



5-2015

# Viewing Privilege Through a Prism: Attorney-Client Privilege in Light of Bulk Data Collection

Paul H. Beach

Follow this and additional works at: <http://scholarship.law.nd.edu/ndlr>

 Part of the [Civil Procedure Commons](#), [Ethics and Professional Responsibility Commons](#), and the [National Security Commons](#)

## Recommended Citation

Paul H. Beach, *Viewing Privilege Through a Prism: Attorney-Client Privilege in Light of Bulk Data Collection*, 90 Notre Dame L. Rev. 1663 (2014).

Available at: <http://scholarship.law.nd.edu/ndlr/vol90/iss4/10>

This Note is brought to you for free and open access by the Notre Dame Law Review at NDLScholarship. It has been accepted for inclusion in Notre Dame Law Review by an authorized administrator of NDLScholarship. For more information, please contact [lawdr@nd.edu](mailto:lawdr@nd.edu).

## NOTES

---

# VIEWING PRIVILEGE THROUGH A PRISM: ATTORNEY-CLIENT PRIVILEGE IN LIGHT OF BULK DATA COLLECTION

*Paul H. Beach\**

### INTRODUCTION

On June 22, 2009, President Obama signed into law the Family Smoking Prevention and Tobacco Control Act, banning the sale of flavored cigarettes in the United States<sup>1</sup>—including clove cigarettes.<sup>2</sup> The move was not without opposition, particularly from abroad. Indonesia, a major manufacturer and exporter of clove cigarettes, filed a dispute over the law with the World Trade Organization in response.<sup>3</sup> That dispute quickly became “one of the WTO’s more high-profile” disputes, highlighting a clash between the competing interests of free trade and domestic health policy.<sup>4</sup>

Surprisingly, the legacy of that four-year-long trade dispute may have little to do with health policy, free trade, or clove cigarettes. Rather, the dispute may be best remembered for its role in uncovering the surveillance of American law firms by foreign intelligence services and for expanding the role of bulk data collection in the United States. In February 2014, as the WTO dispute between Indonesia and the United States waned, the Australian

---

\* J.D. Candidate, University of Notre Dame Law School, 2016; B.S., Grand Valley State University 2011. I thank Professor Tidmarsh for reviewing early drafts of this work, and the members of Volume 90 of the *Notre Dame Law Review*. All errors are my own.

1 Vicki Needham, *US, Indonesia Settle Fight over Clove Cigarettes*, THE HILL, Oct. 3, 2014, <http://thehill.com/policy/finance/219755-us-indonesia-settle-clove-cigarette-dispute>.

2 Clove cigarettes are filled with a mix of tobacco, cloves, and clove oil. *Clove Cigarettes*, AM. CANCER SOC’Y (Feb. 13, 2014), <http://www.cancer.org/cancer/cancercauses/tobaccocancer/questionsaboutsmokingtobaccoandhealth/questions-about-smoking-tobacco-and-health-other-forms-of-smoking>.

3 *United States—Measures Affecting the Production and Sale of Clove Cigarettes*, WORLD TRADE ORG. (Oct. 3, 2014), [http://www.wto.org/english/tratop\\_e/dispu\\_e/cases\\_e/ds406\\_e.htm](http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds406_e.htm).

4 *Indonesia Announces Deal with US on Clove Cigarettes Trade Dispute*, BRIDGES (Oct. 9, 2014), <http://www.ictsd.org/bridges-news/bridges/news/indonesia-announces-deal-with-us-on-clove-cigarettes-trade-dispute>.

Signals Directorate intercepted the communications of an American law firm representing the government of Indonesia in the proceedings.<sup>5</sup> According to the leaked document at the center of this revelation, “the Australian agency received ‘clear guidance’” from the office of the National Security Agency’s (NSA) general counsel as part of its activities.<sup>6</sup> Despite notifying the NSA that the contents of the communications appeared to be privileged attorney-client communications, the Directorate continued covering the communications between the law firm and its client, “providing highly useful intelligence for interested US customers”<sup>7</sup> after receiving guidance from the American agency.

News of this monitoring understandably raised immediate concerns for many attorneys. The American Bar Association (ABA) responded quickly in an open letter to General Keith Alexander, the director of the NSA.<sup>8</sup> In that letter, ABA Director James R. Silkenat voiced the concern on many lawyers’ minds: that confidential client communications were being compromised by government surveillance.<sup>9</sup> The ABA acknowledged the policies in place that aim to minimize the impact of gathering potentially privileged information by the NSA<sup>10</sup> and requested additional information regarding policies to protect communications from third parties and other foreign surveillance organizations.<sup>11</sup>

Understandably, General Alexander’s response to the ABA was silent regarding the allegations of spying on an American law firm.<sup>12</sup> His response did, however, set out to reassure the ABA that the NSA respected, and would continue to respect, the attorney-client privilege.<sup>13</sup> The NSA, General Alex-

5 James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES, Feb. 15, 2014, <http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?smid=pl-share&r=0>.

6 Debra Cassens Weiss, *Mayer Brown Was Reportedly Spied on by NSA Ally; Law Firm Says It Wasn't Subject of Alleged Scrutiny*, ABA JOURNAL (Feb. 18, 2014, 1:07 PM), [http://www.abajournal.com/news/article/mayer\\_brown\\_responds\\_to\\_report\\_it\\_was\\_subjected\\_to\\_spying\\_by\\_nsa\\_ally](http://www.abajournal.com/news/article/mayer_brown_responds_to_report_it_was_subjected_to_spying_by_nsa_ally).

7 Risen & Poitras, *supra* note 5 (internal quotation marks omitted).

8 Letter from James R. Silkenat, ABA President, to Gen. Keith B. Alexander, NSA Dir. 1 (Feb. 20, 2014) [hereinafter Silkenat Letter] (noting that “[t]he attorney-client privilege is a bedrock legal principle of our free society and is important in both the civil and criminal contexts”), *available at* [http://www.americanbar.org/content/dam/aba/uncategorized/GAO/2014feb20\\_privilegedinformation\\_1.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/uncategorized/GAO/2014feb20_privilegedinformation_1.authcheckdam.pdf).

9 *Id.* at 2.

10 *Id.* For more information on the NSA’s minimization procedures, see *infra* notes 187–92 and accompanying text.

11 Silkenat Letter, *supra* note 8, at 2.

12 Letter from Gen. Keith B. Alexander, NSA Dir., to James R. Silkenat, ABA President 1 (Mar. 10, 2014) [hereinafter Gen. Alexander Letter], *available at* [http://www.americanbar.org/content/dam/aba/images/abanews/nsa\\_response\\_03102014.pdf](http://www.americanbar.org/content/dam/aba/images/abanews/nsa_response_03102014.pdf).

13 *Id.* at 1. Addressing the concerns that stemmed from the work of Australian signals intelligence, General Alexander noted that the NSA “cannot and does not ask its foreign partners to conduct any intelligence activity that [the NSA] would be prohibited from conducting itself in accordance with U.S. law.” *Id.*

ander assured, was unable to target the communications of Americans anywhere in the world where they enjoy a reasonable expectation of privacy.<sup>14</sup> The General also noted the considerable procedures in place aimed at handling and protecting privileged communications inadvertently gathered by the NSA.<sup>15</sup> In the months since this exchange, there has been little to no development to this story.

Importantly, this saga does not appear to be an isolated event. As a result of the bulk data collection programs uncovered by former NSA contractor Edward Snowden,<sup>16</sup> news agencies have spent considerable energy covering, discussing, and debating government bulk data collection.<sup>17</sup>

This Note will argue that the attorney-client privilege is justified not only by the popular instrumentalist rationales, but also by noninstrumentalist thinking. It will further argue that Federal Rule of Evidence 502 gives federal courts the tools to protect the attorney-client privilege in light of bulk data collection. Even where courts do not find that traditional modes of communication constitute reasonable steps to protect a confidential communication, general considerations of fairness—as noted in Rule 502’s committee notes—should encourage courts to uphold attorney-client privilege in future situations of bulk data collection disclosures. Part I will discuss the establishment, development, and operations of the national security surveillance and signals intelligence apparatuses in the United States. It will also examine the legal basis for state surveillance and bulk data collection programs and legal challenges to those programs with an eye toward the issue of attorney-client privilege. Part II of this Note will examine the establishment and development of attorney-client privilege and the waiver of that privilege in the United States. Finally, Part III will analyze the methods courts should adopt in considering a future case involving privileged information gathered through bulk data collection.

---

14 *Id.*

15 *Id.* at 2–3. These procedures will be addressed below. *See infra* notes 187–92.

16 *See infra* note 29.

17 For a fraction of the coverage of the leaked NSA files, see Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA’s Secret Tool to Track Global Surveillance Data*, THE GUARDIAN, June 11, 2013, <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>; Andy Müller-Maguhn et al., *Treasure Map: The NSA Breach of Telekom and Other German Firms*, SPIEGEL ONLINE (Sept. 14, 2014, 12:13 PM), <http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html>; James Risen & Nick Wingfield, *Web’s Reach Binds N.S.A. and Silicon Valley Leaders*, N.Y. TIMES, June 19, 2013, <http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html?gwh=637578456D69D3EF0CB64CFDDC57F944&gwt=pay>; Craig Timberg & Ellen Nakashima, *Agreements with Private Companies Protect U.S. Access to Cables’ Data for Surveillance*, WASH. POST, July 6, 2013, [http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01\\_story.html](http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html).

