Brooklyn Law Review

Volume 82 | Issue 4 Article 9

1-1-2017

Reevaluating Attorney-Client Privilege in the Age of Hackers

Anne E. Conroy

Reevaluating Attorney-Client Privilege in the Age of Hackers

"Dance like no one is watching; email like it may one day be read aloud in a deposition."[1]

INTRODUCTION

In 2014, a group hacked Sony Pictures Entertainment servers and made public Sony's financial information, along with engrossingly candid email exchanges between its executives.[2] A year later, hackers released the email addresses, partial credit card information, and sexual preferences of over thirty million Ashley Madison users.[3] Shortly after the release of this data, two different search tools appeared online[4] allowing interested Internet users to discover who had an account with the "Life is Short. Have an Affair" dating website.[5] In 2016, over 100 media organizations published coverage of 11.5 million documents obtained through a hack of a Panamanian law firm, Mossack Fonseca.[6] The documents revealed financial assets of celebrities, athletes, and world leaders and came to be known as the "Panama Papers."[7] In the final weeks leading up to the 2016 presidential election, WikiLeaks[8] released a treasure trove of

---

[1] Olivia Nuzzi (@Olivianuzzi), TWITTER (Dec. 13, 2014, 1:18 PM), https://twitter.com/olivianuzzi/status/543877654576107520 [https://perma.cc/MJC6-6HBY].

[2] Sam Biddle, *Everything You Need to Know About Sony' s Unprecedented Hacking Disaster*, GAWKER (Dec. 15, 2014), http://sonyhack.gawker.com/everything-you-need-to-know-about-sonys-unprecedented-h-1671217518 [https://perma.cc/CLJ9-FHB8].

[3] Daniel Victor, *The Ashley Madison Data Dump, Explained*, N.Y. TIMES, Aug. 19, 2015, http://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html [https://perma.cc/7A39-GGQN]. *The Hill* reported that 15,000 government emails were revealed in the hack. Cory Bennett, *15,000 Government Emails Revealed in Ashley Madison Leak*, HILL (Aug. 19, 2015), http://thehill.com/policy/cybersecurity/251431-ashley-madison-leak-appears-real-includes-thousands-of-government-emails [https://perma.cc/LUH9-HRF8].

[4] Victor, *supra* note 3.

[5] Bennett, *supra* note 3.

[6] Susan Miller, *Panama Papers Explainer: What You Should Know*, USA TODAY (Apr. 3, 2016), http://www.usatoday.com/story/news/2016/04/03/panama-papers-explainer-what-you-should-know/82591116/ [https://perma.cc/5JGD-YLWL].

[7] *See id.*

[8] According to its website, "WikiLeaks specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption. It has so far published more than 10 million

emails from Democratic candidate Hillary Clinton's national campaign chairman, John Podesta.[9] While the contents of the emails were fairly mundane,[10] the releases nevertheless dominated news cycles, capturing the interest of and commentary from voters, political operatives, and the media.[11] Each of the hacks has had far-reaching consequences, ranging from a prime minister's resignation,[12] to exposure of national security measures.[13] Of course, each hack has also led to the fear that

documents and associated analyses." *What Is WikiLeaks*, WIKILEAKS (Nov. 3, 2015), https://wikileaks.org/What-is-Wikileaks.html [https://perma.cc/8VBX-PMZ4].

[9] Peter Nicholas, *WikiLeaks' Clinton Emails Present Painful Dilemma*, WALL ST. J. (Oct. 27, 2016), http://blogs.wsj.com/washwire/2016/10/27/wikileaks-clinton-emails-present-painful-dilemma/; Politico Staff, *WikiLeaks' Assange Denies Russia Behind Podesta Hack*, POLITICO (Nov. 3, 2016), http://www.politico.com/story/2016/11/julian-assange-russia-john-podesta-wikileaks-230676 [https://perma.cc/MY79-DZRD].

[10] *See, e.g.*, *84 Rejected Clinton Campaign Slogans Revealed by WikiLeaks*, FOX NEWS INSIDER (Oct. 20, 2016), http://insider.foxnews.com/2016/10/20/84-rejected-clinton-campaign-slogans-revealed-wikileaks [https://perma.cc/73M5-D8LS] (a compilation of potential campaign slogans the Clinton campaign considered and rejected). *But see* Byron Tau, *WikiLeaks Reveals UFO Messages in Clinton Campaign Emails*, WALL ST. J. (Oct. 10, 2016), http://blogs.wsj.com/washwire/2016/10/10/wikileaks-reveals-ufo-%E2%80%8Bmessages-in-clinton-campaign-emails/ [https://perma.cc/KLE5-TTN8] (The former lead singer of power punk band Blink 182 emailed Podesta, writing about their mutual interest in unidentified flying objects.).

[11] The Wall Street Journal commented that "[n]ever in modern history has the public gotten so vivid a window into how a campaign thinks and functions from its earliest stages." Nicholas, *supra* note 9. A member of the media commented that "[i]t's like reading one of the post-campaign books while the campaign is still going on." Brian Stelter (@brianstelter), TWITTER (Oct. 14, 2016, 9:50 PM), https://twitter.com/brianstelter/status/786972357755740161 [https://perma.cc/636Z-HCHF]. Other journalists lamented how nonjournalists scour through thousands of released emails and circulate snapshots of conversations taken out of context and without analysis. Jesse Singal, *'Citizen Journalism' Is a Catastrophe Right Now, and It'll Only Get Worse*, N.Y. MAG. (Oct. 19, 2016), http://nymag.com/selectall/2016/10/citizen-journalism-is-a-catastrophe-itll-only-get-worse.html [https://perma.cc/E92N-NUHM] ("Every time WikiLeaks drops a new trove of Hillary Clinton or Democratic National Committee emails . . . countless citizen journalists rush to pore over the documents, posting *j'accuse* screen-grabs ripped from context that are quickly retweeted through huge, hyperactive networks of anti-Clinton Twitter denizens.").

[12] Steven Erlanger et al., *Iceland's Prime Minister Steps Down Amid Panama Papers Scandal*, N.Y. TIMES (Apr. 5, 2016), https://www.nytimes.com/2016/04/06/world/europe/panama-papers-iceland.html [https://perma.cc/8ZYN-YN4C].

[13] Greg Miller & Ellen Nakashima, *WikiLeaks Says It Has Obtained Trove of CIA Hacking Tools*, WASH. POST (Mar. 7, 2017), https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html?utm_term=.461967c3b8b9 [https://perma.cc/X79P-QVTR]. For a detailed description of the impact of a cyberattack on national critical infrastructure see Gabriel K. Park, Note, *Granting an Automatic Authorization for Military Response: Protecting National Critical Infrastructure from Cyberattack*, 38 BROOK. J. INT'L L. 797, 801–07 (2013).

anything sent by email may one day end up on the internet.[14] According to security experts, this trend is only growing.[15]

These examples highlight a recurring theme that has emerged in the increasingly digital world of the twenty-first century: hackers breach a security system and post internal, confidential information online for anyone to comb through. In all of the above instances, hackers revealed, at best, inadequate cybersecurity measures[16] and, at worst, questionable legal activities. Indeed, several hackers have publicly stated that their motives are altruistic, that they want to provide the public with critical information about major companies or governmental agencies.[17]

This digital version of whistleblowing, called "hacktivism,"[18] is certainly attractive to the media, which has not balked at widely covering the confidential communications revealed by the hacks. News organizations can lean on broad First Amendment protection that permits the publication of illegally obtained materials,[19] so long as the organization itself

---

[14] *See* Olivia Oran, *On Wall Street, a High-Ranking Few Still Avoid Email*, REUTERS (Nov. 1, 2016), http://www.reuters.com/article/us-wall-street-email-idUSKBN12W4F7 [https://perma.cc/HYZ9-9DHT].

[15] *See, e.g.*, Dino Grandoni, *Ashley Madison, a Dating Website, Says Hackers May Have Data on Millions*, N.Y. TIMES (July 20, 2015), http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html [https://perma.cc/L8TB-N3JX] ("'I think we're going to see more of it as people see how effective [hacking] is,' said Bruce Schneier, chief technology officer for Resilient Systems, a security company . . . ."); *see* Singal, *supra* note 11 ("We're all engaging in a big, messy experiment in how human beings produce, consume, and disseminate knowledge . . . .").

[16] *Infra* Section III.A discusses the need for attorneys to take adequate cybersecurity precautions to avoid hacks, or risk a court finding an implied waiver of attorney-client privilege.

[17] For example, after Wikileaks published thousands of documents allegedly detailing the Central Intelligence Agency's hacking tools, its founder, Julian Assange, pledged to provide further information to several tech giants whose products the CIA targeted. Assange stated that he would provide the tech companies with the information so that they could identify and patch their own security flaws. Thomas Fox-Brewster, *Julian Assange: Wikileaks May Have Evidence CIA Spied on US Citizens*, FORBES (Mar. 9, 2017), https://www.forbes.com/sites/thomasbrewster/2017/03/09/julian-assange-cia-spying-american-citizens-apple-google-help/#1c2d614430a1 [https://perma.cc/M99N-FUWV]. Some experts expressed doubts, however, that Assange's motives were so pure when several days after releasing the files he still had not provided Google or Microsoft with the additional information. Thomas Fox-Brewster, *Google, Microsoft Still Waiting on Wikileaks to Deliver CIA Hacking Tools*, FORBES (Mar. 11, 2017), https://www.forbes.com/sites/thomasbrewster/2017/03/11/google-microsoft-waiting-on-wikileaks-cia-exploits/#75de475754c9 [https://perma.cc/3YJH-YF5N].

[18] Rajiv Gupta, *The Panama Papers Signal a New Kind of Cyber Attack*, FORTUNE (Apr. 9, 2016), http://fortune.com/2016/04/09/panama-papers-mossack-fonseca/ [https://perma.cc/45X3-B63G].

