12

Technology, Self-Inflicted Vulnerability, and Human Rights

G. Alex Sinha

I INTRODUCTION

Since 2013, perhaps no human rights issue has received as much sustained attention as the right to privacy. That was the year the first Snowden revelations reached the public, detailing sophisticated, large-scale US government surveillance programs designed to capture or analyze incredibly large volumes of digital data. In the weeks and months that followed, media reports confirmed that the US government had, at various recent points, run programs designed to scan and harvest data contained in e-mails, track Internet browsing activity, collect data from cell phones, collect digital contact lists (including e-mail and instant messaging contacts), and collect photographs of Internet users all over the world.[1] Other governments have been revealed to engage in similar practices.[2]

Targeting the use of digital technologies is an obviously fruitful approach for state surveillance programs. By the middle of 2016, one estimate placed worldwide Internet use at more than 3.5 billion people.[3] Cell phone use is even more widespread, with recent reports suggesting the world is approaching five billion

[1] For a brief summary of key Snowden revelations, see Human Rights Watch and American Civil Liberties Union, *With Liberty to Monitor All* (2014), pp. 8–11, www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf. In the interest of full disclosure, note that I was the researcher and author of that report. *See also* J. Risen and L. Poitras, "N.S.A. Collecting Millions of Faces from Web Images," *The New York Times*, May 31, 2014, www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html (describing the collection of photographs for facial recognition purposes).

[2] *See, e.g.*, R. Gallagher, "U.K.'s Mass Surveillance Databases were Unlawful for 17 Years, Court Rules," *The Intercept*, October 17, 2016, https://theintercept.com/2016/10/17/gchq-mi5-investigatory-powers-tribunal-bulk-datasets/.

[3] *See* "World Internet Usage and Population Statistics," Miniwatts Marketing Group, www.internetworldstats.com/stats.htm.

https://doi.org/10.1017/9781316838952.012 Published online by Cambridge University Press

mobile users.[4] Significant numbers of people also use other technologies conducive to tracking, such as E-ZPass or Global Positioning System (GPS) devices. Those numbers are likely to increase in the coming years, which is particularly significant because of the way in which digital technologies lend themselves to insecure use and mass surveillance.

The ongoing global conversation about the legality of surveillance practices has focused on a number of dimensions of the human right to privacy, but there has been little serious discussion of a major factor in the expansion of the insecure use of digital technologies: the user. A significant portion of the information collected by surveillance (or otherwise made vulnerable to unintended recipients) is exposed voluntarily, sometimes deliberately or knowingly, or with unjustified ignorance of the risks of transmitting it in a particular manner. This chapter argues that, as human rights bodies, governments, and advocacy groups seek to understand the protections provided by the human right to privacy, it is also essential to clarify the conditions (if any) under which a person may waive those protections. The purpose of this chapter is therefore to help launch a conversation about waiving the human right to privacy and the role of the state in fostering the ability of individuals to make better choices in protecting their privacy.[5]

II INDIVIDUAL CHOICE AND THE HUMAN RIGHT TO PRIVACY

The Snowden revelations have triggered increased engagement on the right to privacy among civil society organizations,[6] multiple votes within the United Nations General Assembly,[7] research by the United Nations High Commissioner for Human Rights,[8] and the establishment of a new special rapporteur on privacy by the Human Rights Council.[9] Pressure is also building on the Human Rights Committee to

[4] "Number of mobile phone users worldwide from 2013 to 2019 (in billions)," Statista, www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/.

[5] "Waiver" here is defined narrowly; it refers to discrete choices or events that remove specific, otherwise-protected information from under the umbrella of the human right to privacy (instead of a broad, blanket alienation of the right to privacy for all of one's protected matters).

[6] *See, e.g.*, *With Liberty to Monitor All*; "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor," PEN American Center, https://pen.org/chilling-effects; "Surveillance Self-Defense," Electronic Frontier Foundation, https://ssd.eff.org/en; A. Toh, F. Patel, and E. Goitein, "Overseas Surveillance in an Interconnected World," Brennan Center for Justice, www.brennancenter.org/publication/overseas-surveillance-interconnected-world.