## I. BULK DATA COLLECTION IN THE UNITED STATES

### A. *Background*

Recognizing in 1952 that the “communications intelligence . . . activities of the United States are a national responsibility,”<sup>18</sup> President Truman set out to lay the framework to modernize American signals intelligence for the modern age.<sup>19</sup> In a memorandum to the Secretaries of State and Defense, the President made the first references to a “National Security Agency,”<sup>20</sup> conceptualizing the agency as “provid[ing] an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments.”<sup>21</sup> Just days after the President’s memorandum, on November 4, 1952,<sup>22</sup> Secretary of Defense Robert A. Lovett “accomplished the actual establishment of the new National Security Agency” in a “remarkably sparse announcement” and memorandum.<sup>23</sup>

The next sixty-one years of the NSA’s existence were impressive. The Agency proved vital to American intelligence gathering, providing communications and signals intelligence in a number of crucial situations. For example, in 1952 the NSA exposed “a massive soviet espionage effort.”<sup>24</sup> The organization also provided intelligence support during the Cuban Missile Crisis,<sup>25</sup> provided signals intelligence during Operation Desert Storm,<sup>26</sup> and provided continuing integral signals intelligence throughout the United States’ engagement in Iraq and Afghanistan.<sup>27</sup>

Despite this storied history, the NSA was able to largely avoid media attention and recognition. That became more difficult in the wake of the September 11 attacks,<sup>28</sup> and the situation changed dramatically in June of 2013, when then-NSA contractor Edward Snowden leaked information

18 Memorandum from President Harry Truman to Sec’y of State Dean Acheson & Sec’y of Def. Robert Lovett 1 (Oct. 24, 1952) [hereinafter Truman Memo]; *see also* THOMAS L. BURNS, NSA, THE ORIGINS OF THE NATIONAL SECURITY AGENCY 1940–1952, at 97–108 (1990) (approved for release Sept. 8, 2004) (describing the work of the Brownell Committee and the early establishment of the NSA).

19 BURNS, *supra* note 18, at 97.

20 *Id.*

21 Truman Memo, *supra* note 18, at 5.

22 BURNS, *supra* note 18, at 108.

23 *Id.*; *see also* Memorandum from the Dir. of the Nat’l Sec. Agency (Canine), Reps. of the Military Servs. & Joint Chiefs of Staff to Sec’y of Def. Lovett (Nov. 20, 1952), *available at* <https://history.state.gov/historicaldocuments/frus1950-55Intel/d136> (confirming the implementation of Secretary Lovett’s directive).

24 NSA/CSS 60TH, NSA 60TH ANNIVERSARY TIMELINE (Dec. 14, 2012), [https://www.nsa.gov/about/cryptologic\\_heritage/60th/](https://www.nsa.gov/about/cryptologic_heritage/60th/).

25 *Id.*

26 *Id.*

27 *Id.*

28 *See, e.g.*, James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, <http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all>.

regarding NSA bulk data collection programs to the press.<sup>29</sup> In the following months, a number of previously unknown or little-known data collection programs would become public knowledge.<sup>30</sup> While this was hardly the first instance of government surveillance of Americans' communications,<sup>31</sup> the "dragnet" style of the NSA's programs startled many commentators.<sup>32</sup>

Much of the coverage of Snowden's leaks centered largely on two NSA data collection programs: PRISM and XKeyscore.<sup>33</sup> The program garnering most of the attention from the press has been PRISM, which "collect[s] [data] directly from the servers of . . . Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, Youtube, [and] Apple."<sup>34</sup> "That program, which has been known for years, copies [metadata] as it enters and leaves the United States, then routes it to the NSA for analysis."<sup>35</sup> Another NSA program revealed is called XKeyscore. XKeyscore is the "'widest reaching' means of gathering data from across the Internet,"<sup>36</sup> and collects not only metadata, but also content data from the Internet.<sup>37</sup> An advantage of XKeyscore is the

29 Mirren Gidda, *Edward Snowden and the NSA Files—Timeline*, THE GUARDIAN (Aug 21, 2013, 5:54 PM), <http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline>.

30 *Id.*

31 Indeed, in the 1960s, the NSA intercepted and monitored the communications of United States Senator Frank Church as part of a program called Operation Minaret. Matthew M. Aid & William Burr, *Secret Cold War Documents Reveal NSA Spied on Senators*, FOREIGN POLICY (Sept. 25, 2013), [http://www.foreignpolicy.com/articles/2013/09/25/it\\_happened\\_here\\_NSA\\_spied\\_on\\_senators\\_1970s](http://www.foreignpolicy.com/articles/2013/09/25/it_happened_here_NSA_spied_on_senators_1970s).

32 That is not to say that the NSA was without its defenders throughout the course of this saga. See, e.g., Walter Pincus, *Intelligence Community's Defense of NSA Collection Programs*, WASH. POST, Aug. 14, 2013, [http://www.washingtonpost.com/world/national-security/2013/08/14/02674a96-043b-11e3-9259-e2aafe5a5f84\\_story.html](http://www.washingtonpost.com/world/national-security/2013/08/14/02674a96-043b-11e3-9259-e2aafe5a5f84_story.html) (describing President Obama's defense of the program).

33 See, e.g., Glenn Greenwald & Spencer Ackerman, *How the NSA Is Still Harvesting Your Online Data*, THE GUARDIAN, June 27, 2013, <http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection> (describing the XKeyscore program).

34 Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 7, 2013, [http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497\\_story.html](http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html) (internal quotation marks omitted). Put simply, PRISM seeks to "make [ ] sense of the cacophony of the Internet's raw feed." Stephen Braun et al., *PRISM Is Just Part of a Much Larger, Scarier Government Surveillance Program*, BUS. INSIDER (June 15, 2013, 9:54 AM), <http://www.businessinsider.com/prism-is-just-the-start-of-nsa-spying-2013-6#ixzz2WIkGyDqZ>.

35 Stephen Braun et al., *Secret to PRISM Program: Even Bigger Data Seizure*, ASSOCIATED PRESS (June 15, 2013, 2:53 PM), <http://bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure>.

36 Yannick LeJacq, *How the NSA's XKeyscore Program Works*, NBC NEWS (July 31, 2013, 7:12 PM), <http://www.nbcnews.com/tech/security/how-nas-xkeyscore-program-works-f6C10812168>.

37 See *id.* (noting that content remains on the XKeyscore system for only three to five days while metadata is stored for thirty days).

ability to catalog tremendous amounts of metadata and content data for later review, sometimes up to five years later.<sup>38</sup>

In the wake of these leaks, much of the focus centered on the NSA's collection of metadata, which can be described as "data about data."<sup>39</sup> Metadata collection apparently constitutes the vast majority of the information gathered by NSA bulk data collection programs.<sup>40</sup> However, disclosures about programs such as XKeyscore, suggest that NSA surveillance goes beyond merely collecting information about the delivery path or forwarding information of communications.<sup>41</sup> Rather, the NSA and other agencies have "tapp[ed] directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets."<sup>42</sup> Perhaps this is unsurprising, considering that the concerns that triggered the ABA's letter to General Alexander were due to monitoring of communications, not simply the collection of metadata *about* those communications.<sup>43</sup> This is important to keep in mind when considering an application to attorney-client privilege.

### B. *Legal Basis for Bulk Data Collection Programs in the United States*

The legal basis for the government's bulk data collection is anchored in the Foreign Intelligence Surveillance Act (FISA), originally enacted in 1978.<sup>44</sup> A key purpose of FISA was "to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes."<sup>45</sup> The Act was seen as "an important first step towards full-scale legislative regulation of the intelligence activities" in the United States.<sup>46</sup> To achieve this goal, Congress also established a court charged with evaluating applications for electronic surveillance and granting those applications

---

38 *Id.*

39 MARIAN K. RIEDY ET AL., *LITIGATING WITH ELECTRONICALLY STORED INFORMATION* 118 (2007). Metadata includes data about a computer's operating system, about the creators and editors of documents, and importantly, information about email "regarding the creation, forwarding information, delivery path and receipt" of the communication. *Id.*

40 *See, e.g.*, Gellman & Poitras, *supra* note 34; *see also* Braun et al., *supra* note 34 ("Prism makes sense of the cacophony of the Internet's raw feed. It provides the government with names, addresses, conversation histories and entire archives of email inboxes.").

41 *See* Gellman & Poitras, *supra* note 34.

42 *Id.*

43 Needham, *supra* note 1.

44 50 U.S.C. § 1881a (2012); *see also* Adam Florek, Comment, *The Problems with PRISM: How a Modern Definition of Privacy Necessarily Protects Privacy Interests in Digital Communications*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 571, 572 (2014) (discussing passage of FISA and subsequent amendments).

45 *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013).

46 *Foreign Intelligence Surveillance Act of 1978: Hearing before the Subcomm. on Intelligence and the Rights of Ams.*, 95th Cong. 2 (1977) (statement of Sen. Birch Bayh, Chairman, Subcomm. on Intelligence and the Rights of Ams. of the Select Comm. on Intelligence).

where appropriate.<sup>47</sup> Judges for this Foreign Intelligence Surveillance Court (FISC) were appointed by the Chief Justice of the United States, and served for nonrenewable terms of seven years.<sup>48</sup> The FISC offered a detached oversight element to intelligence gathering.<sup>49</sup> Some have argued, however, that over time, the FISC eventually came to approve surveillance programs that even Congress would have balked at.<sup>50</sup>

In 2008, Congress amended FISA.<sup>51</sup> The 2008 amendments are often cited as providing the legal basis for government bulk data collection programs such as PRISM and Xkeyscore noted above.<sup>52</sup> The amendments, far from providing a blank check to surveillance agencies, actually established a number of limits on data acquisitions. Acquisitions of data must not intentionally target persons located within the United States;<sup>53</sup> may not target a U.S. person located outside the United States;<sup>54</sup> and may not target communications located entirely within the United States.<sup>55</sup> Furthermore, all acquisitions must be consistent with the Fourth Amendment.<sup>56</sup>

Despite these control mechanisms, the result of the 2008 FISA amendments appears to have been a significant expansion of the government's ability to conduct surveillance.<sup>57</sup> The effect of this expanded authority is clear. "Unlike traditional FISA surveillance," the 2008 amendments "do[ ] not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power," nor does it "require the Government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur."<sup>58</sup>

This is true despite the fact that "[o]n its face, [the FISA Amendments] simply authorized a national security subpoena power."<sup>59</sup> That is, the amendments do not expressly provide for any methods that would be unavailable to a federal prosecutor in a domestic criminal case.<sup>60</sup> The expan-

---

47 See 50 U.S.C. § 1803.

48 *Id.* § 1803(a)(1).