[19] Hacks violate multiple federal laws relating to computer crimes. For a full discussion of those crimes, see OFFICE OF LEGAL EDUC. EXEC. OFFICE FOR U.S. ATTORNEYS, PROSECUTING COMPUTER CRIMES: COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION CRIMINAL DIVISION (2010), https://www.justice.gov/sites/default/files/

was not involved in the illegal activity.[20] The constitutional protection stems from the "assumption that the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society."[21] While the products of the hacks fall squarely within that precedent, another reason hacks appeal to journalists is precisely because of a constitutional right that journalists do *not* enjoy: the right to protect the anonymity of their sources. In *Branzburg v. Hayes*, the Supreme Court held that the First Amendment confers to journalists no special right to protect the identity of confidential sources.[22] In the four decades since that decision, the press has had to rely on alternate methods to protect their sources, much to the dismay of First Amendment scholars.[23] In contrast, hacktivism at once provides journalists with massive amounts of newsworthy information as well as tools to protect the source's anonymity.[24]

These hacks also provide attorneys with enticing opportunities to comb through previously confidential files, but there is no constitutional protection for attorneys to review the illegally obtained files.[25] Imagine a scenario where an attorney represents a client in litigation against Sony for discrimination based on gender. After the publicized hack,[26] it would be tempting—and perhaps even required if the lawyer is to

---

criminal-ccips/legacy/2015/01/14/ccmanual.pdf [https://perma.cc/T9KY-FRUR]. For an analysis of current legislation governing data security, see William Stanton, Note, *Securing America's Data*, 83 BROOK. L. REV. __ (forthcoming 2018). Because of the increase in hacking, there are calls for additional legislation to make a wider range of activity unlawful. *See generally* Myra F. Din, Note, *Breaching and Entering: When Data Scraping Should Be a Federal Computer Hacking Crime*, 81 BROOK. L. REV. 405 (2015).

[20] Bartnicki v. Vopper, 532 U.S. 514, 535 (2001) ("[A] stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern.").

[21] Associated Press v. United States, 326 U.S. 1, 20 (1945).

[22] Branzburg v. Hayes, 408 U.S. 665, 685 (1972).

[23] Joel M. Gora, *The Source of the Problem of Sources: The First Amendment Fails the Fourth Estate*, 29 CARDOZO L. REV. 1399, 1404–05 (2008).

[24] For example, the hackers that exposed the Panama Papers communicated with journalists remotely, via encrypted messages. One commenter noted that "[t]his generation's Watergate will be conducted through shared folders." Gupta, *supra* note 18.

[25] Gentile v. State Bar of Nev., 501 U.S. 1030, 1073–74 (1991) (noting when acting in their professional capacity, lawyers do not have the same First Amendment rights as other citizens and "may be regulated under a less demanding standard than that established for regulation of the press").

[26] Hacks occur frequently, but not all are publicly disclosed. James R. Silkenat, *Keynote Address: Privacy and Data Security for Lawyers*, 38 AM. J. TRIAL ADVOC. 449, 450, 450–51 (2015). This note focuses on hacks that were publicly disclosed and extensively reported on.

"zealously assert[] the client's position"[27]—for the attorney to look through the hacked files for a smoking-gun email or memo that proves Sony's liability in the action. Indeed, the hypothetical attorney would find ample ammunition to use against Sony in the discrimination suit.[28] As ethics and evidentiary rules stand, however, it is not clear if an attorney may view leaked documents, let alone use them as evidence in litigation.

While American Bar Association (ABA) Model Rule 4.4(b) governs attorney conduct when in receipt of documents sent inadvertently, it is silent on attorneys in receipt of documents obtained illegally.[29] Coincidentally, this is the exact scenario facing an attorney in the event of a publicized hack and, because of the ABA's silence, the attorney must face it without clear guidance.[30] Nor is there a clear rule from the courts on the boundaries for attorneys when there is a publicized hack. When determining what documents litigants may admit as evidence in other contexts, such as when a disgruntled employee sends an adversary confidential files, some courts have precluded all use of documents and information obtained outside the normal discovery process.[31] Other courts have applied a test similar to the one applied to news organizations, holding that there is no basis for prohibiting the admission of stolen documents into evidence so long as the party receiving the documents was not involved in any illegal conduct in obtaining them and the documents are not protected by attorney-client privilege.[32]

The ethical dilemma is compounded for attorneys when the leaked documents are protected by attorney-client

---

[27] MODEL RULES OF PROF'L CONDUCT pmbl. para. 2 (AM. BAR ASS'N 1983) [hereinafter MODEL RULES].

[28] Hacked emails revealed, among other things, that Sony paid female executives and actresses less than their male counterparts. William Boot, *Exclusive: Aaron Sorkin Thinks Male Film Roles Have Bigger 'Degree of Difficulty' Than Female Ones*, DAILY BEAST (Dec. 15, 2014), http://www.thedailybeast.com/articles/2014/12/15/exclusive-sony-emails-reveal-why-aaron-sorkin-thinks-hollywood-has-a-women-problem.html [https://perma.cc/W7GC-EBRB].

[29] MODEL RULES, *supra* note 27, r. 4.4(b). As discussed *infra* Sections I.B and I.C, rule 4.4(b) does not provide guidance on what else the attorney in receipt of the file should do or whether or not the privilege is waived by the inadvertent disclosure.

[30] As discussed *infra* Section I.B, the ABA Committee on Ethics suggests that attorneys should give notice to opposing counsel and obtain a judicial ruling as to the admissibility of the document before even viewing it.

[31] *In re* Shell Oil Refinery, 143 F.R.D. 105, 109 (E.D. La. 1992) (stating that the plaintiffs could not make use of documents provided by one of the defendant's employees without authorization "unless the documents are publicly available or were previously produced by [Defendant]").

[32] Madanes v. Madanes, 186 F.R.D. 279, 292 (S.D.N.Y. 1999) ("Such a sanction would have no deterrent value since the punishment would fall on the blameless party rather than on the wrongdoer who may have no interest in the litigation. Moreover, the passive recipient of non-privileged material would be deprived of information to which she would otherwise be entitled through the discovery process.").

privilege. The privilege is a bedrock legal principle that protects a client from providing a court or adversary with confidential communications exchanged in the course of providing or receiving legal advice with an attorney, even if the communications are relevant to litigation.[33] The 11.5 million documents that comprise the Panama Papers came from a law firm, and thus it is almost certain that many of the documents fall within the scope of attorney-client privilege.[34] Aside from Podesta's tips on cooking risotto,[35] WikiLeaks also posted at least two legal memos written for the Clinton Foundation.[36] Both memos—clearly labeled "Attorney-Client Privilege"—were reported on by multiple news sites and were reposted in full on the *Washington Post*'s and the *Daily Caller*'s websites.[37]

Each of these increasingly all-too-predictable hacks, which make millions of documents available to anyone with an Internet connection, diminishes the attorney-client privilege protection. Attorney-client privilege is a pillar of the legal profession, and its members should go to great lengths to protect it.[38] But when privileged documents are posted online

---

[33] *See* Fisher v. United States, 425 U.S. 391, 403 (1976). How the privilege is established and its scope of protection is discussed *infra* Section I.A.

[34] Josh Gerstein, *Panama Papers Pose Ethics Issues for U.S. Prosecutors*, POLITICO (Apr. 6, 2016), http://www.politico.com/story/2016/04/panama-papers-ethics-issues-prosecutors-221609#ixzz45RD5dfLs [https://perma.cc/8PRK-D3NL].

[35] Virginia Chamlee, *Wikileaks: John Podesta's Emails Offer the Secret to Creamy Risotto*, EATER (Oct. 11, 2016), http://www.eater.com/2016/10/11/13246824/wikileaks-john-podesta-clinton-risotto [https://perma.cc/Y3WB-LLW5] (describing an email in which Podesta shares tips for making risotto).

[36] Rosalind S. Helderman & Tom Hamburger, *Inside 'Bill Clinton Inc.': Hacked Memo Reveals Intersection of Charity and Personal Income*, WASH. POST (Oct. 26, 2016), https://www.washingtonpost.com/politics/inside-bill-clinton-inc-hacked-memo-reveals-intersection-of-charity-and-personal-income/2016/10/26/3bf84bba-9b92-11e6-b3c9-f662adaa0048_story.html [https://perma.cc/LB4L-YAJF]; Richard Pollock, *BOMBSHELL: Clinton Foundation Donors Expected 'Benefits in Return for Gifts'*, DAILY CALLER (Oct. 14, 2016), http://dailycaller.com/2016/10/14/bombshell-clinton-foundation-donors-expected-benefits-in-return-for-gifts/ [https://perma.cc/25Z6-S3NT].

[37] One memo to the Clinton Foundation, written by Simpson Thatcher, & Bartlett LLP attorneys, summarized the results of a governance review and details the firm's interviews with the Clinton Foundation's board of directors and staff. Pollock, *supra* note 36. The other memo was written to "help clarify [the aide's] activities on behalf of the President—both on behalf of non-profit Foundation activities and the management of the [sic] his for-profit business opportunities." Doug Band, Teneo to Victoria Bjorklund, Jennifer Reynoso, Simpson Thatcher, President Bill Clinton, Clinton Foundation Founder et al., (Nov. 16, 2011), https://assets.documentcloud.org/documents/3183007/Memo-from-Bill-Clinton-aide-on-how-Teneo.pdf [https://perma.cc/5YNA-DEUE]. It is worth noting that, by virtue of writing this note, this author read the memo and is now citing directly to it, potentially encouraging more attorneys to view and read it. All this despite the memo's clear label that it is protected by attorney-client privilege.

[38] *See* Letter from James R. Silkenat, President of the Am. Bar Ass'n, to Gen. Keith B. Alexander, Dir. of the Nat'l Sec. Agency (Feb. 20, 2014), http://www.americanbar.org/content/dam/aba/uncategorized/GAO/2014feb20_nsainterceptionofprivilegedinfo_l.authcheckdam.pdf [https://perma.cc/ET6C-UE6T] (The president of the ABA wrote to the National Security Agency's Director and General Counsel

and are the subject of constant news coverage, is the claim of privilege ever so futile that a court should consider it implicitly waived?