[7] *See* G.A. Res. 68/167, *The right to privacy in the digital age*, U.N. Doc. A/Res/68/167 (December 18, 2013); G.A. Res. 69/166, *The right to privacy in the digital age*, U.N. Doc. A/Res/69/166 (December 18, 2014).

[8] Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, U.N. Doc. A/HRC/27/37 (June 30, 2014).

[9] *See* "Human Rights Council creates mandate of Special Rapporteur on the right to privacy," Office of the United Nations High Commissioner for Human Rights, March 26, 2015, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15763&LangID=E.

update its interpretation of the right to privacy under the International Covenant on Civil and Political Rights (ICCPR), primarily to account for changes in circumstances and technological developments that render its previous interpretation from the 1980s practically obsolete.[10]

This flurry of activity has largely left aside the relevance of individual users and the choices they make in the storage and transmission of their private information. Consider the state of the debate about US human rights obligations related to privacy – obligations that have occupied center stage since media outlets began publishing the Snowden revelations. Although a number of international agreements address the right to privacy,[11] a primary source of human rights obligations for the United States is the ICCPR, to which the United States has been a party since 1992. Article 17 of the ICCPR stipulates that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence ... [and e]veryone has the right to the protection of the law against such interference."[12] Additional articles in the covenant inform the scope and rigidity of individual rights, such as by addressing the geographic range of state duties under the covenant or the conditions under which a right might be limited or outweighed by other considerations (such as protecting national security).

The ICCPR does not explicitly address the role of individual choice in connection with the right to privacy,[13] which means choice has not factored much into a debate that has largely followed the text of the covenant. For example, a significant dispute has arisen about the meaning of the covenant's ban on "arbitrary" and "unlawful" interference with protected privacy interests.[14] Multiple UN rights experts have recently concluded that non-arbitrariness requires states, *inter alia*, to ensure the *necessity* of interferences with the right to privacy and the *proportionality* of their invasive practices.[15] Such requirements are intended to ensure the

[10] *See, e.g.*, American Civil Liberties Union, *Information Privacy in the Digital Age* (New York: ACLU Foundation, 2015), www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf; G. Alex Sinha, "NSA Surveillance Since 9/11 and the Human Right to Privacy" (2014) **59** *Loyola Law Review* 861–946.

[11] *See, e.g.*, G.A. Res. 217 (III) *A Universal Declaration of Human Rights*, art. 12 (December 10, 1948); Inter-Am. Comm'n H.R. 9th Conf., *American Declaration of the Rights and Duties of Man*, art. V (May 2, 1948); Council of Europe, *European Convention on Human Rights*, art. 8.

[12] International Covenant on Civil and Political Rights ("ICCPR"), art. 17.

[13] Two ICCPR Articles, 18 and 19, do refer to individual choice (to one's right to choose a belief system and to choose preferred media, respectively). *See* ICCPR, arts. 18, 19. But those choices are essential to the rights themselves rather than related to the waiver of a covenant right. Ibid.

[14] ICCPR, art. 17.

[15] *See, e.g.*, "Privacy in the Digital Age," ¶¶ 22–23; *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, ¶ 17, U.N. Doc. A/HRC/13/37 (December 28, 2009); *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, ¶ 29, U.N. Doc. A/HRC/23/4 (April 17, 2003); *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, ¶ 29, U.N. Doc. A/HRC/29/32 (May 22, 2015).

continued relevance of the human right to privacy in the digital era and would, in theory, provide a check on large-scale surveillance of the sort revealed by Snowden.[16] Thus far, however, the United States has rejected requirements like necessity and proportionality, arguing that those standards do not necessarily follow from a ban on arbitrary and unlawful interference.[17] Instead, the United States insists that its programs need only be (and consistently are) "reasonable" because they are authorized by law and not arbitrary.[18]