49 See Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513, 1513–14 (2014).

50 See *id.* at 1514.

51 FISA Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2474.

52 Florek, *supra* note 44, at 572.

53 50 U.S.C. § 1881a(b)(1).

54 *Id.* § 1881a(b)(3).

55 *Id.* § 1881a(b)(4).

56 *Id.* § 1881a(b)(5).

57 See Florek, *supra* note 44, at 574–75 (providing an overview of the development of surveillance programs after September 11 and the impetus behind the 2008 FISA amendments).

58 *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013).

59 Kerr, *supra* note 49, at 1528 (providing the example that "if a federal prosecutor in Topeka or San Antonio could not issue a lawful grand jury subpoena for the records, the FISC could not enter an order requiring a third party to hand over those records under Section 215").

60 *Id.* at 1527–28.

sion, then, comes not from the 2008 amendments directly but rather from FISC interpretations of that law, which allow for “astonishing” programs not directly authorized by the text of the 2008 amendments.<sup>61</sup>

Despite—or perhaps because of—the 2008 FISA amendments, there have been a number of legal challenges to the NSA’s bulk data collection practices.<sup>62</sup> To date, however, those challenges have met little success. In *Clapper v. Amnesty International, U.S.A.*, for example, the difficulty of a successful challenge to data collection practices was highlighted when the Supreme Court found a challenge to data collection failed because “it is speculative whether the Government will imminently target communications” of a party.<sup>63</sup> For the purposes of this Note, it will be unnecessary to examine these cases any further; what is important to take away is that the bulk data collection programs operated by the NSA are unlikely to be dismantled any time soon. For that reason, this Note will assume the underlying legality of the NSA’s bulk data collection programs.

## II. THE ATTORNEY-CLIENT PRIVILEGE

### A. *Origins and Development of Attorney-Client Privilege*

To understand the impact of bulk data collection on attorney-client privilege in the United States, one must first look to the development of privilege in this country and in England before it. It is important to begin this process with a baseline understanding of privilege. Testimonial privileges prevent the disclosure of certain communications during the course of litigation.<sup>64</sup> Importantly, privilege protects the communication itself, but not the underlying facts contained in that communication.<sup>65</sup>

Dean Wigmore conditioned the existence of privilege as relying on “four fundamental conditions.”<sup>66</sup> First, the communication must be made in confidence; second, the confidentiality of the communications must be essential to the nature of the communication; third, the relay between the two communicating parties must be of the sort that, “in the opinion of the community ought to be seditiously fostered”; and fourth, that the injury of disclosure would outweigh the benefits.<sup>67</sup> Wigmore’s four-element framework for understanding privilege remains influential today.<sup>68</sup>

---

61 *Id.* at 1527 (“[T]he quality of the FISC’s legal analysis was surprisingly poor. The FISC had authorized vastly more surveillance than outside observers could have imagined based on the public text of the statute. In the hands of the FISC judges, acting in secret, the text of FISA was no longer a reliable guide to executive branch authority.”).

62 *See, e.g., Clapper*, 133 S. Ct. 1138.

63 *Id.* at 1148.

64 *See* *Upjohn Co. v. United States*, 449 U.S. 383, 395 (1981).

65 *Id.*

66 JOHN HENRY WIGMORE, *A TREATISE ON THE ANGLO-AMERICAN SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW* § 2290 (1923).

67 *Id.*

68 JONATHAN AUBURN, *LEGAL PROFESSIONAL PRIVILEGE: LAW AND THEORY* 3 (2000) (describing Wigmore’s narrative of privilege as being “almost universally accepted”).

Contemporary courts have further refined Dean Wigmore's requirements, and now generally hold that:

The privilege applies only if (1) the asserted holder of the privilege is or sought to become a client; (2) the person to whom the communication was made (a) is a member of the bar of a court, or his subordinate and (b) in connection with this communication is acting as a lawyer; (3) the communication relates to a fact of which his attorney was informed (a) by his client (b) without the presence of strangers (c) for the purpose of securing primarily either (i) an opinion on law or (ii) legal services or (iii) assistance in some legal proceeding, and not (d) for the purpose of committing a crime or tort; and (4) the privilege has been (a) claimed and (b) not waived by the client.<sup>69</sup>

The attorney-client privilege is frequently cited as the oldest of all privileges over communications,<sup>70</sup> and was asserted and recognized in England as early as the reign of Elizabeth I.<sup>71</sup> However, the prevailing view is that this sixteenth-century privilege has little to do with the contemporary understanding of it.<sup>72</sup> Originally, attorneys held the privilege.<sup>73</sup> This was thought necessary to protect the honor of the professionals, lest they be forced to share client secrets learned in confidence.<sup>74</sup>

Despite these somewhat alien origins, centuries of litigation gradually transformed attorney-client privilege into something more recognizable to the modern observer.<sup>75</sup> By the early eighteenth century, arguments were commonly made in English trials that the privilege in fact should rest with the client;<sup>76</sup> by the middle of that century, courts regularly accepted those

69 *United States v. Woodruff*, 383 F. Supp. 696, 696–97 (E.D. Pa. 1974) (quoting *United States v. United Shoe Mach. Corp.*, 89 F. Supp. 357, 358–59 (D. Mass. 1950)).

70 See, e.g., EDNA SELAN EPSTEIN, *THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE* 4 (5th ed. 2007); WIGMORE, *supra* note 66, § 2291; Gregg F. LoCascio, *Reassessing Attorney-Client Privileged Legal Advice in Patent Litigation*, 69 NOTRE DAME L. REV. 1203, 1205 (1994).

71 EPSTEIN, *supra* note 70, at 4.

72 See PAUL R. RICE, *ATTORNEY-CLIENT PRIVILEGE IN THE UNITED STATES* §§ 1.2–3 (2008). *But see* AUBURN, *supra* note 68, at 5–6 (arguing that in fact Wigmore's widely accepted view of honor-based privilege is incorrect, and that instead Elizabethan-era privilege was much more in line with the justifications given for the privilege today).

73 RICE, *supra* note 72, § 1.1; WIGMORE, *supra* note 66, § 2290 (citing *Berd v. Lovelace*, (1577) 21 Eng. Rep. 33 (ch.)).

74 RICE, *supra* note 72, § 1.1. *But see* AUBURN, *supra* note 68, at 5–6 (arguing that Wigmore's view of privilege as being based on the honorable status of a lawyer does not provide a complete view of the development of the privilege, and asserting that it is "less likely [than frequently asserted] that the privilege was originally founded on some respect for the special status of the lawyer").

75 As Dean Wigmore noted, "[p]robably in no rule of evidence having so early an origin were so many points still unsettled until the middle of the 1800s." WIGMORE, *supra* note 66, § 2291.

76 RICE, *supra* note 72, § 1.3; see *Annesley v. Anglesey*, 17 How. St. Tr. 1139, 1237 (1743). The client-oriented ownership of privilege was actually pronounced as early as 1679. See WIGMORE, *supra* note 66, § 2291 (citing *Lea v. Wheatley*, 20 How. St. Tr. 574

arguments.<sup>77</sup> It was not until 1776, however, that notions of attorney honor were thoroughly rejected as an insufficient basis for attorney-client privilege.<sup>78</sup> As Professor Paul R. Rice has noted, this shift was important; only the “‘owner’ of the privilege held the power to waive it.”<sup>79</sup> With a shift toward “ownership” by the client, English courts acknowledged that only the client—not the attorney—could waive the privilege.<sup>80</sup>

Although it took decades for English courts to find that attorney-client privilege belonged fully to the client,<sup>81</sup> early American courts to rule on the issue were clear that the privilege belonged to the client. State courts in Connecticut,<sup>82</sup> New York,<sup>83</sup> and Pennsylvania<sup>84</sup> all ruled that the privilege was only the client’s to waive. By the time it came to American courts, “the privilege was firmly established as belonging to the client.”<sup>85</sup> Indeed, early American courts generally looked to English law to form their views in most areas of evidentiary privilege.<sup>86</sup>

Alongside this shift from attorney to client “ownership” of privilege, the traditional justification of honor fell out of favor with courts deciding questions of privilege.<sup>87</sup> By the early eighteenth century a “new theory” of attorney-client privilege that rested on ensuring the client’s “freedom of apprehension in consulting his legal advisor” came about.<sup>88</sup> By 1777, English

(1678)). However, that notion did not gain traction for nearly a century. See WIGMORE, *supra* note 66, § 2291.

77 See WIGMORE, *supra* note 66, § 2291.

78 RICE, *supra* note 72, § 1.3; WIGMORE, *supra* note 66, § 2290.

79 RICE, *supra* note 72, § 1.3.

80 *Id.*

81 *Id.* (citing WIGMORE, *supra* note 66).