With massive document leaks moving from rare to commonplace, courts and bar associations must provide clear parameters to guide attorneys in deciding whether they may ethically view or admit into evidence hacked documents that may be protected by attorney-client privilege. Part I of this note summarizes general rules that govern attorneys in receipt of unsolicited and potentially privileged documents, as well as factors that courts weigh when considering a party's claim of privilege, despite a document's inadvertent or unauthorized disclosure. Part II examines cases where litigants have argued to exclude stolen or hacked documents from ever appearing in court. Part III proposes that, in an age of hackers, courts should shift the burden of protecting privileged files from the receiver of the files to the party claiming the privilege. With these changes, lawyers will have clear notice as to the ethical and procedural boundaries in which they must operate when dealing with publicized hacks that may include privileged files. To accomplish this, ethics rules should permit attorneys to consume media coverage of publicized hacks and courts should determine whether the party claiming privilege took adequate cybersecurity precautions against the all-too-predictable hack. These changes would shift the burden to the party claiming privilege to demonstrate that the file or files remain confidential, despite the publicized hack.

I. CONCERNS FACING LAWYERS IN RECEIPT OF UNSOLICITED FILES

While corporations and individuals must grapple with how best to deal with the public relations nightmare of a publicized leak of sensitive information, attorneys interested in accessing the leaked files must navigate ethical dilemmas posed by the hack with no clear guideposts. Attorney-client privilege is not a constitutionally protected right; rather, it is an evidentiary rule that exists to protect the communications between a client and an attorney in the course of seeking and providing legal advice.[39] Note that the attorney-client privilege

---

requesting that procedures be put in place to prevent the erosion of the attorney-client privilege in the event that the government was surveilling attorney communications with clients.).

[39] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981). Note that the attorney-client privilege is separate and apart from an attorney's duty of confidentiality.

is separate and apart from an attorney's duty of confidentiality. An attorney's duty of confidentiality is governed by ABA Rule 1.6 and is a general ethics rule, not an evidentiary rule.[40] This note focuses on the ethics and evidentiary rules governing the scope of the privilege and that severely restrict an attorney's ability to view and use as evidence documents that are subject to privilege. A client's ability to refuse to disclose to an adversary confidential communications between him and his attorney has long been recognized as a vital rule that leads to "full and frank" discussions between the parties.[41] These "full and frank" discussions, the logic goes, result in more comprehensive and effective legal representation because the client is not worried that what he reveals to his attorney will later be used against him in litigation.[42] Because invoking the privilege limits otherwise discoverable materials, it is in tension with "the policy of broad disclosure" during litigation.[43] Thus, courts generally construe the scope of privilege narrowly "so that it applies *only* where confidentiality is deemed necessary to encourage consultation with a lawyer."[44]

As the Supreme Court noted in *Upjohn Co. v. United States*, "if the purpose of the attorney-client privilege is to be served, the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected."[45] Courts have been willing to adjust the contours of the privilege so long as the change furthers the underlying principles of candid disclosure when parties give and receive legal advice as well as efficient and accurate justice through broad disclosure of relevant evidence during litigation.[46] This era of hackers releasing sensitive documents to the public calls for courts to adapt how they apply the attorney-client privilege. The hacks themselves are eroding attorney and client confidence that their communications will remain confidential, not the post-hack fear that the documents may be used in litigation.

An attorney's duty of confidentiality is governed by ABA Rule 1.6 and is a general ethics rule, not an evidentiary rule. This note focuses on the ethics and evidentiary rules governing the scope of attorney-client privilege.

[40] MODEL RULES, *supra* note 27, r. 1.6.

[41] Mohawk Indus., Inc. v. Carpenter, 558 U.S. 100, 108 (2009).

[42] *See id.*

[43] David B. Smallman, *The Purloined Communications Exception to Inadvertent Waiver: Internet Publication and Preservation of Attorney-Client Privilege*, 32 TORT & INS. L.J. 715, 721 (1997).

[44] *Id.* (emphasis added).

[45] Upjohn Co. v. United States, 449 U.S. 383, 391 (1981). .

[46] Robert G. Clyne & Alexander P. Conser, *Attorney-Client Privilege and the Admiralty Practitioner in the Twenty-First Century*, 89 TUL. L. REV. 1179, 1202 (2015).

There are no uniform guidelines or rulings from the courts such that an attorney or client can predict whether particular communications will remain protected by privilege if they are posted on the Internet without the client's authorization. Moreover, the lack of guidance from bar associations and courts means that an attorney determining whether to view hacked files that are part of constant news coverage, some of which may be protected by privilege, cannot predict if ethics rule permit him to view the files. Until courts come up with a consistent rule for dealing with this increasingly common scenario, attorneys must work within the already established framework of ethical rules guiding the use of privileged documents.

A. Burden of Protecting the Attorney-Client Privilege

Attorney-client privilege is established when a client and attorney exchange communications in the course of providing legal advice.[47] There is a clear mandate for the holders of privilege to act competently to preserve confidentiality by appropriately "safeguard[ing] information relating to representation of a client against inadvertent or unauthorized disclosure."[48] In *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc.*, the district court articulated the standard for determining if a party took adequate precautions, finding that the paramount considerations are: "(1) the effect on uninhibited consultation between attorney and client of not allowing the privilege in these circumstances; and (2) the ability of the parties to the communication to protect against the disclosures."[49]

The second prong provides the grayest area in this inquiry due to the prevalence of technology in people's personal and professional lives. The party invoking privilege has the burden to show both that it intended the files to be confidential and that it "took all possible precautions" to keep them confidential.[50] This guidance is key in the age of hacks as it

---

[47] For a detailed discussion of each element needed to establish the privilege, see Daniel Northrop, Note, *The Attorney-Client Privilege and Information Disclosed to an Attorney with the Intention that the Attorney Draft a Document to be Released to Third Parties: Public Policy Calls for at Least the Strictest Application of the Attorney-Client Privilege*, 78 FORDHAM L. REV. 1481, 1485–91 (2009).

[48] MODEL RULES, *supra* note 27, r. 1.6 cmt. 18.

[49] Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 260 (N.D. Ill. 1981) (finding that case law, especially in "eavesdropper" cases, reveals that the relevant rule looks to whether the party invoking privilege intended to keep the communication confidential).

[50] United Mine Workers of Am. v. Arch Mineral Corp., 145 F.R.D. 3, 6 (D.D.C. 1992).

places the burden to take precautions not on the attorney viewing the leaked files but on the attorney and client who seek to protect the files.[51] But many ethics rules also place a burden on the attorneys in receipt of unsolicited files by requiring them to refrain from viewing the files "if there are 'obvious indications' that privileged documents were disclosed."[52] These rules serve to hold accountable both the party claiming privilege and the party in receipt of unsolicited files. Both parties must protect the privilege by taking adequate precautions against breaching the confidentiality of the communications. But, as discussed in Section III.A, it is impractical to place such a burden on the "receiving" party in the event of a hack.

B. Inadvertent Disclosure of Files Subject to Privilege

While attorney-client privilege dates back to the sixteenth century,[53] the advent of email communications has increasingly forced attorneys into the ethical quandary of "to view or not to view." Advances in technology have also greatly aided attorneys in efficiently receiving and viewing documents but have also provided a myriad of ways to send confidential and privileged documents to the wrong recipient. The Federal Rules of Evidence (Rules of Evidence) provide that an inadvertent disclosure does not automatically waive the claim of privilege if:

> (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26 (b)(5)(B).[54]

No evidentiary rule provides guidance for attorneys who receive files sent inadvertently and therefore they must look to

---

[51] There are traditional precautions available to indicate documents are privileged and thus protecting the claim of privilege, such as clearly marking files "Attorney-Client Privilege" and limiting distribution of the file to only the necessary parties. As discussed *infra* Section III.A, however, these traditional methods are rendered virtually meaningless after a publicized hack as thousands of citizens and journalists pour through documents, regardless of whether they are clearly marked as subject to attorney-client privilege or not.

[52] *See generally* Burke T. Ward et al., *Electronic Discovery: Rules for a Digital Age*, 18 B.U. J. SCI. & TECH. L. 150 (2012) ("The Advisory Committee . . . notes that under F.R.C.P. 26(b)(5)(B), a party does not have to review documents as they were produced to determine whether an inadvertent production occurred, but should review only to follow up if there are 'obvious indications' that privileged documents were disclosed.").

[53] PAUL R. RICE, ATTORNEY-CLIENT PRIVILEGE IN THE UNITED STATES § 1.1 (1993).

[54] FED. R. EV. 502(b).

other sources to guide their conduct. Attorneys can, however, look to ethics rules and the Federal Rules of Civil Procedure (Federal Rules) for such guidance. Additionally, when an attorney receives a document or email related to a client's case "and knows or reasonably should know that . . . [it] was inadvertently sent, [the attorney should] promptly notify the sender."[55] This ABA ethics rule, as explained in its accompanying formal opinion, covers such situations where an attorney attaches the wrong file to an email in error and sends to opposing counsel or where an attorney is mistakenly copied on emails between a third party and the third party's attorney.[56] In the discovery phase of litigation, Federal Rule 26 provides attorneys protection against inadvertent disclosure of privileged information during large document productions of electronically stored information (ESI). At the outset of discovery, in addition to withholding information that is privileged, the Federal Rules encourage parties to negotiate "quick peek" and "claw back" arrangements.[57] These arrangements allow the producing party to provide ESI while still preserving a claim of privilege even after the ESI has been sent to the requesting party.[58] The Supreme Court updated Rule 26 a decade ago in recognition of the need both for extensive discovery of electronic files and also the need to mitigate the risk of inadvertent disclosure of privileged files.[59] The rule allows litigants to provide documents first and invoke privilege later—to claw the privileged document back from an adversary—confident that a court will not find that the inadvertent disclosure waived the privilege. This rule serves to further the goal of broad discovery while also maintaining the confidentiality of files protected by privilege.