Another dispute concerns the geographic scope of state duties under the covenant. Article 2(1) provides that "[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant."[19] The United States typically interprets the phrase "within its territory and subject to its jurisdiction" conjunctively, such that it only accepts duties under the covenant toward people of whom both modifiers are true.[20] Key human rights bodies, including the Human Rights Committee (the UN body tasked with interpreting the ICCPR), have rejected that reading and interpret the phrase disjunctively.[21] This disagreement has garnered increased attention as a result of US surveillance

[16] In light of the consensus coalescing among those human rights bodies, advocacy groups like the American Civil Liberties Union have attempted to map out in substantial detail the nature of state obligations under Article 17. *See*, *e.g.*, "Informational Privacy in the Digital Age."

[17] *See*, *e.g.*, K. L. Razzouk, "Explanation of Position on draft resolution L.26/ Rev. 1 The Right to Privacy in the Digital Age," http://usun.state.gov/remarks/6259 (the link was active at the time of this writing).

[18] *See* ibid.; ICCPR art. 17(1).

[19] ICCPR art. 2(1).

[20] While he was a legal advisor at the US State Department, Harold Koh advocated for relaxing that standard and accepting that some ICCPR obligations might attach to US conduct outside of its own territory. *See* Harold Hongju Koh, "Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights," www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf. As recently as its 2015 submission to the Human Rights Committee, which monitors state compliance with the ICCPR, the United States has nevertheless continued to assert the original, narrower view. *See* Permanent Mission of the United States of America to the Office of the United Nations, "One-Year Follow-up Response of the United States of America to Priority Recommendations of the Human Rights Committee on its Fourth Periodic Report on Implementation of the International Covenant on Civil and Political Rights," ¶ 33, www.state.gov/documents/organization/242228.pdf. By contrast, the United States has softened its position on the extraterritorial obligations under another human rights convention, the Convention Against Torture. White House Office of the Press Secretary, "Statement by NSC Spokesperson Bernadette Meehan on the U.S. Presentation to the Committee Against Torture," www.whitehouse.gov/the-press-office/2014/11/12/statement-nsc-spokesperson-bernadette-meehan-us-presentation-committee-a.

[21] *See*, *e.g.*, Human Rights Committee, "Concluding observations on the fourth report of the United States of America," ¶ 4, www.justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf. *See also* Ryan Goodman, "UN Human Rights Committee Says ICCPR Applies to Extraterritorial Surveillance: But is that so novel?," www.justsecurity.org/8620/human-rights-committee-iccpr-applies-extraterritorial-surveillance-novel/.

revelations, because the narrower position turns would-be beneficiaries of human rights protection into unprotected targets of surveillance.

Yet another dimension of the ongoing debate about the human right to privacy concerns the limitations clauses built into the ICCPR. The United States has emphasized that it takes a broad reading of those limitations – especially the national security limitation articulated in, among other places, Articles 19, 21, and 22.[22] The US government routinely cites national security considerations to justify practices of concern to human rights bodies, including surveillance.[23] The implications of that approach are far-reaching in light of the ongoing War on Terror, which lacks any obvious or imminent endpoint.

Overall, the contours of this debate are unsurprising; the language of the covenant is a natural focal point for states and human rights bodies alike, and their disagreements, in turn, frame the contributions of interested advocacy groups. But the issue of personal choice casts a shadow over all such textual analysis. It is surely uncontroversial that one can, at least sometimes, waive privacy protection for particular pieces of information by exposing them to collection.[24] It should also be uncontroversial that some digital information, even if it can be obtained by intelligence agencies or hackers, remains protected by the human right to privacy. Yet through the insecure use of digital technologies, people increasingly expose enormous swaths of protected information with unclear levels of intentionality and culpability – even as the covenant remains silent on waiver generally and the ongoing debates about the human right to privacy fail to provide much clarity. The conditions under which one waives legal privacy protections are therefore both extremely important and extremely unclear.

