materials they disclose to the government, including those protected by the attorney-client privilege or attorney work product doctrine, may later be sought by third parties in collateral litigation. While the merits of any waiver argument will be decided by a court, companies conducting internal investigations can take the proactive steps outlined above, and in parts one and two, to maximize their chances of establishing and preserving the attorney-client privilege and attorney work product protections as they investigate, cooperate, and potentially litigate issues related to the breach.

Eric J. Gorman is a litigation partner based in Skadden's Chicago office.[36] He has conducted a substantial number of corporate internal investigations and represented companies and their boards in government investigations involving the SEC and DOJ. Mr. Gorman has handled investigations in the U.S. and abroad, and has advised boards of directors and senior executive teams in connection with U.S. criminal and regulatory issues. His litigation experience also includes defending against large-scale class actions, and prosecuting and defending transaction-related litigation and other high-value claims.

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

[1] *See, e.g., United States v. Yihao Pu*, 814 F.3d 818 (7th Cir. 2016) (criminal prosecution for stealing high frequency trading code from investment firm); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x. 384, 386 (6th Cir. 2016) (putative class action asserting claims for invasion of privacy, negligence, bailment, and violations of Fair Credit Reporting Act arising out of company's alleged failure to protect against dissemination of customer data after hackers broke into company's computer network and allegedly stole plaintiffs' personal information); *Torres v. Wendy's Co.*, 195 F. Supp. 3d 1278, 1280 (M.D. Fla. 2016) (putative class action alleging breach of implied contract, negligence and deceptive and unfair trade practices relating to malware detected on company's payment processing system); *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522 (D. Minn. Oct. 23, 2015), E.C.F. No. 662 (consolidated class actions brought by financial institutions and consumers arising out of Target's 2013 security breach announcement); Davis v. Target Corp. et al., No. 14-cv-203 (D. Minn. Jan. 21, 2014) (shareholder derivative litigation filed against company's officers and directors alleging breach of fiduciary duties for allegedly failing to oversee information security program and failing to provide customers with prompt and accurate disclosure of data breach).

[2] Order on Mot. to Exclude, *Wadler v. Bio–Rad Labs., Inc.*, No. 15-CV-02356-JCS, 2016 WL 7369246, at *1 (N.D. Cal. Dec. 20, 2016).

[3] *Id.* at *16.

[4] *See, e.g., Kintera, Inc. v. Convio, Inc.*, 219 F.R.D. 503, 511 (S.D. Cal. 2003).

[5] *See Oasis Int'l Waters, Inc. v. United States*, 110 Fed. Cl. 87, 99–100 (2013) ("[A]lthough the privilege protects the substance of attorney-client communications, it does not protect disclosure of the underlying facts by those who communicated with the attorney." (citation omitted)).

[6] *See, e.g., In re Martin Marietta Corp.*, 856 F.2d 619, 626 (4th Cir. 1988) ("We think that when there is subject matter waiver, it should not extend to opinion work product.").

[7] *See, e.g., In re Pac. Pictures Corp.*, 679 F.3d 1121, 1130 (9th Cir. 2012) ("Involuntary disclosures do not automatically waive the attorney-client privilege."); *see also In re Subpoenas Duces Tecum*, 738 F.2d 1367, 1373 (D.C. Cir. 1984) ("The distinction between voluntary disclosure and disclosure by subpoena is that the latter, being involuntary, lacks the self-interest which motivates the former. As such, there may be less reason to find waiver in circumstances of involuntary disclosure.").

[8] *See, e.g., In re Steinhardt Partners, L.P.*, 9 F.3d 230, 232-35 (2d Cir. 1993).

[9] *See, e.g., Police & Fire Ret. Sys. of Detroit v. Safenet, Inc.*, No. 06 Civ. 5797(PAC), 2010 WL 935317, at *2 (S.D.N.Y. Mar. 12, 2010).

[10] *See, e.g., In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 302, 306 (6th Cir. 2002).

[11] 572 F.2d 596 (8th Cir. 1978) (*en banc*).

[12] *Id.* at 611.

[13] *See, e.g., United States v. Mass. Inst. of Tech.*, 129 F.3d 681, 686 (1st Cir. 1997); *Westinghouse Elec. Corp. v. Republic of Phil.*, 951 F.2d 1414, 1425 (3d Cir. 1991); *In re Martin Marietta Corp.*, 856 F.2d at 623; *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d at 302; *In re Pac. Pictures Corp.*, 679 F.3d 1121, 1128 (9th Cir. 2012); *Permian Corp. v. United States*, 665 F.2d 1214, 1220 (D.C. Cir. 1981). The Fourth Circuit's ruling in *Martin Marietta* also addressed attorney work product.

[14] *See In re Qwest Commc'ns Int'l*, 450 F.3d 1179, 1192 (10th Cir. 2006); *Genentech, Inc. v. U.S. Int'l Trade Comm'n*, 122 F.3d 1409, 1417 (Fed. Cir. 1997).

[15] *See Pensacola Firefighters' Relief Pension Fund Bd. of Trustees v. Merrill Lynch Pierce Fenner & Smith, Inc.*, 265 F.R.D. 589, 596 (N.D. Fla. 2010); *see also S.E.C. v. Brady*, 238 F.R.D. 429, 440-41 (N.D. Tex. 2006).