If parties have *not* negotiated such a "claw back" agreement, however, the Federal Rules still provide guidance on how litigants must proceed in the event of an inadvertent disclosure of privileged documents during discovery. The party claiming the privilege must notify the receiving party and

---

[55] MODEL RULES, *supra* note 27, r. 4.4(b) (emphasis added).

[56] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-440 (2006).

[57] N. Thomas Connally & Jon M. Talotta, *The New Federal Rules of Civil Procedure: What Every Corporate Counsel Should Know and Do* 3, ABA CORP. COUNSEL NEWSL. (Dec. 16, 2006), http://apps.americanbar.org/buslaw/newsletter/0056/materials/pp6.pdf [https://perma.cc/MYF6-4EH5].

[58] *Id.*

[59] John K. Villa, *Clawbacks, Quick Peeks, and Running with Scissors*, ACC DOCKET, Jan./Feb. 2007, at 82, https://www.wc.com/portalresource/lookup/poid/Z1tOl9NPluKPtDNIqLMRVPMQiLsSw43CmO3!/document.name=/Line%20312_PUBLICATION%20-%20Clawbacks,%20Quick%20Peeks%20and%20Running%20with%20Scissors.pdf [https://perma.cc/72P8-8BUA].

establish the basis for the claim of privilege.[60] Upon receipt of that notification, the receiving party must either return or destroy the information, refrain from using it in any way, and may request that the court rule on the claim of privilege.[61] The party claiming the privilege must also preserve the information until the court makes its determination.[62]

The Federal Rules and the ABA Ethics Rules serve to give attorneys guidance on how to proactively address common inadvertent disclosure situations. The party claiming privilege is motivated to take adequate precautions against disclosure of the files and to label files so their privileged status is readily apparent. The receiving party is obligated to notify and destroy or return, with the goal of restoring the privileged document to its original, confidential status. In the age of hacks, however, receiving attorneys are not faced with the choice of whether to open an attachment they think was sent to them in error. Instead, receiving attorneys are faced with the choice of reading the *Washington Post*'s coverage of a presidential election or not. A receiving attorney reading the *Washington Post* and subsequently notifying the owner of the privilege of the disclosure would be a fruitless exercise because the owner is likely already well aware of the hack due to widespread news coverage. Moreover, in those scenarios, there is generally no path back to restoring confidentiality, precisely because of the news coverage.[63] The point of these ethics and procedural rules—that the mistake of providing an opponent with privileged information may be avoided or minimized simply by notifying the other attorney to return to file—cannot and should not apply to a hack.

C. Unauthorized Disclosure of Files Subject to Privilege

Traditional guidelines from bar associations that govern an attorney's obligation are less clear when an attorney receives an "unauthorized" disclosure of files that might be protected by privilege. While inadvertent disclosures occur by mistake, unauthorized disclosures are made purposefully by third parties who do not have permission to share a file, such

---

[60] FED. R. CIV. P. 26(a)(5)(B).

[61] *Id.*

[62] *Id.*

[63] For example, while it is not public exactly how much traffic the Wikileaks documents received, the *Washington Post* article reporting on and linking to a legal memo sent to the Clinton Foundation received over 5200 comments from readers suggesting at least that many people read the article. Helderman & Hamburger, *supra* note 36; *see also supra* note 11 and accompanying text.

as disgruntled employees or hackers.[64] Most guidelines place the burden of protecting the confidentiality of the privileged communication on the receiving attorney. State bar association ethics rules vary from state-to-state[65] and are not on point for the increasingly relevant and prevalent situation of publicized hacks.

Bar association rules and opinions that govern attorney conduct when in receipt of potentially stolen documents do not logically apply to publicized hacks. For example, the D.C. Bar Association requires an attorney who receives a document that likely was taken without authorization to

> refrain from reviewing and using the document if: 1) its privileged status is readily apparent on its face; 2) receiving counsel knows that the document came from someone who was not authorized to disclose it; and 3) receiving counsel does not have a reasonable basis to conclude that the opposing party waived the attorney-client privilege with respect to such document.[66]

This rule makes sense if an attorney is currently engaged in litigation and receives files belonging to an adversary from an anonymous source or a disgruntled employee. In publicized hacks, however, documents stolen and released on the Internet are often marked as protected by attorney-client privilege, making their privileged status readily apparent on their face. Further, by definition, hackers are never authorized to disclose a company's files, and therefore the receiving attorney cannot conclude the hacked party waived the attorney-client privilege. Applying the D.C. Bar's Rule 1.15(b) to a publicized hack would require an attorney to refrain from reading widely circulated news reports on a hack. This is yet another example of how traditional ethics rules are woefully inept at guiding attorneys through the ethical minefield of publicized hacks.

---

[64] *See, e.g.*, D.C. Bar Legal Ethics Comm., Op. 318 (2002).

[65] *Compare* N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 700 (1998) ("Lawyer who receives unsolicited communication from former employee of adversary's law firm regarding alteration of documents may not communicate further with employee and should seek judicial guidance as to the use of the unauthorized communication."), *with* D.C. Bar Legal Ethics Comm., Op. 318, *supra* note 64 ("When counsel in an adversary proceeding receives a privileged document from a client or other person that may have been stolen or taken without authorization from an opposing party, Rule 1.15(b) requires the receiving counsel to refrain from reviewing and using the document if: 1) its privileged status is readily apparent on its face; 2) receiving counsel knows that the document came from someone who was not authorized to disclose it; and 3) receiving counsel does not have a reasonable basis to conclude that the opposing party waived the attorney-client privilege with respect to such document.").

[66] D.C. Bar Ethics Comm., Op. 318, *supra* note 64.

The ABA's Standing Committee on Ethics and Professional Responsibility (ABA Committee on Ethics) provides no guidance on appropriate steps in the event of an attorney receiving files sent without authorization. In 2011, the ABA Committee on Ethics explained that Model Rule 4.4(b) and its notice requirement apply only to inadvertent disclosures from opposing counsel.[67] While the ABA Committee on Ethics acknowledged that there might be laws that preclude a receiving attorney from retaining files sent without authorization, it stated explicitly that the issue was "a matter of law beyond the scope of Rule 4.4(b)."[68] This is the exact scenario an attorney is faced with in the event of a publicized hack, and the ABA Committee on Ethics dodged providing attorneys with guidance on the issue. Instead, it noted that it may still be in the lawyer's "best interest to give notice [to opposing counsel] and obtain a judicial ruling as to the admissibility of the . . . attorney-client communications before attempting to use them, and if possible, before the . . . lawyer reviews them."[69]

In short, the ABA Committee on Ethics suggests that attorneys faced with a now common ethical dilemma—reading a *Washington Post* article quoting and linking directly to a legal memo from the Clinton Foundation[70]—head to the courts for a judicial ruling on the issue. While perhaps an attorney already engaged in litigation may efficiently seek a judicial ruling on situations involving privileged documents,[71] requesting that attorneys refrain from reading certain news articles until a court may rule is not practical.

A practical and predictable rule is sorely needed in this area, for attorneys risk serious consequences if a court finds that they improperly reviewed files protected by attorney-client privilege. In *Castellano v. Winthrop,* a mother who was engaged in ongoing litigation with the father of her children

---

[67] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-460 (2011) ("[T]his Committee found that Rule 4.4(b) *does not obligate a lawyer to notify a lawyer to notify opposing counsel* that the lawyer has received privileged or otherwise confidential materials of the adverse party from someone who was not authorized to provide the materials, if the materials were not provided as 'the result of the sender's inadvertence.'" (emphasis added) (citing ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-442 (2006))).

[68] *Id.*

[69] *Id.*

[70] *See supra* note 37 and accompanying text.

[71] *See* Gomez v. Vernon, 255 F.3d 1118, 1135 (9th Cir. 2001) ("The result here does not set up an impractical or insurmountable hurdle for counsel facing an ethical dilemma concerning privileged documents. The path to ethical resolution is simple: when in doubt, ask the court.").

illegally obtained his flash drive, which contained thousands of documents.[72] The mother then retained a law firm, whose attorneys then spent over one hundred hours reviewing the files on the flash drive, some of which were subject to attorney-client privilege.[73] Upon discovering that the firm was going through the flash drive, the father's counsel filed an emergency petition to order the return of the flash drive and request the dismissal of the firm from the action.[74]

The trial court ordered a seal of the information from the flash drive placed in the court file.[75] The court further indemnified the father against any damages he might suffer from the improper use of the files contained on his flash drive.[76] The trial court also disqualified the firm from the action because it obtained "an informational advantage."[77] In upholding the order, the Court of Appeals for Florida cited the Florida Bar Commission on Professional Ethics covering what an attorney must do when he receives confidential files he knows or should know were obtained illegally.[78] This case illustrates the quandary facing attorneys after a publicized hack of an adversary: read news articles reporting on the contents of your opponent's privileged files at the risk of ultimately being disqualified from your litigation.

D. Waiver of Privilege

Even if a document or communication is protected by attorney-client privilege, a court may determine that the privilege has been "waived." A finding of express or implied waiver precludes a client from refusing to disclose files by invoking the privilege.

Though express waiver of privilege is rare,[79] it occurs when:

> [A] party discloses privileged information to a third party who is not bound by the privilege, or otherwise shows disregard for the privilege by making the information public. Disclosures that effect an express waiver are typically within the full control of the party holding the privilege.[80]

---

[72] Castellano v. Winthrop, 27 So. 3d 134, 135 (Fla. Dist. Ct. App. 2010).
[73] *Id.*
[74] *Id.*
[75] *Id.* at 136.
[76] *Id.*
[77] *Id.* (internal quotations omitted).
[78] *Id.* at 137.
[79] RICE, *supra* note 53, § 9.24.
[80] Bittaker v. Woodford, 331 F.3d 715, 719 (9th Cir. 2003).