Vulnerability can be chosen, such as when people share private information in public fora (like public websites). It can be recklessly or negligently assumed, such as when people undertake to store or transmit personal information in insecure ways (whether knowingly or because they lack a reasonable appreciation for the risk). It can arise through no fault of a user when it results from justifiable ignorance on the user's part. And it can be imposed by circumstance in spite of a user's best efforts, such as by the mere fact that surveillance authorities and hackers around the world typically have more power to harvest information than even the most committed individuals have to protect it. Any reasonable understanding of the waiver of the right to privacy must account for different notches on this spectrum.[25]

[22] *See* ICCPR, arts. 19, 21, 22.

[23] *See, e.g.*, US Department of State, "Report of the United States of America Submitted to the U.N. High Commissioner for Human Rights in Conjunction with the Universal Periodic Review," ¶ 83, www.state.gov/j/drl/upr/2015/237250.htm; "One-Year Follow-up Response," ¶ 29.

[24] Truly public information – especially information one has *chosen* to make public – can likely be collected without interfering with a person's privacy, family, home, or correspondence. It is therefore difficult to see how it could fall within the scope of Article 17.

[25] In the context of US constitutional law, one is protected from searches and seizures by government agents when one has a reasonable expectation of privacy. Whether the proper

For simplicity, we might assume that posting private information – say, political leanings and hobbies – on a public Facebook page constitutes some sort of waiver of privacy protection for that information, meaning that such information would fall outside the scope of the protections contained in Article 17. But what about intermediate cases that expose us to broader-than-intended intrusions, such as posting the same information on a semipublic Facebook page that is set to restrict access only to approved "friends"? Or sending sensitive information via unencrypted e-mail to a single recipient? Or running a sensitive Google search from a personal computer alone in one's home? Or carrying a cell phone that could just as well connect to a stingray as a cell phone tower? Or attempting to send an encrypted message but accidentally sending the message unencrypted?

These examples underscore a complicating underlying factor: Even when we want to protect our privacy, we are often fundamentally incapable of employing digital technology securely, whether due to ignorance, lack of skill, or inherent limitations in the technology itself. Yet we constantly use such technology anyway. Consider the example of the United States, which in some ways is a particularly risky place for such a casual approach to technology. Not only does the United States aggressively gather as much data as it can through perhaps the most powerful surveillance apparatus in the world, but it also features some problematic legal precedents for privacy under domestic law.

A string of Supreme Court cases has established the legal principle that voluntary disclosure of information to third parties eliminates one's expectation of privacy for that information, thereby defeating constitutional privacy protections that would require law enforcement to get a warrant for it.[26] In several cases decided between 1952 and 1971, the court consistently held that the Fourth Amendment prohibition on unreasonable search and seizure does not apply to the contents of a person's utterances that are voluntarily communicated to a government agent or informant.[27] A second series of cases, decided between 1973 and 1980, extended that rule to business records that are provided to a third party. For example, in *United States v. Miller*, the Supreme Court ruled that there is no reasonable expectation of privacy in checks and deposit slips provided to banks, as those are "negotiable instruments" rather than "confidential communications" and the data they contain are

international law analysis deploys a similar concept, the spectrum laid out here is a useful starting point for identifying potentially relevant subjective and objective markers (such as intentions, expectations, reasonableness, and so forth). As discussed below, however, the proper approach to waiver under Article 17 is unlikely to mirror (closely, at any rate) the approach under US domestic law.

[26] For particularly helpful background on these cases, see Orin S. Kerr, "The Case for the Third-Party Doctrine" (2009) 107 *Michigan Law Review* 561, 567–70.