82 See, e.g., *Mills v. Griswold*, 1 Root 383, 383 (Conn. Super. Ct. 1792) (“Voluntary communications of a party under engagements of secrecy, are to be testified, by a witness except those made to an attorney who is under oath to keep his client’s secrets.”); see also *Calkins v. Lee*, 2 Root 363, 364 (Conn. Super. Ct. 1796) (citing *Mills v. Griswold* for the same proposition).

83 *Baker v. Arnold*, 1 Cai. 258, 266 (N.Y. Sup. Ct. 1803) (“This is the privilege of the client, and not of the attorney.”).

84 *Heister v. Davis*, 3 Yeates 4 (Pa. 1800) (“It is the privilege of the client, and not of the counsel or attorney.”).

85 “[A]n attorney shall not be permitted to betray a secret with which he has been intrusted by his client. This is the privilege of the client, and not of the attorney.” *Baker*, 1 Cai. at 266 (cited in Rice, *supra* note 72, § 1.3 n.24); see also EPSTEIN, *supra* note 70 at 4–5 (noting that today’s attorney-client privilege “exists as a privilege against testimonial compulsion of the attorney with respect to matters conveyed to the attorney by the client”).

86 *Developments in the Law—Privileged Communications*, 98 HARV. L. REV. 1450, 1457 n.22 (1985) [hereinafter *Developments in the Law*] (“It is clear . . . that the eighteenth-century English treatises were the only substantial source of evidentiary precedent and teaching available to the early American courts . . .”); *id.* at 1458 (“To the extent that American judges of that time sought precedent and authority to decide privilege questions, they were forced to look to the English common law.”).

87 See WIGMORE, *supra* note 66, § 2291; Vincent C. Alexander, *The Corporate Attorney-Client Privilege: A Study of the Participants*, 63 ST. JOHN’S L. REV. 191, 216–17 (1989).

88 WIGMORE, *supra* note 66, § 2290.

courts no longer consistently recognized honor as a sufficient basis of attorney-client privilege.<sup>89</sup> Instead, attorneys had to find “an alternative rationale” to defend the existence of privilege.<sup>90</sup> And they did. Attorneys quickly found a new footing for the existence of the privilege; arguments resting on “social utility” took the place of honor in defending the existence of the privilege.<sup>91</sup> The alternative justification, then, focused on “the promotion of client candor”<sup>92</sup> and “freedom of consultation”<sup>93</sup> for potential clients.

### B. *Modern Justifications for Attorney-Client Privilege*

Not unlike the eighteenth century, the twentieth century witnessed new developments in the justifications for attorney-client privilege.<sup>94</sup> The two overarching justifications for privilege in general can be described as “instrumental” and “non-instrumental.”<sup>95</sup> The instrumentalist rationale is essentially utilitarian in nature, arguing that the protection for privileged communications is desirable because it furthers desirable policy goals.<sup>96</sup> A noninstrumentalist argument, meanwhile, favors the protection of privileged communications because failing to do so would be inherently wrong.<sup>97</sup> While these arguments may ultimately arrive at the same conclusion—the protection of privileged communications—they take markedly different paths. The instrumentalist rationale has been the dominant justification for the existence of privilege after the traditional rationales noted above began to dissipate.<sup>98</sup> It holds that the privilege exists only to encourage free, open, and frequent disclosure from client to attorney.<sup>99</sup>

Recall again Dean Wigmore’s “four fundamental conditions” necessary to acknowledge attorney-client privilege.<sup>100</sup> This understanding of privilege can itself be seen as an instrumentalist approach,<sup>101</sup> and American courts

89 See JAMES AITKEN, *THE TRIAL AT LARGE OF JAMES HILL* 71 (2d ed. 1777) (“[T]he wisdom of the law knows nothing of that point of honour.”).

90 Alexander, *supra* note 87, at 217.

91 *Id.*

92 *Id.*

93 WIGMORE, *supra* note 66, § 2291.

94 See 23 CHARLES A. WRIGHT & KENNETH W. GRAHAM, JR., *FEDERAL PRACTICE AND PROCEDURE: EVIDENCE* § 5422.1 (1980 & Supp. 2014).

95 *Id.*

96 See *id.* (explaining that an instrumentalist argument “takes the form, ‘X is good because it will bring about Y’”).

97 See *id.* (“A ‘non-instrumental argument’ says that ‘X is intrinsically good (or bad)’ . . .”).

98 See *Developments in the Law*, *supra* note 86, at 1458–59; LoCascio, *supra* note 70, at 1203 (describing instrumentalist approaches as the “prevailing application”).

99 See *Developments in the Law*, *supra* note 86, at 1483–84 (noting that the crux of the instrumentalist argument in favor of attorney-client privilege is that it is sound public policy to encourage clients to be totally open and honest with their attorneys).

100 WIGMORE, *supra* note 66, § 2285.

101 See EDWARD J. IMWINKELRIED, *THE NEW WIGMORE: EVIDENTIARY PRIVILEGES* § 5.1.1 (2014) (“Wigmore’s variation of the instrumental rationale was based on a factual assump-

have long claimed to adopt the instrumentalist rationale it illustrates. In 1888, in *Hunt v. Blackburn*, the Supreme Court grounded the existence of attorney-client privilege in “necessity,” noting that the “assistance [of counsel] can only be safely and readily availed of when free from the consequences or the apprehension of disclosure.”<sup>102</sup>

This view has been consistently reaffirmed in more recent Supreme Court cases. In *Fisher v. United States*, for example, the Court addressed attorney-client privilege as a “practical matter,” finding that it was designed to “encourage clients to make full disclosure to their attorneys.”<sup>103</sup> Again in *Upjohn Co. v. United States*, the Court took an instrumentalist view of attorney-client privilege.<sup>104</sup> Reviewing the purpose of the privilege there, the Court asserted that “[t]he privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer’s being fully informed by the client.”<sup>105</sup>

On the surface, instrumentalist reasoning appears to do essentially all of the substantive work in federal courts deciding issues of privilege. The Supreme Court’s stated rationale in *Hunt* offers support for this view.<sup>106</sup> Further, when the Court reasserted the basic instrumentalist rationale for attorney-client privilege in *Fisher*, it noted five circuit court opinions that also demonstrate a commitment to instrumentalism as the basis for privilege, even where those cases did not rely on *Hunt*.<sup>107</sup>

Examining just a few of these cases demonstrates the widespread presence of instrumentalist thinking in federal courts. For example, the Ninth Circuit’s *Baird v. Koerner* opinion makes clear that the public policy of encouraging candor is in fact “‘more fundamental’ . . . than the policy of the attorney-client privilege” itself,<sup>108</sup> and that the privilege is to be “strictly limited to the purposes for which it exists.”<sup>109</sup> That is, for the purpose of encouraging open dialogue between client and attorney.<sup>110</sup> By the reasoning of *Baird*, then, privilege exists only to further a desirable public policy. Other circuits are equally unequivocal. In *Prichard v. United States*, the Sixth

---

tion, that is, a causal connection between the existence of a privilege and the average person’s willingness to make disclosures necessary to the maintenance of the relation.” (footnotes omitted)).

102 *Hunt v. Blackburn*, 128 U.S. 464, 470 (1888).

103 *Fisher v. United States*, 425 U.S. 391, 403 (1976).

104 *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

105 *Id.*

106 *Hunt*, 128 U.S. at 470 (finding that the attorney-client privilege is rooted in the “necessity” of ensuring clients do not have apprehension over sharing information with their attorneys).

107 *Fisher*, 425 U.S. at 403 (citing, inter alia, *Baird v. Koerner*, 279 F.2d 623 (9th Cir. 1960), and *Prichard v. United States*, 181 F.2d 326 (6th Cir. 1950)); see also *Baird*, 279 F.2d at 631–32 (examining the purpose of privilege without relying on *Hunt* as a precedent); *Prichard*, 181 F.2d at 328 (same).

108 *Baird*, 279 F.2d at 631 (quoting WIGMORE, *supra* note 66, § 2291).

109 *Id.* at 631–32.

110 See *supra* note 96 and accompanying text.

Circuit adopted the view that privilege “is designed to influence [the client] when he may be hesitating between . . . disclosure and . . . secrecy.”<sup>111</sup> These two circuits are largely representative of the federal courts in adopting the instrumentalist understanding of privilege.<sup>112</sup>

Noninstrumental arguments resurfaced during the last quarter of the twentieth century, however, and are not irrelevant.<sup>113</sup> Not unlike the original justification of honor, modern noninstrumentalist justifications rely on a fundamental sense of right and wrong.<sup>114</sup> The noninstrumentalist justification holds that “compelled disclosure” due to lack of privilege is “intrinsically wrong, regardless of [the] effect the privilege may have on client candor.”<sup>115</sup> Put another way, “there are things even more important to human liberty than accurate adjudication. One of them is the right to be left by the state unmolested in certain human relations.”<sup>116</sup> This argument may not be compelling at first blush, but it is worth further consideration. After all, this “bedrock legal principle of our free society”<sup>117</sup> owes its original existence to noninstrumentalist justifications.<sup>118</sup> Charles Fried illustrates this view in another context, where he argues that “it is immoral for society to limit [a person’s] liberty other than according to the rule of law.”<sup>119</sup> It is also immoral, Fried says, to bar that person from “discovering what the limits of [society’s] power over him are.”<sup>120</sup> If it is immoral to bar a person from learning these limits, it must also be immoral to bar anyone from informing others of the limits of society’s power over him.<sup>121</sup> Fried’s thinking, then, would view privilege, a protection of a client’s ability to consult with an attorney, as a [n]ecessary [e]ntailment of the [g]ranting of [r]ights.<sup>122</sup>

There are multiple iterations of these justifications, and a number of them may work together concurrently. Jonathan Auburn has described three basic categories of noninstrumentalist justifications: the “dignity theory,” the “treachery theory,” and “the privacy rationale.”<sup>123</sup> These views of privilege, as

111 *Prichard*, 181 F.2d at 328 (quoting WIGMORE, *supra* note 66, § 2306).