A court is unlikely to find an express waiver of privilege in the case of a hack because the documents that hackers release are no longer "within the full control of the party holding the privilege."[81] Moreover, an express waiver of privilege is unlikely to occur unless the corporation or individual states that he is waiving privilege in order to address allegations or accusations about contents of the files in question.[82] When determining whether files released and widely disseminated by hackers are still protected by privilege, courts should consider whether the party claiming privilege utilized sufficient precautions against a hack such that the privilege is not implicitly waived.

While privilege is deemed waived if a client purposefully discloses a file protected by privilege, there is no consensus on whether the attorney-client privilege is automatically waived by an inadvertent or unauthorized disclosure.[83] Under some circumstances, the simple failure to keep a file confidential—regardless of the circumstances of its disclosure—is deemed a waiver of the privilege.[84] While other courts look to whether disclosure of the file was unintentional or inadvertent before determining whether the party waived privilege,[85] many courts do not bother with that distinction. In an attempt to deter the use of stolen documents, those courts have stated there is no waiver of privilege if privileged communications are disclosed by a third party with no authorization.[86]

Courts have examined scenarios in which parties have left privileged documents in locations that were obviously vulnerable to third party access and have found an implicit waiver of attorney-client privilege.[87] A court might consider public

---

[81] *Id.*

[82] But see *infra* notes 99–110 and accompanying text for a discussion of how a party's conduct after a hack may risk a court finding an express waiver due to the disclosure of the contents of a legal memo.

[83] Gloria A. Kristopek, *To Peek or Not to Peek: Inadvertent or Unsolicited Disclosure of Documents to Opposing Counsel*, 33 VAL. U. L. REV. 643, 653 (1999).

[84] *See, e.g.*, Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 257 (N.D. Ill. 1981).

[85] *See, e.g.*, *id.*

[86] Smallman, *supra* note 43, at 728 ("These rulings appropriately protect clients' expectations of confidentiality when communicating with their attorneys, discourage the theft of privileged material, and preserve the integrity of the judicial process, particularly if there is a suspicion that the theft was undertaken either at the direction of or with the encouragement of a litigation adversary.").

[87] The scenarios center around what sort of access third-parties have to the privileged documents:

> When the client leaves privileged documents in a place where third parties have access to them, courts have held that their privilege status is destroyed. Thus, storing documents in a place accessible to third parties without taking

comments by Sony's Executive Director of Information that it was a "valid business decision to accept the risk of a security breach"[88] in deciding whether Sony's knowing acceptance of risk results in a waiver of the attorney-client privilege for any legal memos that were hacked and posted on the Internet. Thus, as discussed in Section III.A, concrete and substantial technological protections against cybersecurity breaches must be at the top of every company's list of priorities, especially given how frequent and publicized these hacks have become.[89]

When it was first clear that email was not a fad, courts and legal commentators alike acknowledged "that technological advancements exist against which 'no easily available protection exists.'"[90] That argument is now outdated.[91] Email and intranet use are no longer a novelty in the workplace and

---

> any measures to maintain their confidentiality waives the privilege. Similarly, privilege is waived when clients leave papers in a public hallway for delivery to the attorney or on a table in a hotel room occupied by other people. Waiver also results when documents are kept in files that are routinely viewed by third parties, including potentially when email files are kept on a monitored server. Additionally, waiver has been found where electronic storage devices containing privileged documents are sold or conveyed to a third party without removing the documents. Moreover, a client's disposal of privileged documents into a waste paper basket that was then emptied into a dumpster, from which the documents were salvaged by a third party, also destroyed the privilege.

RICE, *supra* note 53, § 9.25 (footnotes omitted).

[88] Andrea Peterson, *Why It's So Hard to Calculate the Cost of the Sony Pictures Hack*, WASH. POST (Dec. 5, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/05/why-its-so-hard-to-calculate-the-cost-of-the-sony-pictures-hack/?utm_term=.548c098061a8 [https://perma.cc/SK7F-J5FJ].

[89] A leading treatise of attorney-client privilege notes that new technologies pose new questions about what steps are deemed "reasonable" enough to protect privileged files:

> Recent issues in cybersecurity have potentially called into question what steps are reasonably required to prevent third parties from accessing privileged communications that are stored in a virtual environment. For example, recent reports associated with Edward Snowden, who leaked thousands of classified documents, detail government monitoring of privileged electronic communications between law firms and clients. Similar reports have uncovered widespread government monitoring of certain private email accounts. The courts have not yet weighed in on what effect, if any, this should have in the privilege realm, although any heightened standard for ensuring confidentiality could inhibit the flow of communication between lawyer and client, diminishing the benefit of the privilege.

RICE, *supra* note 53, § 9.25 (footnotes omitted).

[90] Smallman, *supra* note 43, at 725.

[91] *See* Lois D. Mermelstein, *Ethics Update: Lawyers Must Keep Up with Technology Too*, BUS. LAW TODAY, http://www.americanbar.org/publications/blt/2013/03/keeping_current.html [https://perma.cc/P4CC-3PFN]; *14 States Now Require Lawyers to Keep Up with New Technology*, ANAQUA (May 7, 2015), http://www.anaqua.com/learn/anaqua-perspectives/14-states-now-require-lawyers-keep-new-technology [https://perma.cc/3FUA-ER4D].

password protection alone is woefully insufficient security against hackers.[92] As more of these breaches happen and affect litigation, courts must look at precautions taken in determining if a party made a good faith attempt to protect against a hack.

II. ATTORNEY-CLIENT PRIVILEGE IN ACTION

A. Traditional Application

When litigants seek judicial rulings on the validity of a claim of privilege, courts consider the factors that led to the document's disclosure as well as any indications that the party claiming privilege waived the claim. As discussed in Part I, courts determine the validity of a claim with the goal of encouraging candid conversations between a client and his attorney. If a document has been disclosed, inadvertently or without authorization, courts can attempt to repair the damage to the document's confidential status in several ways, primarily through restricting the use of the document at trial.[93]

The remedy of restricting the use of a privileged document in a court proceeding serves to bolster a client's confidence—both a client engaged in litigation and a client communicating with an attorney for the first time—in the confidentiality of attorney-client communications. The remedy does this by ensuring that if a communication is revealed to an adversary, the court may properly stop the adversary from admitting the files into evidence. But first, the party claiming privilege must demonstrate that he did not waive the privilege.

A court will determine whether or not the party invoking privilege took proper precautions against disclosure of the document. In *Carda v. E.H. Oftedal & Sons*, the district court evaluated a party's claim of privilege when the plaintiff moved to exclude from admission as evidence a letter that was accidentally produced during discovery.[94] The plaintiff had provided his adversary a CD with files as part of discovery,

---

[92] "[I]n 2016 it now appears unreasonable to expect that simply utilizing a password provides any practical protection." United States v. Matish, 193 F. Supp. 3d 585, 619 (E.D. Va. 2016) (citing Caitlin Dewey, *It's Been Six Months Since the Ashley Madison Hack. Has Anything Changed?*, WASH. POST (Jan. 15, 2016), https://www.washingtonpost.com/news/the-intersect/wp/2016/01/15/its-been-six-months-since-the-ashley-madison-hack-has-anything-changed/ [https://perma.cc/U2KK-CSRJ].

[93] Smallman, *supra* note 43, at 728. A court can deem documents inadmissible, order that an attorney cannot question a party from whom the document was stolen about the document, and generally prohibit the use of the document or its contents in the litigation. *Id.*

[94] Carda v. E.H. Oftedal & Sons, CIV. 04-5036-KES, 2005 U.S. Dist. LEXIS 26368, at *4 (D.S.D. Apr. 28, 2005).

some of which he argued were sent inadvertently and should be excluded as evidence because they were protected by attorney-client privilege.[95] The court denied the motion to exclude a letter the plaintiff sent to his attorney, finding that the party waived the privilege because "carelessness with privileged material [is treated] as indication of waiver."[96] The court found that a cursory review of file names on the CD could have "easily" prevented the disclosure.[97]

Beyond adequate security precautions, courts also look to the actions of the parties claiming privilege *after* documents are released into the public domain. In *Dukes v. Wal-Mart Stores*, an unnamed source leaked a copy of a memo written by the law firm Akin Gump Strauss Hauer & Feld LLP to the *New York Times*.[98] The *New York Times* did not publish the Akin Gump memo but did "report several findings contained in the Memo" in articles published both online and in print versions of the newspaper.[99] The article included comments from a Wal-Mart spokesperson who was quoted "as having responded that the company considered the Memo 'confidential and privileged.'"[100] Wal-Mart, Akin Gump's client and the defendant in the lawsuit, alerted the plaintiffs that the *New York Times* was going to report on the memo and explained that it still maintained its claim that privilege protected the file and the disclosure of the memo was not authorized.[101]

Eight months after the article was reported by the news, plaintiff's counsel received an envelope with no return address.[102] Inside the envelope was a document on Akin Gump letterhead that was marked "PRIVILEGED & CONFIDENTIAL . . . DO NOT REPRODUCE WITHOUT THE EXPRESS CONSENT OF LESTER C. NAIL."[103] The receiving attorney suspected that it was the leaked document, did not read it, and informed

---

[95] *Id.*

[96] *Id.* at *10 (quoting Gray v. Bicknell, 86 F.3d 1472, 1484 (8th Cir. 1996)).

[97] *Id.* at *9–10.

[98] Dukes, v. Wal-Mart Stores, Inc., No. 01-cv-2252 CRB (JSC), 2013 WL 1282892, at *2 (N.D. Cal. Mar. 26, 2013).

[99] *Id.* at *1; *see* Steven Greenhouse, *Report Warned Wal-Mart of Risks Before Bias Suit*, N.Y. TIMES (June 3, 2010), http://www.nytimes.com/2010/06/04/business/04lawsuit.html [https://perma.cc/72AH-2JLR]. This is in contrast to the Clinton memorandum, discussed *supra* note 37, which was posted in its entirety by the *Washington Post* and the *Daily Caller*.