[27] *See On Lee* v. *United States*, 343 U.S. 747 (1952); *Lopez* v. *United States*, 373 U.S. 427 (1963); *Lewis* v. *United States*, 385 U.S. 206 (1966); *Hoffa* v. *United* States, 385 U.S. 293 (1966); *United States* v. *White*, 401 U.S. 745 (1971).

https://doi.org/10.1017/9781316838952.012 Published online by Cambridge University Press

"voluntarily conveyed" to the banks.[28] In *Smith v. Maryland*, the Court reinforced its earlier holdings as applied to records of phone calls placed by a criminal suspect. The Court held that, because dialing numbers from one's phone involves providing those numbers to the phone company, the police can collect records of those calls, without a warrant, through the use of a pen register installed on the telephone company's (rather than the suspect's) property.[29]

In one sense, each of these rulings was quite narrow. The first cluster addressed a criminal defendant's communications with a government agent or informant, *Miller* concerned checks and deposit slips provided to a bank, and *Smith* addressed the right of a criminal suspect to assert Fourth Amendment protection for the numbers he dials from his home phone. Yet in all of these cases, the Court held that constitutional privacy protections under the Fourth Amendment to the US Constitution simply did not apply, at least in part because the parties asserting their rights had voluntarily disclosed the information in question to a third party. The cases are thus suggestive of a rule that extends to many other contexts.

As many have noted,[30] the underlying rule – sometimes referred to as the "third-party doctrine"[31] – has sweeping implications in the current era. Most people now turn over a significant and growing proportion of their private information to third-party service providers. E-mail providers like Google rather notoriously scan the text of our messages for key words so they can tailor their advertising to matters of interest to specific users. The specific websites we visit are recorded by Internet service providers (ISPs).[32] And, just like in Mr. Smith's case, significant information about our phone activity – now including text messages as well as calls – passes through the hands of our phone service providers.

In fairness, there is a question as to whether the third-party doctrine would extend to the content of communications (rather than metadata) passing through the hands of a service provider.[33] The phone numbers in *Smith* are considered metadata, and it is debatable whether the monetary values on checks and deposit slips from *Miller*

[28] 425 U.S. 435 (1976).

[29] *See Smith* v. *Maryland*, 442 U.S. 735 (1979). Other cases in this second series include *Couch* v. *United States*, 409 U.S. 322 (1973) and *United States* v. *Payner*, 447 U.S. 727 (1980).

[30] *See, e.g.*, J. Villasenor, "What You Need to Know about the Third-Party Doctrine," *The Atlantic*, www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/; C. Cohn and P. Higgins, "Rating Obama's NSA Reform Plan: EFF Scorecard Explained," Electronic Frontier Foundation, www.eff.org/deeplinks/2014/01/rating-obamas-nsa-reform-plan-eff-scorecard-explained.

[31] *See, e.g.*, Kerr, "The Case for the Third-Party Doctrine."

[32] Google records every search conducted on its search engine. B. Caddy, "Google tracks everything you do. Here's how to delete it," *Wired*, www.wired.co.uk/article/google-history-search-tracking-data-how-to-delete. That has driven some users to use search engines that claim they do not, such as DuckDuckGo. *See* DuckDuckGo, "Why You Should Care – Search History," https://duckduckgo.com/privacy#s2.

[33] *See, e.g.*, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

count as content.[34] The first series of cases discussed above concerned content, but that content was conveyed (sometimes unknowingly) *to* a government agent or informant rather than *through* a third-party service provider. One might attempt to distinguish these cases, as Orin Kerr has done, carving out Fourth Amendment protection for content but not metadata.[35] Others, like Greg Nojeim, argue that metadata can be sensitive enough to warrant Fourth Amendment protection on its own, even if precedent does not necessarily support that view.[36] There is no clear consensus on the matter in US courts, although the holding in *Smith* could arguably reach content, because the court does not explicitly distinguish between content and metadata: "[T]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[37] And although Justice Sonia Sotomayor has questioned the third-party doctrine precisely for its implications at a time when so much of our daily activity involves third parties,[38] it remains unclear how US courts will continue to apply the doctrine.

In light of what appear to be tangible legal risks, not to mention the practical likelihood that various state intelligence agencies and others are likely to obtain nontrivial proportions of our digital data, it is therefore worth inquiring how deliberately and culpably people appear to store and transmit so much sensitive information insecurely.