112 AUBURN, *supra* note 68, at 3–6 (describing the “almost universal[ ]” acceptance of Wigmore’s construction of privilege).

113 See 23 WRIGHT & GRAHAM, *supra* note 94, § 5422; Alexander, *supra* note 87, at 217.

114 See 23 WRIGHT & GRAHAM, *supra* note 94, § 5422.1.

115 Alexander, *supra* note 87, at 217.

116 David W. Louisell, *Confidentiality, Conformity and Confusion: Privileges in Federal Court Today*, 31 TUL. L. REV. 101, 110 (1956).

117 Silkenat Letter, *supra* note 8, at 1.

118 See *supra* notes 75–79 and accompanying text.

119 Charles Fried, *Correspondence: The Lawyer as Friend*, 86 YALE L.J. 573, 586 (1977) (Professor Fried’s reply to Edward Dauer and Arthur Leff).

120 *Id.*

121 See *id.*

122 Note, *The Attorney-Client Privilege: Fixed Rules, Balancing, and Constitutional Entitlement*, 91 HARV. L. REV. 464, 480 (1977) [hereinafter *Fixed Rules, Balancing, and Constitutional Entitlement*]. That note argues against Professor Fried’s thinking on the grounds that it suggests that “abrogation of privilege for any client . . . would constitute a wrongful impediment to the discovery of legal rights,” a result that is not reflected in our system. *Id.* at 481.

123 AUBURN, *supra* note 68, at 18 (footnotes omitted).

well as the argument that attorney-client privilege is a “[n]ecessary [e]ntailment of the [g]ranting of [r]ights”<sup>124</sup> ultimately view privilege as a means of securing the rights of individuals rather than focusing on society as a whole.<sup>125</sup> “The rights-based rationale contends that the attorney-client privilege is justified because it protects both the privacy and the dignity of the client.”<sup>126</sup> Ultimately, then, noninstrumentalist justifications do not condition the existence of the attorney-client privilege on whether it actually encourages candor, but tend to uphold the privilege even where it did not achieve that instrumentalist goal in order to protect the rights of the client.

While courts outwardly claim to apply the instrumentalist approach, some observers have suggested that noninstrumentalist arguments are more influential than meets the eye.<sup>127</sup> Indeed, there is room for the possibility that instrumentalist and noninstrumentalist rationales are at play concurrently, even in the Supreme Court decisions examined above.<sup>128</sup> If courts were to subscribe exclusively to the instrumentalist rationale—as they appear to do in *Baird* and *Prichard*—evidence that the existence of privilege does not advance the stated policy goals should theoretically lead courts not to enforce the privilege. This is because upholding the privilege comes at the expense of the fact-finding goal of courts without providing the benefit of increasing client candor.<sup>129</sup> This result, however, seems unlikely considering the long line of precedent in both English and American law suggesting that the attorney-client privilege is “indispensable to the lawyer’s function as advocate.”<sup>130</sup>

A number of empirical studies have examined how, and to what extent, the existence of attorney-client privilege shapes the behavior of attorneys and clients.<sup>131</sup> One study surveyed 105 rural subjects, asking them about “a series of hypothetical disclosure situations.”<sup>132</sup> The results there suggested that “many clients give information not because of confidentiality guarantees, but

124 *Fixed Rules, Balancing, and Constitutional Entitlement*, *supra* note 122, at 480.

125 See Casey Nix, Note, *In re Sealed Case: The Attorney-Client Privilege—Till Death Do Us Part?*, 43 VILL. L. REV. 285, 292 (1998).

126 *Id.* (citing Deborah Stavile Bartel, *Drawing Negative Inferences upon a Claim of the Attorney-Client Privilege*, 60 BROOK. L. REV. 1355, 1363 (1995)).

127 See 23 WRIGHT & GRAHAM, *supra* note 94, § 5422.

128 See *id.* (“These contrasting styles of argumentation are not, of course, mutually exclusive.”); *Developments in the Law*, *supra* note 86, at 1485 (“[I]nstrumental and noninstrumental arguments are not . . . mutually exclusive.”).

129 See 23 WRIGHT & GRAHAM, *supra* note 94, § 5422 (“Since instrumental arguments usually depend upon some causal relationship between the privilege and other conduct—e.g., the attorney-client privilege encourages clients to be more candid and therefore leads to a more accurate portrayal of the facts in litigation—such arguments could be supported or defeated by empirical research into the conduct of privileged persons.”).

130 Geoffrey C. Hazard, Jr., *An Historical Perspective on the Attorney-Client Privilege*, 66 CALIF. L. REV. 1061, 1061 (1978).

131 For a convenient overview of a number of empirical studies and their findings, see Edward J. Imwinkelried, *Questioning the Behavioral Assumption Underlying Wigmorean Absolutism in the Law of Evidentiary Privileges*, 65 U. PITT. L. REV. 145, 156–59 (2004).

132 Fred C. Zacharias, *Rethinking Confidentiality*, 74 IOWA L. REV. 351, 380 (1989).

because they view lawyers as honorable professionals who customarily promise discretion.”<sup>133</sup> Another survey focused on corporate lawyers and clients.<sup>134</sup> There, results demonstrated that, “at least in the corporate context,” the “factual premise on which privilege is based . . . is largely a matter of faith, supported by minimal empirical evidence.”<sup>135</sup>

Other surveys have focused on the members of professional associations such as the Association of Corporate Counsel and the National Association of Criminal Defense Lawyers. These studies suggest that privilege is in fact much more influential in encouraging candor.<sup>136</sup> For example, a 2005 study by the Association of Corporate Counsel surveyed corporate counsel and found that attorneys believed ninety-three percent of senior employees of the companies they represent rely on the attorney-client privilege in sharing information with their counsel.<sup>137</sup>

While the results of these studies are mixed, an important division can be seen between random empirical studies and studies of members of particular professional associations. Studies “based on random selections and/or geographically based data sets[,] rather than interest group . . . surveys, challenge the [empirical] assumptions underlying the arguments for . . . absolute privilege, i.e., that substantially more (and substantially more candid) communication will occur between counsel and client, to the benefit of the justice system.”<sup>138</sup> It is worth emphasizing the fact that the professional association surveys noted above focus on attorneys’ beliefs about how the privilege operates to increase client candor.<sup>139</sup> Considering that modern privilege is held only by the client, a focus on the attorney’s view is likely less helpful than a client-based study. It seems, then, that when focusing on average clients of varying degrees of sophistication, the underlying instrumentalist assumption of attorney-client privilege is weak at best.<sup>140</sup> Yet despite findings suggesting candid communications would continue in the absence of privilege, courts continue to enforce the attorney-client privilege.<sup>141</sup>

---

133 *Id.* at 381.

134 Alexander, *supra* note 87, at 193.

135 Laurence A. Steckman & Richard Granofsky, *The Assertion of Attorney-Client Privilege by Counsel in Legal Malpractice Cases: Policy, Privilege, and the Search for Truth in Cases Involving Implied Waivers*, 45 TORT TRIAL & INS. PRAC. L.J. 839, 883 n.242 (2010) (discussing the results of the Alexander study).

136 *Id.* at 885–86.

137 *Id.* at 886 (citing *Association of Corporate Counsel Survey: Is the Attorney-Client Privilege Under Attack?*, ASS’N OF CORPORATE COUNSEL 2 (Apr.6, 2005), available at <http://www.acc.com/vl/public/Surveys/loader.cfm?csModule=security/getfile&pageid=16315&title=ACC%20Survey%3A%20Is%20the%20Attorney-Client%20Privilege%20Under%20Attack>).

138 *Id.* at 886.

139 *See id.* at 885–87.

140 *See id.*

141 *See, e.g., Baird v. Koerner*, 279 F.2d 623, 631–32 (9th Cir. 1960); *Prichard v. United States*, 181 F.2d 326, 328 (6th Cir. 1950).

Despite the insistence of federal courts that the instrumentalist rationale is the only justification for the attorney-client privilege,<sup>142</sup> it appears that noninstrumentalist justifications must be doing at least some of the work in preserving the privilege in the American legal system. In the absence of noninstrumentalist justifications, the empirical research suggests that an absolute attorney-client privilege is unnecessary; if instrumentalism was truly the only justification considered, courts would not continue to sacrifice their ability as factfinders to preserve the attorney-client privilege.<sup>143</sup> Because the attorney-client privilege continues in spite of the empirical studies noted above, courts appear to rely on at least some noninstrumentalist justifications in deciding questions of attorney-client privilege.<sup>144</sup> This is true in the context of both individual clients and corporate clients.<sup>145</sup>

The boundaries and proper application of the attorney-client privilege can be better comprehended with an understanding of both the instrumentalist and noninstrumentalist justifications for the privilege. With these views in mind, a review of the legal standards of inadvertent and implied waiver is appropriate. The next Section will examine the current state of the Federal Rules of Evidence and their application in cases regarding privilege and waiver.

### C. *Legal Standards of Inadvertent and Implied Waiver*

Though certain aspects of privilege in the United States have remained largely the same since the Founding,<sup>146</sup> other areas of the law, such as implied and inadvertent waiver, have been considerably more flexible. This Part will focus on the development and current status of inadvertent waiver

---

142 See, e.g., *Baird*, 279 F.2d at 631–32.

143 See, e.g., *Hawkins v. Stables*, 148 F.3d 379, 383 (4th Cir. 1998) (noting that the privilege “impedes [the] full and free discovery of the truth” (alteration in original) (quoting *In re Grand Jury Proceedings*, 727 F.2d 1352, 1355 (4th Cir. 1984))).