[100] *Dukes*, 2013 WL 1282892 at *2. As discussed *infra* Section III.A, Wal-Mart's comment to the newspaper should be considered as an attempt to still protect the privilege of the document and thus the court should not find any explicit waiver of privilege.

[101] Dukes, 2013 WL 1282892 at *2.

[102] *Id.*

[103] *Id.* at *3.

defendant's counsel of his receipt of the document.[104] As the ABA suggests in this situation,[105] the parties went to court to decide whether or not plaintiffs could keep and use the memo "however they [saw] fit."[106]

The court evaluated the precautions taken by Wal-Mart before the leak of the memo to the *New York Times*[107] and held that the disclosure of the memo to the newspaper did not automatically waive the document's privileged status.[108] The court also rejected plaintiff's argument that Wal-Mart's public comments on the memo, which were quoted in the article, destroyed the privilege because the comments were made "extrajudicially and without prejudice to the opposing party, [and thus] there exists no reason in logic or equity to broaden the waiver beyond those matters actually revealed."[109] The court ultimately ruled that the memo was still protected by the attorney-client privilege because Wal-Mart took reasonable precautions to keep the memo confidential and its comments after the leak did not constitute a waiver.[110]

In contrast to *Dukes*, where there were only reports of the leaked memo's contents in the news, courts have considered whether privileged documents were widely available to the public in its evaluation of an attorney-client privilege claim. For example, in *Bible v. United Student Aid Funds, Inc.*, USA Funds filed a motion to strike certain paragraphs and exhibits from the opposing party's pleadings.[111] The information in the pleadings came from documents that were improperly disclosed in a wholly unrelated litigation and subsequently uploaded to Wikileaks.[112] Though uploaded to Wikileaks in violation of a court order in the unrelated litigation, the plaintiff obtained the documents legally from a publicly available online source, which had hosted the documents in question for more than five

---

[104] *Id.* at *2–3.

[105] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-440 (2006).

[106] *Dukes*, 2013 WL 1282892 at *8.

[107] The Court noted the all-caps lettering designating the memo confidential and privileged, the limited number of copies available of the memo (five total), and the fact that each copy was individually numbered on the cover. *Id.* at *3.

[108] *Id.* at *6.

[109] *Id.* at *8 (internal quotations omitted) (quoting *In re* von Bulow, 828 F.2d 94, 103 (2d Cir. 1987)).

[110] *Id.* at *3, 6. This situation is distinguishable from the more recent hacks, as discussed *infra* Part III.

[111] Bible v. United Student Aid Funds, Inc., No. 1:13-CV-00575-TWP, 2014 WL 1048807, at *3 (S.D. Ind. Mar. 14, 2014), *rev'd and remanded*, 799 F.3d 633 (7th Cir. 2015), *reh'g denied*, 807 F.3d 839 (7th Cir. 2015), and *cert. denied*, 136 S. Ct. 1607, 195 L. Ed. 2d 241 (2016).

[112] *Id.* at *3–4.

years.[113] The court noted its inability to limit access to the publicly available documents, finding Ms. Bible part of "the 'constantly expanding universe' of people who would have access to the documents online as a result of the original breach of the protective order."[114] The court further noted that it did not have effective power to limit the distribution of such publicly available files.[115]

In *Brown & Williamson Tobacco Corp. v. Regents of the University of California*, the court justified finding the privilege was extinguished and any court order to require the return of the files inappropriate, because "it is simply too late . . . [t]he genie is out of the bottle. The documents are out."[116] Even though a third party stole the privileged documents, the court found that the documents had become part of the public domain and any attempt to order the documents returned to Brown & Williamson would be futile.[117] Both *United Student Aid Funds* and *Brown & Williamson Tobacco Corp.* demonstrate a trend of courts looking to the "futility" of precluding attorneys from using privileged documents in litigation once the documents have been widely disseminated or reported on despite the privileged status.

B. In re Ashley Madison

In 2016, a court heard a case arising directly out of a publicized hack. Initially, the group responsible for the Ashley Madison hack, Impact Team, released just a small portion of the data it had hacked from the dating website.[118] Impact Team did so, they said in a statement, in an effort to blackmail Avid Life Media, the owner of Ashley Madison.[119] As the motive for the hack, the group cited Ashley Madison's policy of charging users a fee to scrub their accounts from the site without actually deleting any accounts.[120] When Avid did not shut down the site, Impact Team released almost ten gigabytes of compressed data, basically every document stored on Avid's

---

[113] *Id.*

[114] *Id.* at *4.

[115] *Id.*

[116] Brown & Williamson Tobacco Corp. v. Regents of the Univ. of Cal., No. 967298, at *4 (May 25, 1995).

[117] *Id.*

[118] Victor, *supra* note 3.

[119] *Id.* There was speculation that North Korea hacked Sony out of revenge for the release of *The Interview*. Biddle, *supra* note 2.

[120] Grandoni, *supra* note 15.

servers.[121] In addition to individual user data, researchers also found "huge numbers of internal documents, memos, org charts, contracts, sales techniques, and more."[122]

Impact Team released an unapologetic message to the Ashley Madison users whose identities it revealed online: "Find yourself in here? . . . It was [Avid] that failed you and lied to you. Prosecute them and claim damages. Then move on with your life. Learn your lesson and make amends. Embarrassing now, but you'll get over it."[123]

A group of users took the advice and sued Avid in federal court.[124] Despite the plaintiffs' assurance that they would not use "any of the original documents leaked in the data breach," Avid moved to have the court preclude plaintiffs' use of "news articles discussing, and in some cases, quoting those documents."[125] The court granted Avid's motion, finding that "the fact that the content of some of Avid's internal documents . . . has been to some extent placed on the internet and reported in news articles does not change the nature of the documents . . . [t]hey remain stolen documents."[126] The court was not persuaded by the plaintiffs' argument that they would not use the original documents marked as protected by attorney-client privilege or that documents were widely available online.[127]

This ruling provides broad protection for a company who finds itself the victim of a hack, but it directly contravenes the goal of broad file disclosure during litigation and candid conversation between attorneys and clients. The ruling limits the ability of litigants to use information that was widely disseminated and discussed nationally, at the expense of their case, without actually providing any deterrent to hackers.

---

[121] Tim Schiesser, *Data from Ashley Madison Hack Released in Massive 10 GB Dump*, TECHSPOT (Aug. 19, 2015), http://www.techspot.com/news/61808-data-ashley-madison-hack-released-massive-10-gb.html [https://perma.cc/B28J-53N7].

[122] Dan Goodin, *Ashley Madison Hack Is Not Only Real, It's Worse than We Thought*, ARS TECHNICA (Aug. 19, 2015), http://arstechnica.com/security/2015/08/ashley-madison-hack-is-not-only-real-its-worse-than-we-thought/ [https://perma.cc/3NNA-TR94].

[123] Bennett, *supra* note 3.

[124] *In re* Ashley Madison Customer Data Sec. Breach Litig., No. MDL No. 2669, 2016 U.S. Dist. LEXIS 57619 (E.D. Mo. Apr. 29, 2016).

[125] *Id.* at *9.

[126] *Id.* at *19. The fact that the documents were stolen was the most important factor to the court, not the documents' dissemination online or any document's privileged status. *Id.* at *19–20.

[127] *Id.* at *19.

III. EVALUATING PRIVILEGE IN THE AGE OF HACKERS

Predictability and practicality must always be key considerations of courts in determining whether a document continues to be protected by attorney-client privilege after a publicized hack. People should be extremely wary of what they include in electronic communications, knowing that they may one day be part of a subpoena or, worse, released on the Internet by vindictive hackers.[128] That companies are hacked is now predictable, but how courts evaluate a claim of privilege after the file has been released to the public by a hacker is anything but. While attorneys may be subject to greater ethical obligations than non-attorneys,[129] courts must apply the attorney-client privilege protection practically after a hack.

As discussed in Part I, the evidentiary rule of attorney-client privilege exists to encourage candid discussions between a client and his attorney[130] but is in tension with the broad disclosure of files relevant to litigation.[131] A court that restricts the use of documents that have been the topic of national news coverage serves neither the policy of broad disclosure during litigation nor the encouragement of candid discussions between clients and attorneys.[132] Hackers are destroying confidence that *any* communication may remain confidential, let alone a privileged communication. Indeed law firms are specifically targeted *because of* the sensitive information they hold.[133] Moreover, for the privilege to encourage candid conversations, courts' application of the privilege "must be clear and

---

[128] *See* Ken Broda-Bahm, *Dance Like No One Is Watching; Email Like It May One Day Be Read Aloud in a Deposition*, PERSUASIVE LITIGATOR (July 28, 2016), http://www.persuasivelitigator.com/2016/07/dance-like-no-one-is-watching-email-like-it-may-one-day-be-read-aloud-in-a-deposition.html [https://perma.cc/6ZRR-FWQJ]. In 2016 alone, hackers released emails from the Democratic National Committee, political operative Donna Brazile, and former Secretary of State Colin Powell. *Id.*; Dylan Byers, *Donna Brazile Out at CNN Amid Leaks to Clinton Campaign*, CNN MONEY (Oct. 31, 2016), http://money.cnn.com/2016/10/31/media/donna-brazile-cnn-resignation/ [https://perma.cc/TDW8-7HD7]; *The Emails in Which Colin Powell Slams Hillary Clinton and Donald Trump*, CBS NEWS, http://www.cbsnews.com/media/5-emails-in-which-colin-powell-slammed-hillary-clinton/ [https://perma.cc/C9SY-MVZE] (last updated Sept. 14, 2016).

[129] *See* Gentile v. State Bar of Nev., 501 U.S. 1030, 1073–74 (1991).

[130] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

[131] Smallman, *supra* note 43, at 721 and accompanying text.

[132] *See supra* Part I for a full discussion of these policies.