III THE VOLUNTARINESS OF INSECURE USE OF TECHNOLOGY

It is impossible to deny that cell phones and the Internet are convenient for managing private matters, and many of us sometimes elect to use them when we know (or should know) that it is insecure to do so. But in light of the possible implications for waiving the human right to privacy, it is important to recognize that the use of digital technologies is often less voluntary than might appear at first glance. While there is obviously some element of choice in when and how people adopt technologies, there is a large measure of compulsion as well. Many employers assign e-mail addresses to employees, the use of which is more or less mandatory. Certain employers also issue smartphones to remain in better contact with their

[34] Some simply reject the distinction between metadata and content, such as the Office of the UN High Commissioner of Human Rights. *See* "The right to privacy in the digital age," ¶ 19.

[35] O. Kerr and G. Nojeim, "The Data Question: Should the Third-Party Doctrine Be Revisited?," *ABA Journal*, www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/.

[36] Ibid.

[37] *Smith*, 442 U.S. at 743–44.

[38] "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *United States v. Jones*, 132 S. Ct. 945, 957, 181 L. Ed. 2d 911 (2012) (Sotomayor J. concurring) (internal citations omitted).

employees, or to enable employees to remain in better contact with clients. Universities often require students to use online systems to access course materials and other important information. Indeed, online research has become all but unavoidable for a number of jobs and scholarly endeavors. For many people, unplugging is not even a meaningful possibility.

There are also broader practical concerns that raise questions about the voluntariness of much Internet and phone use. The obvious utility of cell phones can make it prohibitive to eschew them. For example, cell phones are unparalleled as a parenting tool for remaining in contact with one's children. Even for those who can do without a cell phone, the choice to do so can impose substantial costs. Moreover, increasing cell phone use has correlated with a dramatic decline in the installation and maintenance of pay phones, making it ever more impractical to hold out for privacy reasons.[39]

Similarly, refusing to use the Internet may ultimately foreclose access to a range of substantive goods.[40] Remaining in touch with others is just one example. For those of limited means, long-distance communication without the Internet is especially difficult, as phone calls can be expensive and postal mail is slow. But instant messaging and voice-over-IP services (like Skype) permit free communication with other users all over the world. Similarly, staying up to date on current events, managing one's finances, and planning travel – not to mention applying for food assistance or other government benefits – are all increasingly difficult without the Internet, as companies and governments have scaled back support for non-Internet-based interaction. Resisting new technologies can be so costly that it hardly resembles a genuine choice.[41]

Moreover, there is good reason to conclude that many users of digital technologies simply fail to appreciate their vulnerability, rather than knowingly assuming that vulnerability.[42] People routinely surrender sensitive or damaging personal information to third parties that cannot safeguard it properly, as evidenced (for example) by recent hacks of Sony, Target, Yahoo, and the Ashley Madison website.[43] The Ashley

[39] D. Andreatta, "As pay phones vanish, so does lifeline for many," *USA Today*, www.usatoday.com/story/news/nation/2013/12/17/pay-phone-decline/4049599/.

[40] *See* Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," ¶¶ 78, 85, www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Some have interpreted this report as suggesting that access to the Internet is itself a human right. *See, e.g.*, D. Kravets, "U.N. Report Declares Internet Access a Human Right," *Wired*, www.wired.com/2011/06/internet-a-human-right/.

[41] Richard Stallman has discussed a similar issue in the specific context of software selection. *See* R. Stallman, "National Institute of Technology – Trichy – India – 17 February 2004," Free Software Foundation, www.gnu.org/philosophy/nit-india.en.html.

[42] Whether that ignorance is justifiable may depend on a case-by-case analysis that considers the sophistication of the user and the nature of the technology at issue.

[43] *See* FBI National Press Office, "Update on Sony Investigation," www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation; M. Riley et. al., "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *Bloomberg*, www.bloomberg.com/news/

Madison hack, for instance, exposed the identities of many people who had used the site to set up extramarital affairs. Some of those people were seriously harmed by the revelation, including employees of the US federal government who used their official work e-mail addresses to set up accounts.[44] It is implausible that most of these people were indifferent to publication of their private information, and much more likely that they did not fully appreciate their vulnerability.