144 But cf. Elizabeth G. Thornburg, *Sanctifying Secrecy: The Mythology of the Corporate Attorney-Client Privilege*, 69 NOTRE DAME L. REV. 157, 183 (arguing that both instrumentalist and noninstrumentalist justifications for the attorney-client privilege are grounded in “myth[s],” and that these myths are “often exaggerated” in the noninstrumentalist context).

145 But cf. Melanie B. Leslie, *Government Officials as Attorneys and Clients: Why Privilege the Privileged?*, 77 IND. L.J. 469, 485–86 (2002); Thornburg, *supra* note 144, at 185 (arguing that noninstrumentalist justifications are even less compelling when applied to corporations, because “[w]hile corporations are in many instances treated as fictitious persons, they are not in fact persons, and the arguments made for personal confidentiality cannot simply be transferred to corporate clients,” and that “[c]orporations, unlike humans, have no right to individual autonomy, and no legal or moral claims to dignity” (footnotes omitted) (internal quotation marks omitted)). While these arguments have some appeal, noninstrumentalist justifications as applied to corporations should not be quickly dismissed, considering that the Supreme Court has upheld the right of corporations to exercise other, seemingly very personal, rights. See, e.g., *Burwell v. Hobby Lobby Stores, Inc.*, 134 S. Ct. 2751, 2759 (2014) (upholding the free exercise rights of a closely held, for-profit corporation).

146 See *supra* notes 81–85 and accompanying text.

and address the primary justifications for inadvertent waiver in the United States today.

Two basic classes of communications are relevant here: first, those that fall outside the boundary of attorney-client privilege in the first place—these communications are unprivileged and are not relevant to the purposes of this Note; and second, communications that initially fall within the scope of attorney-client privilege but, for one reason or another, find the privilege over the communication waived.

While these are important distinctions to make, the immediate result of unprivileged communication and a communication for which privilege has been waived is the same: the communication is not protected.<sup>147</sup> An important distinction between unprivileged communications and situations of waived privilege is the permanence of the admissibility of the communication at issue. All things being equal, an unprivileged communication was potentially admissible from the start and will remain unprivileged.<sup>148</sup> The waiver of privilege over a once-privileged communication, meanwhile, is not always permanent; there are circumstances in which an inadvertent waiver of privilege, for example, may be cured.<sup>149</sup>

It is the latter situation that is of primary concern for the purposes of this Note. There is no reason to think that an otherwise unprivileged communication should enjoy privilege merely because the contents of the communication were compromised as part of a bulk data collection program.

This Note will focus on one particular issue of implied waiver that may be called the “eavesdropper”<sup>150</sup> or “bystander”<sup>151</sup> exception. This form of waiver “generally applies where information is communicated in the presence of a third party,”<sup>152</sup> and waiver can be in effect even where the disclosure to a third party is inadvertent.<sup>153</sup> Under the early common law, however, even the theft of a confidential document or clandestine eavesdropping would create a waiver of privilege.<sup>154</sup> The rationale underlying the eavesdropper exception is that a party should not enjoy privilege over communications “where the party asserting the privilege was somehow derelict in protecting the communication.”<sup>155</sup> This rule was grounded in the observa-

---

147 See 8 CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 2016.2 (Supp. 2014).

148 *Id.*

149 *Id.*

150 R. Aubrey Davis III, *Big Brother the Sneak or Big Brother the Sentry—Does a New Bureau of Prisons Regulation Truly Abrogate the Attorney Client Privilege?*, 27 HAMLINE L. REV. 163, 176 (2004).

151 *Suburban Sew ‘N Sweep, Inc. v. Swiss-Bernina, Inc.*, 91 F.R.D. 254, 258 (N.D. Ill. 1981).

152 Davis, *supra* note 150, at 176 (citing *Conn. Mut. Life Ins. Co. v. Shields*, 18 F.R.D. 448, 451 (S.D.N.Y. 1955)).

153 Davis, *supra* note 150, at 177.

154 RICE, *supra* note 72, § 9:28.

155 Davis, *supra* note 150, at 177 (citing *Eigenheim Bank v. Halpern*, 598 F. Supp. 988, 991 (S.D.N.Y. 1984)).

tion that once the confidentiality of the underlying communication had been lost, there was simply no confidentiality left to protect.<sup>156</sup>

In an effort to resolve the inconsistencies that developed in federal caselaw regarding the rules of waiver,<sup>157</sup> the federal courts adopted Federal Rule of Evidence (FRE) 502.<sup>158</sup> Rule 502 was aimed particularly at “resolv[ing] some longstanding disputes in the courts about the effect of certain disclosures of communications or information protected by the attorney-client privilege . . . specifically those disputes involving inadvertent disclosure.”<sup>159</sup> The rule seeks to “provide a predictable, uniform set of standards” for determining the results of disclosures of attorney-client communications.<sup>160</sup>

The committee notes to FRE 502 highlight the differing conclusions courts arrived at when deciding whether an inadvertent disclosure would constitute an implied waiver of the attorney-client privilege.<sup>161</sup> A small minority of courts only found waiver where disclosures were intentional; a separate minority of courts applied waiver strictly, without regard for whether the party took reasonable steps to avoid disclosure; and a majority of courts adopted a third approach, examining whether the party had taken reasonable steps to protect the communication.<sup>162</sup> Under that approach, if the party did take reasonable steps, no waiver would be implied. If not, the attorney-client privilege dissolved. FRE 502(b) states:

Disclosure. . . . in a federal proceeding . . . does not operate as a waiver [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).<sup>163</sup>

In doing so, the rule adopts the third approach noted above by looking to—among other things—the disclosing party’s precaution in protecting its communication.<sup>164</sup>

156 RICE, *supra* note 72, § 9:28.

157 See Elizabeth King, *Waving Goodbye to Waiver? Not So Fast: Inadvertent Disclosure, Waiver of the Attorney-Client Privilege, and Federal Rule of Evidence 502*, 32 CAMPBELL L. REV. 467, 514 (2010) (noting that the factors before Rule 502 “are open to varied interpretations” and that Rule 502 itself has a “[p]otential for [u]npredictability”).

158 FED. R. EVID. 502 advisory committee’s note.

159 *Id.*

160 *Id.*

161 See *id.*

162 *Id.*

163 *Id.* 502(b).

164 *Id.*

The first of the three prongs of FRE 502(b)—inadvertence—is “a simple one”<sup>165</sup>: courts will look to whether the disclosure was unintentional and unknowing.<sup>166</sup> While courts traditionally placed a limit on what would be accepted as inadvertent—a grossly negligent disclosure, for example, would likely be treated as intentional<sup>167</sup>—today the calculus is much more straightforward.<sup>168</sup>

The second and third steps to applying Rule 502 are largely in line with the weighing of factors seen in traditional common law. While the rule does not explicitly adopt any caselaw, the Committee’s notes point to *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*<sup>169</sup> and *Hartford Fire Insurance Co. v. Garvey*<sup>170</sup> as establishing useful factors courts might consider when applying FRE 502’s test.<sup>171</sup> In *Lois Sportswear*, Levi Strauss allowed Lois to review some 30,000 documents held at Levi’s office in response to an interrogatory from Lois as part of litigation.<sup>172</sup> After examination of the documents, Lois requested production of roughly 3,000 documents, at which point Levi Strauss realized many of the documents contained privileged materials.<sup>173</sup> In determining whether the inadvertent disclosure constituted a waiver of privilege, the Southern District of New York looked to five elements to determine whether a waiver occurred: (1) the precautions taken to prevent the disclosure; (2) how long it took to rectify the disclosure; (3) the scope of discovery; (4) the extent of the disclosure relative to the scope of discovery; and (5) overarching considerations of fairness and protection of the privilege.<sup>174</sup> While a court is not bound to apply these elements as they appeared in *Lois Sportswear*, FRE 502 accommodates each of them.<sup>175</sup>

In contrast with the harsh rule under early common law that waived privilege when communications were “purloined,”<sup>176</sup> modern courts have generally approached the issue more in line with the balancing factors seen in the *Lois Sportswear* and *Hartford Fire Insurance* cases above. Importantly, the harsh

165 RICE, *supra* note 72, § 9:73 n.1 (phrasing the inquiry as whether “the disclosure occur[ed] by mistake or unintentionally” (quoting *Datel Holdings, Ltd. v. Microsoft Corp.*, No. C-09-05535 EDL, 2011 WL 866993, at \*3, \*11 (N.D. Cal. Mar. 11, 2011))).

166 See *Sidney v. Focused Retail Prop. I, LLC*, 274 F.R.D. 212, 215 (N.D. Ill. 2011); *Amobi v. D.C. Dep’t of Corr.*, 262 F.R.D. 45, 53 (D.D.C. 2009).

167 See, e.g., *Ciba-Geigy Corp. v. Sandoz Ltd.*, 916 F. Supp. 404, 411 (D.N.J. 1995) (“While an inadvertent disclosure is, by definition, an unintentional act, if such a disclosure results from gross negligence, courts following the third approach will deem the disclosure to be intentional, thus constituting a waiver of the privilege.”).

168 See, e.g., *Amobi*, 262 F.R.D. at 53 (“Rule 502(b) provides for a more simple analysis of considering if the party intended to produce a privileged document or if the production was a mistake.”).

169 104 F.R.D. 103 (S.D.N.Y. 1985).

170 109 F.R.D. 323 (N.D. Cal. 1985).

171 FED. R. EVID. 502 advisory committee’s note.

172 *Lois Sportswear*, 104 F.R.D. at 104.