[133] *See also* Sara Randazzo & Dave Michaels, *U.S. Charges Three Chinese Traders with Hacking Law Firms*, WALL ST. J. (Dec. 27, 2016), http://www.wsj.com/articles/u-s-charges-three-chinese-traders-with-hacking-law-firms-1482862000 [https://perma.cc/9FA2-G99G] (Prosecutors stated that five law firms were targeted by hackers 100,000 times between March and September 2015.).

consistent."[134] Based on the current ethics rules and opinions, discussed in Part I, and the current body of case law, discussed in Part II, it is anything but clear how a court would rule on an attorney viewing a hacked file or admitting it into evidence. This critical predictability is currently missing in the age of hacking and must be addressed by the courts while furthering the goals of litigation and attorney-client privilege.

Courts should look to whether the party claiming privilege had adequate cybersecurity to prevent against hacks and whether the party's actions after the hack indicate an implicit waiver. Even if the party had adequate cybersecurity and did not implicitly waive privilege after the hack, courts should still place the burden on that party to demonstrate that the file remains confidential, despite the hack. Confidentiality is a key component of the attorney-client privilege and if a file becomes a topic of national conversation, permitting a party who was hacked to invoke privilege would be futile and go against the court's interest in broad disclosure of information during litigation.

A. Shifting the Burden of Protecting Privileged Files in the Age of Hackers

Ethics rules should not place the burden on attorneys—who had no involvement in illegal activity and who merely visit a news organization's website—to protect the attorney-client privilege of an opposing party after a publicized hack. As discussed in Sections I.B and C, current ethics rules place the burden on attorneys in receipt of unsolicited files to act to

---

[134] RICE, *supra* note 53, at § 2.3; *see also In re* Grand Jury Investigation, 599 F.2d 1224, 1235 (3d Cir. 1979) ("[W]e agree with the majority view that the incentive to confide is at least partially dependent upon the client's ability to predict that the communication will be held in confidence."); Berg Elecs., Inc. v. Molex, Inc., 875 F. Supp. 261, 262 (D. Del. 1995) ("If we intend to serve the interests of justice by encouraging clients to consult with counsel free from the apprehension of disclosure, then courts must work to apply the privilege in ways that are predictable and certain. . . . An uncertain privilege is a privilege that is little better than no privilege at all." (internal citation omitted)). *But see* Mohawk Indus. v. Carpenter, 558 U.S. 100, 109–10 (2009) (The Supreme Court denied a request for an immediate appeal to an order compelling the disclosure of information which the appellant claimed was protected by privilege. In denying the claim, the Court said that postponing an appellate review of the order "does not meaningfully reduce the *ex ante* incentives for full and frank consultations between clients and counsel." Because, among other reasons, "clients and counsel are unlikely to focus on the remote prospect of an erroneous disclosure order, let alone on the timing of a possible appeal." While the Court may have had sound reasoning in applying its rules on interlocutory appeals, it did not further the purpose of privilege's protection of candid conversations between attorneys and clients for the decision does not promote predictability on how courts evaluate claims of privilege.).

protect the confidentially of the files protected by privilege. The ethics rules require attorneys who "know[] or reasonably should know that" the files were sent inadvertently or without authorization to not read the files and to notify the sender.[135] Ethics rules guiding attorneys in receipt of files they suspect might be stolen place an even greater burden on the receiving attorney. While ethics rules vary depending on the state and scenario, many require attorneys in receipt of privileged files they reasonably believe were sent without authorization to notify opposing counsel, refrain from reading, and even obtain a judicial ruling on what further actions to take.[136] These ethics rules are not practical where the confidentiality of a privileged document no longer exists as a result of a hack dominating news cycles. Bar associations should revise ethics rules to reflect this new scenario.

An ethics rule proscribing attorneys from visiting the hacker's website *directly* to view potentially privileged files would permit attorneys to read news coverage of the files while at the same time limit them from combing through the millions of illegally obtained files of a potential adversary.[137] Such a rule recognizes that once a hack occurs, thousands of files may be available to the public but attorneys must still adhere to ethical rules that govern the legal profession.

Certainly, courts may rightly be concerned that allowing attorneys to look through illegally obtained files just because they are posted online might encourage more hacks of confidential information.[138] Just as the Supreme Court in *Bartnicki v. Vopper* found it unacceptable to punish a news organization for publishing illegally obtained documents, so too should ethics rules and court rulings acknowledge that punishing attorneys who were not involved in the illegal act to be unacceptable. In *Bartnicki,* the Court acknowledged that criminalizing third parties that publish illegally obtained documents might minimize the harm of the illegal act but

---

[135] *See supra* notes 55–56 and accompanying text.

[136] *See supra* Section I.C.

[137] For example, it would prevent attorneys acting on behalf of the U.S. government from seeking evidence of tax evasion from the illegally hacked Panama Papers instead of through its normal investigation procedures. In 2016, the U.S. Attorney for the Southern District of New York opened a criminal investigation into tax evasion and reached out to the media companies in possession of the Panama Papers, the inference being his office wanted to obtain files from the Panama Papers to use in the investigation. Rupert Neate, *Panama Papers: US Launches Criminal Inquiry into Tax Avoidance Claims*, GUARDIAN (Apr. 19, 2016), https://www.theguardian.com/business/2016/apr/19/panama-papers-us-justice-department-investigation-tax-avoidance [https://perma.cc/KQ9R-8B6W].

[138] *See supra* Section II.B.

ultimately found that the means of minimization were not acceptable.[139] The Court noted that "[t]he normal method of deterring unlawful conduct is to impose an appropriate punishment on the person who engages in it."[140] Proscribing attorneys from visiting the illegal source of files but permitting them to view news reports on the files, adds an additional layer of separation between the attorney and the illegal act. Further, such a rule would also recognize the impracticability of requiring attorneys to refrain from viewing files protected by privilege despite widespread dissemination and news coverage of such files.

There are additional steps that lawyers, individuals, and corporations alike should take before and after a hack to protect both confidential and privileged documents. In the context of determining whether or not a file may be admitted into evidence despite a claim of privilege, courts should place the burden on victims of such hacks to demonstrate that they took adequate precautions, suitable to the digital age, to protect against any waiver of attorney-client privilege. Traditional methods of marking a document as confidential and limiting its distribution are insufficient to protect attorney-client privilege in the twenty-first century. Attorneys specifically must also keep abreast of the benefits and risks of technology they use in their practice.[141]

It is inexcusable for attorneys and clients not to update their methods for protecting privilege to meet twenty-first century realities. New technologies and hackers, as a former president of the ABA stated, mean that "a single click by one employee, one lawyer in your office, can mean the difference between being hacked and staying secure. That should make all [attorneys] nervous."[142] Just as courts have found that leaving a physical file unguarded may lead to a waiver of privilege, so too should courts consider whether inadequate cybersecurity might constitute a waiver.[143] Courts should find

---

139 Bartnicki v. Vopper, 532 U.S. 514, 529 (2001).

140 *Id.*

141 American Bar Association Commission on Ethics 20/20 issued a new comment to Rule 1.1, requiring lawyers to keep abreast of the benefits and risks of technology they use in their practices. MODEL RULES, *supra* note 27, r. 1.1 cmt 8 ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . . .").

142 Silkenat, *supra* note 26, at 459.

143 *See, e.g.,* Peterson, *supra* note 88 ("Sony Pictures' internal approach to security may have contributed to the devastating nature of the attack."); Matt Burgess & James Temperton, *The Security Flaws at the Heart of the Panama Papers*, WIRED (Apr. 6, 2016), http://www.wired.co.uk/article/panama-papers-mossack-fonseca-website-

that cybersecurity that fails to adapt and meet the increased risk of hacks results in an implicit waiver of privilege.

There is no shortage of online resources outlining best practices for maintaining the security of a company's files.[144] Techniques for ensuring that documents protected by privilege remain confidential may include encryption of files and active monitoring of file systems.[145] Since technology evolves and sophisticated hackers find ways around cybersecurity, attorneys and clients must continue to examine and update the security systems they have in place.[146] Parties should be able to demonstrate to courts their policies for and assessment of cybersecurity as well as user training and education.[147]

In evaluating a claim of privilege after a hack, courts should consider whether the cybersecurity practices taken *before* a hack were sufficient to reasonably protect against a hack of privileged files. To win a claim of privilege after a hack, the party claiming the privilege should not have to demonstrate that they went above and beyond in their security measures—though, of course, for a variety of other compelling reasons they may want to.[148] Rather the party should demonstrate that they did the minimum to protect their documents. As is standard practice for physical files, they need not show that they had a security guard stationed outside of file cabinets, just that they were not careless.

Additionally, courts should look to actions taken *after* a hack when evaluating whether a party has implicitly waived privilege. Though it may be a fruitless endeavor, after a hack, attorneys should still send requests to websites and news

---

security-problems [https://perma.cc/GPP6-HBLR] ("The front-end computer systems of Mossack Fonseca are outdated and riddled with security flaws, analysis has revealed.").

144 *See generally* CONG. SMALL BUSINESS COMM., CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS, https://smallbusiness.house.gov/uploadedfiles/2_internet_of_things.pdf [https://perma.cc/P94E-NMQM]; JILL RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS (2013). It is worth noting as well that, while technology cannot be avoided in twenty-first century business, some executives avoid using email for important conversations out of fear of a hack. Oran, *supra* note 14.

145 Silkenat, *supra* note 26, at 457–58.

146 *Id.* at 460.

147 *See, e.g., id* at 458. ("Concrete steps must be taken by law firms moving forward if they are to practice law in this age of hackers and surveillance. Talking a good game is not good enough anymore.").