Further, many of those who recognize the privacy threats posed to electronic communication have limited resources and expertise to address the problem. For those who are not adroit with technology, it can be intimidating to pick among the options and get comfortable using the proper tools as a matter of course. Unsurprisingly, there are also conflicting opinions about the efficacy of various measures, and those who lack a technical background are not well placed to make a confident choice.

Security can also be both expensive and slow; at minimum, as one particularly tech-savvy individual put it, proper security measures can impose a significant tax on one's time.[45] Moreover, even those measures that are inexpensive and simple to use may be ineffective without buy-in from one's correspondents. For example, free, easy-to-use software is available for encrypting chats, text messages, and phone calls,[46] but encryption is pointless unless all parties to a communication are willing to use it. And the typical user also has no power whatsoever to improve the security of some of the systems many of us are obligated to use, such as e-mail provided by an employer.

Lacking the time, knowledge, power, and sometimes money necessary to invest heavily in data security, the average person finds himself trapped between two imperfect options: risk the insecurity that comes with the use of ubiquitous and convenient technologies, or forego some of the most efficient tools available for conducting personal or professional business. And, often enough, the world – whether through our employers, our schools, or the demands of our personal lives – picks the first option for us.

Even parties with significant resources strain to maintain security – not necessarily because they are careless or sloppy, but rather because digital data can be vulnerable to collection by any number of actors, and because it can be exceedingly difficult to

articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data; S. Thielman, "Yahoo hack: 1bn accounts compromised by biggest data breach in history," *The Guardian*, www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached; K. Zetter, "Hackers Finally Post Stolen Ashley Madison Data," *Wired*, www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.

[44] E. Fink and L. Segall, "Government workers cope with fallout from Ashley Madison hack," CNN, http://money.cnn.com/2015/08/22/technology/ashley-madison-hack-government-workers/.

[45] *See With Liberty to Monitor All*, p. 34.

[46] Free software is also available for encrypting e-mails, but e-mail encryption remains notoriously clunky.

understand the nature of those vulnerabilities and to institute adequate protections. The US intelligence community, for instance, has failed repeatedly at protecting highly classified information from both whistleblowers and hackers.[47] It is not surprising, therefore, that sophisticated individuals struggle as well. I previously did research on surveillance for Human Rights Watch (HRW) and the American Civil Liberties Union (ACLU), for which I interviewed (among other people) nearly fifty journalists covering intelligence, national security, and law enforcement.[48] Those journalists have an overriding interest in protecting both the identities of their sources and the contents of their conversations. First and foremost, that interest arises from a general feeling of obligation to shield the identities of those who provide them with information. As a practical matter, the journalists also recognize that failure to protect sources effectively could compromise their ability to develop other sources in the future.

Many of the people I spoke with worked for major outlets, like *The New York Times*, *The Wall Street Journal*, *The Washington Post*, NPR, and ABC News.[49] Most also had years, even decades, of experience reporting on sensitive subjects, and a number had already won Pulitzer Prizes. As journalists go, therefore, the group I interviewed was elite in both their level of skill and their access to institutional support for the proper tools of the trade. All of that notwithstanding, these journalists consistently and vividly relayed to me significant ongoing challenges in using digital technologies securely.[50] Nearly all of them told me that the most secure method of doing their work involved avoiding technology as much as possible – meeting sources face-to-face while leaving cell phones at the office, or saving notes in hard copy rather than electronically.

Yet "going dark" by avoiding electronic devices significantly impeded their work, could still draw scrutiny, and was sometimes impossible.[51] To the extent that use of digital technologies is unavoidable, many of the journalists reported upgrading their

[47] Leaving aside the information disseminated by Snowden, the NSA also recently had exploits stolen by hackers. E. Nakashima, "Powerful NSA hacking tools have been revealed online," *The Washington Post*, www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html. Separately, CIA Director John Brennan apparently had his private e-mail hacked by a teenager. K. Zetter, "Teen Who Hacked CIA Director's Email Tells How He Did It," *Wired*, www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/.