[16] *Dellwood Farms, Inc. v. Cargill, Inc.*, 128 F.3d 1122, 1127 (7th Cir. 1997) (noting that "[i]n the case of selective disclosure, the courts feel, reasonably enough, that the possessor of the privileged information should have been more careful, as by obtaining an agreement by the person to whom they made the disclosure not to spread it further.").

[17] *Burden-Meeks v. Welch*, 319 F.3d 897, 899 (7th Cir. 2003).

[18] 9 F.3d 230, 236 (2d Cir. 1993).

[19] *In re Nat. Gas Commodities Litig.*, 232 F.R.D. 208, 211-12 (S.D.N.Y. 2005).

[20] *In re Nat. Gas Commodity Litig.*, No. 03 Civ. 6186VMAJP, 2005 WL 1457666, at *4, 8-9 (S.D.N.Y. June 21, 2005). *See also Police & Fire Ret. Sys. of Detroit*, 2010 WL 935317, at *2.

[21] *Gruss v. Zwirn*, No. 09 Civ. 6441, 2013 WL 3481350, at *8 (S.D.N.Y. July 10, 2013).

[22] *Id.* at *9.

[23] *Lawrence E. Jaffe Pension Plan v. Household International, Inc.*, 244 F.R.D. 412, 433 (N.D. Ill. 2006).
[24] *See Westinghouse*, 951 F.2d at 1429; *In re Subpoenas Duces Tecum*, 738 F.2d 1367, 1375 (D.C. Cir. 1984).
[25] *See United States v. Am. Tel. & Tel. Co.*, 642 F.2d 1285, 1300 (D.C. Cir. 1980) ("The existence of common interests between transferor and transferee is relevant to deciding whether the disclosure is consistent with the nature of the work product privilege. But 'common interests' should not be construed as narrowly limited to co-parties.").
[26] *See, e.g., In re Cardinal Health, Inc. Sec. Litig.*, No. C2 04 575 ALM, 2007 WL 495150, at *9 (S.D.N.Y. Jan. 26, 2007) (no waiver; government and company it was investigating shared common interest in keeping sound financial and accounting practices); *Wsol v. Fiduciary Mgmt. Assocs., Inc.*, No. 99 C 1719, 1999 WL 1129100, at *6 (N.D. Ill. Dec. 7, 1999) (disclosing party and government had common interest in uncovering improper fund management; disclosing party was not a target of government's investigation, and cooperated with government to enhance likelihood that government would obtain restitution).
[27] Mark Eichorn, Assistant Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, FTC, *If the FTC Comes to Call* (May 20, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call ("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.").
[28] *See* Cybersecurity Unit, Computer Crime & Intellectual Property Section, Crim. Div., U.S. Dep't of Justice, *Best Practices for Victim Response and Reporting of Cyber Incidents* (Apr. 2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf (stating among other things that "[o]rganizations should have a plan in place for handling computer intrusions before an intrusion occurs. . . . [including] [p]rocedures for notifying law enforcement and/or computer incident-reporting organization"; "[o]rganizations should attempt to establish a relationship with their local federal law enforcement offices long before they suffer a cyber incident"; and "[i]f an organization suspects at any point during its assessment or response that the incident constitutes criminal activity, it should contact law enforcement immediately.").
[29] *See* footnote 26, *supra*.
[30] *See, e.g., Westinghouse*, 951 F.2d at 1428 (court had "no difficulty" in finding that government and investigating company, which was a target, were adversaries); *Gruss*, 2013 WL 3481350, at *11-12 (court found that SEC was "an adverse government agency," so disclosure waived privilege and work product protection); *United States v. Reyes*, 239 F.R.D. 591, 604 (N.D. Cal. 2006); *U.S. v. Bergonzi*, 216 F.R.D. 487, 498 (N.D. Cal. 2003); *Cooper Hosp./Univ. Med. Ctr. v. Sullivan*, 183 F.R.D. 119, 129 (D.N.J. 1998); *In re Leslie Fay Cos. Sec. Litig.*, 152 F.R.D. 42, 45 (S.D.N.Y. 1993).
[31] *See, e.g., Mass. Inst. of Tech.*, 129 F.3d at 687.
[32] *See, e.g., E.I. DuPont de Nemours & Co. v. Kolon Indus., Inc.*, 269 F.R.D. 600, 609 (E.D. Va. 2010) (holding that company waived fact work product protection over in-house counsel's documents setting forth factual basis for arranging and attending meeting described in press release).
[33] *United States v. Mount Sinai Hosp.*, 185 F. Supp. 3d 383, 394 (S.D.N.Y. 2016) (company's express waiver of privileged documents in connection with billing practices investigation extended to underlying materials, but did not waive privilege or work product protection concerning separate and unrelated investigation conducted by same counsel). *See also United States v. Stewart*, No. 15-cr-00287, Dkt. 141 (S.D.N.Y. July 22, 2016) (waiver over internal investigation materials limited to communications that were disclosed to FINRA).
[34] *See, e.g., Navajo Nation v. Peabody Holding Co.*, 225 F.R.D. 37, 48 (D.D.C. 2009).
[35] *See In re Gen. Motors LLC Ignition Switch Litig.*, 80 F. Supp. 3d 521, 533 (S.D.N.Y. 2015) ("In particular, such disclosure results in a subject matter waiver of undisclosed materials only in those 'unusual situations in which fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary.'" (citing Fed. R. Evid. 502, Committee Notes)).
[36] 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.