173 *Id.* at 104–05.

174 *Id.* at 105; see *Hartford Fire*, 109 F.R.D. at 332.

175 FED. R. EVID. 502(b) advisory committee’s note.

176 RICE, *supra* note 72, § 9:28.

line of thinking that lack of confidentiality eliminates the purpose for privilege has been relaxed; the modern view is better illustrated by *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc.*, which found modern cases “reveal[ ] that the privilege is not simply inapplicable any time that confidentiality is breached . . . [but rather,] the relevant consideration is the intent of the [party asserting privilege] to maintain the confidentiality of the documents as manifested in the precautions they took.”<sup>177</sup>

No federal court has dealt directly with the eavesdropping or purloined communications issue since the adoption of FRE 502. It is clear, however, that modern courts will look to the client’s actions and generally allow the privilege to stand in the context of eavesdropping when the client is not responsible for the breach of confidentiality.<sup>178</sup> Importantly, however, the burden is on the party asserting the privilege in the eavesdropping situation to show that the other party improperly acquired the communications.<sup>179</sup> Where the party asserting the privilege cannot do so, that will serve as “prima facie evidence that the client has failed to satisfy his duty to maintain the confidentiality of those [communications].”<sup>180</sup>

The modern standard seen in FRE 502(b) largely represents the majority approach used at common law. Courts will not automatically waive the privilege upon loss of confidentiality, but they will require a showing from the party asserting the privilege that they adequately guarded the disclosure. Because FRE 502 accommodates the middle ground adopted by courts demonstrated in *Levi Strauss*, there is little reason to believe that FRE 502 substantially changes the landscape of waiver with regard to eavesdropping.

### III. THE ATTORNEY-CLIENT PRIVILEGE IN LIGHT OF BULK DATA COLLECTION

#### A. Analysis

While there is an almost incomprehensible volume of caselaw developing the boundaries of attorney-client privilege, no court has yet addressed the issue of privilege and waiver as a result of bulk data collection and sharing. As with the advent of other technologies, there is surely at least some reason to think that novel waiver issues will emerge as a result.<sup>181</sup>

As noted in Part I, the 2008 amendments to FISA are frequently cited as having paved the way for bulk data collection programs.<sup>182</sup> For all the expansion of bulk data collection, however, FISA does explicitly address privileged

---

177 *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc.*, 91 F.R.D. 254, 260 (N.D. Ill. 1981) (quoted in RICE, *supra* note 72, § 9:28).

178 RICE, *supra* note 72, § 9:28.

179 *Id.*

180 *Id.*

181 See, e.g., Anne G. Bruckner-Harvey, *Inadvertent Disclosure in the Age of Fax Machines: Is the Cat Really Out of the Bag?*, 46 BAYLOR L. REV. 385, 385–86 (1994) (describing a scenario in which a legal secretary accidentally speed-dials a fax of sensitive documents to an unprivileged attorney).

182 See *supra* Part I.

communications as part of the Act's "minimization procedures."<sup>183</sup> The statute states that "[n]o otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character."<sup>184</sup> Coupled with the above explanation of bulk data collection and attorney-client privilege, this statutory protection raises some fundamental questions.

The first and perhaps most important question is whether the minimization procedures implemented by statute are sufficient to protect the attorney-client privilege. While the statute governing the "[u]se of information" gathered under FISA contains provisions directed at safeguarding privileged information,<sup>185</sup> the statutory scheme only speaks to the operations of the American intelligence apparatus.<sup>186</sup> As General Alexander carefully articulated, the "NSA cannot and does not ask its foreign partners to conduct any intelligence activity that it would be prohibited from conducting itself in accordance with U.S. law."<sup>187</sup> To some extent, this is reassuring. However, the statement is notable in its silence on the issue that spurred the ABA to write its letter to the NSA in the first place: where foreign intelligence agencies like the Australian Signals Directorate collect the communications of an American law firm without the request of the NSA and apparently share that information despite its privileged nature.<sup>188</sup> These communications would not have been obtained under FISA, which again deals only with American intelligence gathering.<sup>189</sup> Nor does the collection appear to be in violation of FISA, for the same reasons. The statutory minimization procedures, then, may not resolve the ABA's concerns.

Despite this shortcoming, additional procedures exist to protect privileged communications obtained as part of a bulk data collection program. The NSA has implemented its own minimization procedures in addition to those required by statute,<sup>190</sup> and these procedures include measures dedicated to handling attorney-client communications.<sup>191</sup> The NSA's minimization procedures, however, only address communications between attorneys and their clients who are "known to be under criminal indictment in the United States."<sup>192</sup> Where that is the case, the privileged communications must be segregated and the National Security Division of the Department of

---

183 50 U.S.C. § 1806(a) (2012).

184 *Id.*

185 *Id.*

186 *See* 50 U.S.C. §§ 1881–1881g.

187 Gen. Alexander Letter, *supra* note 12, at 1.

188 *See supra* notes 5–7.

189 *See* 50 U.S.C. § 1802.

190 Memorandum, NSA, Minimization Procedures Used by the National Security Agency in Connection with Acquisition of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (Oct. 31, 2011) [hereinafter *Minimization Procedures*].

191 *Id.* at 7–8.

192 *Id.* at 7.

Justice notified so that the communications can be protected “from review or use in any criminal prosecution.”<sup>193</sup>

In the criminal context, then, the NSA’s minimization procedures are reassuring, but the treatment of certain other communications remains unclear. For example, the NSA’s procedures do not address the circumstances under which circumstances under which communications may be disseminated outside of the NSA.<sup>194</sup> Further, the minimization procedures for attorney-client communications are silent when the communications surround noncriminal issues.<sup>195</sup> Importantly, the very event that spurred the ABA to write to General Alexander is not addressed by the statutory minimization procedures nor the NSA’s own procedures for safeguarding collected data. As a result, the ABA’s initial concerns seem well founded; the collected communications in that situation were not categorically protected.

### B. Proposed Solutions

Considering the apparent sharing of information outside the scope of the statutory and NSA minimization procedures for privilege, the possibility that purloined communications could be submitted during litigation should not be ignored. To demonstrate the issues a court may have to grapple with as a result of these recently revealed technologies, it is helpful to consider potential litigation. Consider the following hypothetical situation: a foreign corporation hires an American law firm to represent it in a civil dispute in a federal court in the United States. As part of unrelated surveillance, a foreign, friendly government collects communications—here, typical password protected email—between the company and its American counsel, sharing them with the NSA. While there is no way to know exactly what happens next,<sup>196</sup> imagine these communications are eventually submitted as evidence in the civil litigation.

A court asked to determine whether these imagined communications remain privileged will not find an answer in FISA’s black letter rule. Courts should thus be prepared to evaluate the communications under FRE 502 and some or all of the five factors noted in *Lois Sportswear*<sup>197</sup> to determine whether the communications remain privileged, or if the privilege was waived when the communications were purloined. This scenario raises some substantial unsettled issues. In determining the status of the communications, courts will need to consider how to treat the information gathered as part of bulk data collection programs. Luckily, FRE 502(b) is equipped to answer

---

193 *Id.* at 8.

194 See David L. Hudson Jr., *NSA Surveillance Policies Raise Questions About the Viability of the Attorney-Client Privilege*, ABA JOURNAL (Sept. 1, 2014, 8:49 AM), [http://www.abajournal.com/magazine/article/nsa\\_surveillance\\_policies\\_raise\\_questions\\_about\\_the\\_viability\\_of\\_the\\_attorn/](http://www.abajournal.com/magazine/article/nsa_surveillance_policies_raise_questions_about_the_viability_of_the_attorn/).

195 See *Minimization Procedures*, *supra* note 190.

196 See *supra* note 190.

197 See *supra* notes 173–75 and accompanying text.

the necessary questions to determine whether a communication should retain its privileged status.

To begin the analysis, courts should consider communications gathered under a bulk data collection scheme to be inadvertently disclosed pursuant to FRE 502(b). After all, the question for determining whether a disclosure was inadvertent is a simple one: whether the disclosure was in fact unintentional and unknowing.<sup>198</sup> Disclosures as the result of a bulk data program will surely be unknown to the parties and be unintentional from the communicating party's perspective. As a result, FRE 502 should apply to disclosures arising from bulk data collection.

This leads to a second important question. It will be crucial for courts to determine whether "the holder of the privilege or protection took reasonable steps to prevent disclosure."<sup>199</sup> This raises a vexing question: Just what are "reasonable steps to prevent disclosure" in a time when bulk data collection is largely common knowledge?<sup>200</sup> The current regime of bulk data collection is, after all, largely in the open; it has been publicly acknowledged and its legality publicly defended.<sup>201</sup> If the hypothetical foreign client retains an American law firm, a court applying FRE 502(b)'s reasonable steps test might show serious skepticism to the notion that the client took reasonable precautions to protect the communications when it is widely known that its communications could be collected and shared in the wake of the recent NSA disclosures.

Courts deciding this issue should keep in mind the justifications underlying the attorney-client privilege, and apply the rule in a way that furthers those justifications. Both the instrumentalist and noninstrumentalist rationales favor an application of the rule that would tend to uphold privilege in the hypothetical situation described above. The instrumentalist justification for attorney-client privilege suggests that courts should ask whether the existence of privilege in this situation furthers the policy goal of client candor, and uphold the privilege only where that is the case.<sup>202</sup> Some attorneys have voiced concerns over disintegration of client trust and the deterioration of client relationships as a result of the NSA's receipt of privileged communica-

---

198 See, e.g., *Sidney v. Focused Retail Prop. I, LLC*, 274 F.R.D. 212, 216 (N.D. Ill. 2011) (finding that Rule 502(b) simply "ask[s] whether the party intended a privileged or work-product protected document to be produced or whether the production was a mistake" (quoting *Coburn Grp., LLC v. Whitecap Advisors LLC*, 640 F. Supp. 2d 1032, 1038 (N.D. Ill. 2009))); *RICE*, *supra* note 72, § 9:73 n.1 (stating the inquiry as, "did the disclosure occur by mistake or unintentionally?" (quoting *Datel Holdings, Ltd. v. Microsoft Corp.*, No. C-09-05535 EDL, 2011 WL 866993, at \*3, \*11 (N.D. Cal. Mar. 11, 2011))).