148 The majority of small businesses go out of business following a hack. Ted Knutson, *New Cybersecurity Aids for Small Businesses Posted Online by Congress*, FIN. ADVISOR (Mar. 10, 2017), http://www.fa-mag.com/news/new-cybersecurity-aids-for-small-businesses-posted-online-by-congress-31774.html?section=43. The average cost of a single data breach was $6.53 million in 2014. Jeff Kosseff, *The Cybersecurity Privilege*, 12 I/S: J. L. & POL'Y INFO. SOC'Y 265, 266 (2016).

organizations requesting that they take down any documents that are protected by privilege. As the First Amendment protects the publishing of newsworthy documents,[149] it is highly unlikely that a news organization would respond positively to such a request. But the attorney could use this post-hack action to demonstrate to the court that the party did not waive privilege, expressly or implicitly. For example, in response to news coverage of the hack, Sony's attorneys sent a letter to the major news sources in possession of Sony's stolen files noting that some of the hacked documents are protected by attorney-client privilege.[150] While commentators noted that this action was likely in vain because of First Amendment protection, the action clearly demonstrated Sony's intent to maintain the files' protected status.[151]

Conversely, a client or attorney publicly commenting on the contents of privileged documents could risk a court finding the party disclosed the contents of the document and thus waived the privilege.[152] A court could interpret a public comment as a voluntary waiver to a third party, thus destroying the file's privilege protection.[153] This provides few good choices for a company wanting to both appropriately deal with the public relations nightmare of a hack and also avoid waiving privilege on certain documents that might be relevant to current or future litigation.[154] For example, in the aftermath of the Wikileaks release of a legal memo, the company that issued the memo, Teneo,[155] publicly commented that "as the memo demonstrates, Teneo worked to encourage clients, where appropriate, to support the Clinton Foundation because of the good work that it does around the world."[156] If an attorney were

---

[149] Bartnicki v. Vopper, 532 U.S. 514, 518 (2001).

[150] Alison Frankel, *Sony's Big Bluff Can't Beat First Amendment*, REUTERS (Dec. 15, 2014), http://blogs.reuters.com/alison-frankel/2014/12/15/sonys-big-bluff-cant-beat-first-amendment/ [https://perma.cc/XM43-RN6G].

[151] *Id.*

[152] *But see* Dukes v. Walmart, No. 01-cv-2252 CRB (JSC), 2013 WL 1282892, at *4–5 (N.D. Cal. Mar. 26, 2013) (example of a post-leak statement that a court found did not waive privilege).

[153] *See generally In re* Qwest Commc'ns Intern. Inc., 450 F.3d 1179 (10th Cir. 2006).

[154] *Dukes*, 2013 WL 1282892 at *1, 8–9 (Wal-Mart was faced with responding publicly about a memo in which its law firm had warned of a sex discrimination suit, while also defending against that very type of suit.). *But see* Smith v. Armour Pharm. Co., 838 F. Supp. 1573, 1577 (S.D. Fla. 1993) ("In the face of public disclosure, Cutter should not be gagged for fear of waiving the privilege that would otherwise apply to the Memorandum.").

[155] Teneo is a corporate consulting firm. Helderman & Hamburger, *supra* note 36.

[156] *Id.* But the company cofounder as well as the spokesperson for the Clinton Foundation declined to comment. *Id.* Glen Caplin, Hillary Clinton's campaign spokesman, declined to comment but generally called the material "hacked by the Russian government

to try to admit into evidence this widely available memo in a suit against the Clinton Foundation, a court would have to determine whether Teneo's comments constitute a disclosure of the communication contained in the memo. That at least one national newspaper made the full text of the memo available on its website poses a different problem: the court would also have to look past the document's perfunctory attorney-client privilege label and consider the futility of trying to restore the memo's confidentiality.

B. Burden of Establishing Confidentiality

Even if the party claiming privilege employed adequate cybersecurity and its post-hack actions demonstrate no waiver of privilege, courts should still require the hacked party to establish that the file sought to be admitted remains confidential. For if a document is widely disseminated and a topic of national conversation, it would be futile to tell an opposing attorney not to view or use it in litigation. The opposing attorney is likely to know the contents of the hacked file and will still be able to use the knowledge to his advantage.[157] Hackers are destroying the confidence that "full and frank" discussions with an attorney—let alone with personal contacts through email—will remain confidential. Courts should find that permitting a party to refuse to produce files by invoking attorney-client privilege is a futile attempt to protect full and frank conversations between clients and attorneys. After a hack, the cat is out of the bag on the contents of any candid conversations. If a court finds that a file no longer remains confidential and the privileged waived, the party who lost on the claim of privilege may still rely on other Rules of Evidence to exclude the document.

Courts apply a "futility" principle in other contexts, such as trade secrets and Freedom of Information Act (FOIA) requests. In trade secret cases courts put the burden on plaintiffs to show "that the trade secret remains a secret *despite* the Internet posting."[158] One court concluded that, even

---

and weaponized by WikiLeaks," which at the very least did not dispute the authenticity of the memo. *Id.*

[157] Unlike *Castellano v. Winthrop*, an attorney cannot avoid documents that are part of a national conversation and therefore should not be penalized in such an extreme way as disqualification as counsel. Castellano v. Winthrop, 27 So. 3d 134, 136 (Fla. Dist. Ct. App. 2010). For examples of courts finding that the public dissemination of files extinguished the claim of privilege, see *supra* notes 110–116.

[158] DVD Copy Control Ass'n., Inc. v. Bunner, 75 P.3d 1, 27 (Cal. 2003) (emphasis added).

though only accessible to the public for a limited time, "once that trade secret has been released into the public domain *there is no retrieving it*."[159] That whoever posted the trade secret online did so illegally is irrelevant to the court's inquiry.[160] A court only looks to whether the trade secret is, in fact, still secret.[161] In cases concerning government secrets, citizens may request access to government documents through a FOIA request.[162] Nine enumerated exemptions, however, grant the government the ability to refuse to confirm or deny the existence of documents, mostly in the context of national security.[163] Even if an agency properly invokes a statutory exemption, a court may still find that the agency waived the exemptions "by officially acknowledging the existence of records" or that the information requested is already public due to another "documented disclosure."[164] Once a document is officially acknowledged, a court can then deem the government to have waived its claim to a FOIA exemption and compel the agency to disclose the requested document.[165]

As in trade secret and FOIA cases, courts should place the burden on a party claiming a file is privileged to demonstrate that the file remains confidential, despite a publicized hack. For example, if a party demonstrates that the privileged file was posted on an obscure website with very little traffic, detected, and removed quickly, the privileged status would not be waived. If the party cannot demonstrate that the file remained confidential, then the court should deem that the privilege is extinguished under a futility principle. This finding

---

[159] Religious Tech Ctr. v. Netcom On-Line Commc'n Servs., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) (emphasis added).

[160] *Id.*

[161] *Id.* ("While the court is persuaded by the Church's evidence that those who made the original postings likely gained the information through improper means . . . this does not negate the finding that, once posted, the works lost their secrecy."); Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995) ("Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve. Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely down loads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet.").

[162] Wolf v. CIA, 473 F.3d 370, 374 (2007) (The act mandates "broad disclosure of government records to the public, [but is] subject to nine enumerated exemptions.").

[163] *Id.*

[164] Courts evaluate the following factors in determining whether the government waived its exception. "First, the information requested must be as specific as the information previously released. Second, the information requested must match the information previously disclosed . . . . Third, . . . the information requested must already have been made public through an official and documented disclosure." *Id.* at 378 (quoting Fitzgibbon v. C.I.A., 911 F.2d 755, 765 (2d Cir. 1990)).

[165] *Id.*

would recognize the reality that once a document has been posted online and reported on extensively, there is no way to recapture its confidentiality. When determining whether the privilege was waived, courts look to "the effect on uninhibited consultation between attorney and client of not allowing the privilege in these circumstances."[166] Courts need to recognize that by the time a court is considering this after a hack, any attempt to ensure client confidence in communications with the attorney is simply pointless.

CONCLUSION

With hacks moving from uncommon to frequent, individuals are much more circumspect about what they are sending via email, especially those in high-profile jobs.[167] Individuals will remain fascinated by the ability to glimpse into private correspondence while journalists weigh the benefit of traffic to their articles with the thought that coverage of hacked documents—especially mundane emails—is encouraging unnecessary hacks.[168] Politicians and legislators will lament the effect the leaks have on media coverage and even elections.[169]

Without a clear rule from the ABA or state bar associations, attorneys will continue to face the ethical dilemma of "to view or not to view" files released as part of the hack. Courts must reevaluate the attorney-client privilege in this age of hackers to further the goal of broad disclosure during litigation while still practically protecting candid conversations between attorneys and clients.

Anne E. Conroy[†]

---

[166] Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 260 (N.D. Ill. 1981).

[167] Oran, *supra* note 14; *see* Nicholas, *supra* note 9.

[168] Andy Greenberg, *TooManyLeaks: A List of Twenty WikiLeaks Copycats*, FORBES (Apr. 8, 2011), https://www.forbes.com/sites/andygreenberg/2011/04/08/toomanyleaks-a-list-of-twenty-wikileaks-copycats/#6ab6281147d9 [https://perma.cc/E7LJ-8NN3].

[169] "Clinton campaign press secretary Brian Fallon [stated]: 'If you are going to write about materials issued by Wikileaks, you should at least state they are product of [an] illegal hack by a foreign gov[ernment] . . . [m]edia needs to stop treating Wikileaks like it is [the] same as FOIA . . . .'" Brian Stelter, *NBC's Search; More Bad News for Billy; Mark Burnett Speaks; Debate Ratings; 'Vice News Tonight' Debuts; Clinton Camp Objecting to Wikileaks Coverage*, CNN MONEY'S RELIABLE SOURCES NEWSL. (Oct. 11, 2016) (on file with author).

[†] J.D. Candidate, Brooklyn Law School, 2018; B.A. Fordham University, 2009. Thank you to Jessica Schneider, Valentina Lumaj, Charles Wood, Liana Goff, and the whole *Brooklyn Law Review* for their help and hard work throughout the past year. Special thanks to Bill, Theresa, Meg, and James for their endless encouragement, patience, and humor.