199 FED. R. EVID. 502(b)(2).

200 See *supra* Section I.A.

201 See, e.g., President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *transcript available at* <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence> ("[N]othing . . . indicated that our intelligence community has sought to violate the law or is cavalier about the civil liberties of their fellow citizens.").

202 See *supra* note 99 and accompanying text.

tions.<sup>203</sup> While the concerns of attorneys may reflect client behavior—it is after all intuitive that finding against the existence of privilege in this hypothetical situation would discourage client candor—the focus should not be on attorneys’ beliefs, but rather on clients’ behavior. Because of the recentness of the NSA revelations and thus the dearth of empirical data regarding client behavior in response to data collection, the instrumentalist justification is admittedly attenuated. Even in the absence of a compelling instrumentalist justification, however, there are other reasons to uphold the existence of the attorney-client privilege in this situation.

Noninstrumentalist justifications—though oft rejected by courts<sup>204</sup>—are at play when courts answer questions of privilege; there should be no difference here. Noninstrumentalist justifications are particularly apposite in this hypothetical scenario. A noninstrumentalist view of this situation might hold that there are very real benefits to the existence and protection of truly private areas in society, and that in a liberal democracy, “it is distasteful for citizens to ‘be[] continually alert for possible’ eavesdroppers.”<sup>205</sup> This reflects Professor Fried’s argument that it is immoral to bar a person from learning “the limits of [society’s] power over him.”<sup>206</sup> A noninstrumentalist justification might hold that privilege in this hypothetical situation should be protected to ensure client privacy and allow them to adequately secure their rights by confidentially communicating with counsel. Even if it should be found that the collection of attorney-client communications does not curb client candor (and thus does not implicate instrumentalist justifications), noninstrumentalism provides valid reasons to uphold privilege—reasons courts appear to consider even where they credit only instrumentalist justifications.<sup>207</sup>

With these justifications in mind, recall that FRE 502(b)(2) directs courts to evaluate whether the holder of the privilege took “reasonable steps to prevent disclosure.”<sup>208</sup> Again, a hypothetical court may question whether a foreign client sending a typical email to its American law firm took reasonable precautions to keep their communications confidential. Potential answers to this question can be divided in two broad categories. The first category, a strict approach, would adopt the view that a foreign client sending the typical email message to its American attorney simply did not take a reasonable step to protect the communication in light of the well-publicized nature of bulk data collection. At the other extreme, a second category would hold that clients and firms need not take extraordinary measures to

---

203 Allison Grande, *Report of NSA Spying on Mayer Brown Rattles Other Firms*, LAW 360 (Feb. 18, 2014, 9:09 PM), <http://www.law360.com/articles/510770/report-of-nsa-spying-on-mayer-brown-rattles-other-firms>.

204 See *supra* Section II.B.

205 IMWINKELRIED, *supra* note 101, § 6.6.3 (alterations in original) (quoting Thomas Scanlon, *Thomson on Privacy*, 4 PHIL. & PUB. AFF. 315, 317, 320 (1975)).

206 See *supra* note 120.

207 See *supra* notes 131–41 and accompanying text (citing empirical research).

208 FED. R. EVID. 502(b)(2).

protect their communications from bulk data collection; rather, the typical password protected email and a belief that the email is secure is adequate. This view might be called a relaxed approach. Each of these categories has certain appeals, but courts should ultimately favor the latter approach—with the understanding that a one-size-fits-all approach will ultimately fit none.

The five factors from *Lois Sportswear*<sup>209</sup> will surely play a role in these decisions. However, three of those factors are particularly fact-specific and could vary tremendously from case to case. The most prominent of the five factors listed in that case is “the precautions taken to prevent the disclosure,” which can be applied more uniformly than the other factors. Another factor, “considerations of fairness and protection of the privilege” can also shed light on how courts should consider FRE 502(b)(2) issues in the context of bulk data collection.

A strict approach will rely on a significant assumption: that clients and attorneys do in fact have the ability to adequately shield their communications from surveillance. Although emails can be encrypted through a number of means,<sup>210</sup> this assumption seems somewhat unlikely. It is “hard to imagine that many law firms could afford the kind of robust technical expertise required to stop intelligence services from getting through” to the communications.<sup>211</sup> An approach that requires foreign clients to take an additional step before communicating with their attorneys is undesirable; it may reduce client candor by making each communication more cumbersome, and might simply deter foreign clients from making use of American law firms. The strict approach, then, may lead to a “Hobson’s choice.”<sup>212</sup> The flaw of this approach is magnified considering that it leads back to the initial question: If a foreign client knows that they likely lack the capabilities to truly secure their communications from collection, why should the token step of encrypting the communications be of any aid? A view of “reasonable precautions” that requires going above and beyond normal email communications might effectively leave foreign clients with no options; declining to press send, however, should not be a client’s only alternative.

A more relaxed approach, meanwhile, could account for the notion that private entities are unlikely to possess the ability to truly protect their com-

---

209 *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985) (“The elements which go into that determination include the reasonableness of the precautions to prevent inadvertent disclosure, the time taken to rectify the error, the scope of the discovery and the extent of the disclosure. There is, of course, an overreaching issue of fairness and the protection of an appropriate privilege which, of course, must be judged against the care or negligence with which the privilege is guarded with care and diligence or negligence and indifference.”).

210 For an overview of just one common encryption protocol, SSL encryption, see *In re Under Seal*, 749 F.3d 276, 279–80 (4th Cir. 2014) (explaining the basic processes and results of encryption).

211 Grande, *supra* note 203 (quoting Claudia Rast, Butzel Long PC shareholder).

212 Thomas Mullaney & Elad Yoran, *PRISM Scatters Attorney-Client Privilege*, LAW 360 (Jul. 17, 2014, 5:48 PM), <http://www.law360.com/articles/558606/prism-scatters-attorney-client-privilege>.

munications from governmental bulk data collection. This allows for two benefits. First, assuming the foundations of the instrumentalist view were supported by empirical study, this approach (unlike the strict approach) might protect the goal of client candor by ensuring that clients must not take additional steps before communicating with their American legal representation. Second, this approach would further the noninstrumentalist justifications of privilege in that clients could more easily secure their rights by consulting legal counsel.

Courts have an additional opportunity to safeguard the attorney-client privilege when applying FRE 502. An additional factor courts should consider is not found in the text of the rule, but rather is found in *Lois Sportswear*, which the committee notes to the rule point to for guidance.<sup>213</sup> That consideration is the “overreaching issue of fairness.”<sup>214</sup> Whether considerations of fairness weigh in favor of upholding the privilege of a communication “has been decided by the courts on a case-by-case basis, and depends primarily on the specific context in which the privilege is asserted.”<sup>215</sup> While the facts of individual cases will vary, in the hypothetical scenario above, the potential for unfairness to the client is clear. However, courts will consider whether the non-disclosing party has “already relied on the [communication] at issue,” and will be more likely to find unfairness toward the *non*-disclosing party where that has occurred.<sup>216</sup>

The hypothetical above, while meeting the requirements for inadvertent disclosure, differs significantly from previous cases when considered in the fairness context. Courts should be willing to examine the “overreaching issue of fairness” with an eye toward the party asserting the privilege in that situation, rather than the party attempting to overcome the privilege. The evaluation of fairness should not be seen as simply a review of the reasonable steps evaluation of FRE 502(b)(2); while the federal rule does not incorporate the fairness element expressly, its committee notes point to *Lois Sportswear*, which treats reasonable steps and fairness as separate considerations. This should leave courts the room to uphold privilege despite the inadvertent waiver of communications as a result of bulk data collection, even where the court may have doubts that a typical email communication is completely safe from collection.

#### CONCLUSION

The attorney-client privilege exists at least in part due to noninstrumentalist justifications. These justifications suggest that privacy and dignity are worthy of defense, even to the extent that doing so may impede the abil-

---

213 FED. R. EVID. 502(b) advisory committee’s note.

214 *Lois Sportswear*, 104 F.R.D. at 105.

215 *In re Grand Jury Proceedings*, 219 F.3d 175, 183 (2d Cir. 2000).

216 *See Bank Brussels Lambert v. Credit Lyonnais (Suisse) S.A.*, 160 F.R.D. 437, 446 (S.D.N.Y. 1995) (finding no unfairness or prejudice where a party in possession of the opponent’s privileged communications did not rely on the communications in preparing its case).

ity of a factfinder. Courts should approach questions of waiver in the context of bulk data collection with these justifications in mind. When applying FRE 502(b)(2)'s reasonable steps test, while considering the burden to place on clients in protecting their communications, a court should consider the practical disparities in technology between government intelligence agencies and law firms and their clients. Finally, because "[t]he attorney-client privilege is a bedrock legal principle of our free society,"<sup>217</sup> courts should consider using the element of fairness from *Lois Sportswear* as a means of protecting the attorney-client privilege from the new technologies of the twenty-first century, even where a more strict application of FRE 502 might suggest otherwise.

---

217 Silkenat Letter, *supra* note 8, at 1.