[48] *With Liberty to Monitor All*, p. 7.

[49] Ibid.

[50] The report details some of their challenges in greater detail. *See* ibid., pp. 22–48.

[51] One major challenge is making initial contact with a source without using e-mail or a phone. First there is a practical problem: you must find the source's precise physical location, which can be prohibitive if he or she is not nearby. Second, many sources do not take kindly to being accosted by a journalist they may not know seeking to develop a relationship they may have reservations about. On the other hand, using e-mail or phone, even with security measures in place, will nearly always leave a link between the journalist and the source that can be discovered later. *See* ibid.

security. For example, a number described learning how to use Tor, how to encrypt e-mails, chats, and texts, and how to purchase and set up air-gapped computers.[52] Some benefitted from data security training run by their outlets. Others with less institutional support described improvising new security measures, sometimes attempting to hide digital trails using methods that were in fact ineffective. One described sharing an e-mail account with a source and exchanging messages via saved, but unsent, drafts. That was the same technique David Petraeus reportedly used, unsuccessfully, in attempting to communicate secretly with his mistress.[53] Whether the journalists benefitted from professional security training or not, they were uniformly skeptical that it was even possible to be entirely secure in one's use of digital technologies. Interviewees commonly expressed the feeling that, when facing off against an adversary as powerful as the National Security Agency, the best one could hope to do is "raise the cost of surveillance."[54]

I found similar results from speaking to attorneys,[55] whose interests in digital security stem from, among other things, their professional responsibility to safeguard confidential client information.[56] I interviewed more than forty attorneys, most of them working on matters of potential interest to the US government, such as criminal defense in the national security context. Just as the journalists expressed significant concerns about managing their relationships with sources, the attorneys largely worried about managing their relationships with clients. Some found that merely warning their clients against using phones and e-mail made the clients increasingly mistrustful and hampered their ability to develop a relationship. And, like the journalists, a number of the lawyers expressed the belief that speaking face-to-face is now essential, notwithstanding the costs and time constraints associated with doing so.

It is noteworthy that these journalists and attorneys – educated, fairly well-resourced people with an unusually high interest in protecting the privacy of some of their interactions – have to wrestle so mightily with the issue of data security. Indeed, merely planning this research required a surprising amount of thought within HRW and the ACLU. I needed a way to reach out to my subjects electronically concerning sensitive matters, and a way to convey to them my competence in

[52] Air-gapped computers are computers that never connect to any insecure network (including the Internet), often configured to sit in a secure room. One journalist equated them to electronic typewriters. *See With Liberty to Monitor All*, p. 32.

[53] *See* D. Leinwand Leger and Y. Alcindor, "Petraeus and Broadwell used common e-mail trick," *USA Today*, www.usatoday.com/story/tech/2012/11/13/petraeus-broadwell-email/1702057/.

[54] *With Liberty to Monitor All*, p. 39.

[55] Ibid., pp. 49–65.

[56] *See* American Bar Association, "Model Rules of Professional Conduct: Rule 1.6: Confidentiality of Information," www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html. Some legal experts anticipate that failure to use secure technologies to store or communicate confidential information may soon become grounds for sanctions. *With Liberty to Monitor All*, pp. 58–59.

protecting any data they might provide. That was a difficult goal to achieve, especially because so much of security turns on the measures taken by one's correspondents. Like many of my research subjects, I therefore had to work with the institutions backing me to develop security protocols that were affordable and practical under the circumstances. Notwithstanding the assistance I had, the process involved some measure of trial and at least one embarrassing security error on my part. In short, true digital security is incredibly difficult or perhaps even impossible to attain – a point that cannot be lost in attempting to understand the relationship between the use of digital technologies and the waiver of the human right to privacy.

IV DRAWING SOME CONCLUSIONS

A modern understanding of the human right to privacy must contend with these questions, and the purpose of this chapter is to highlight the need for an extended conversation about the issue of waiver, especially among human rights authorities.[57] This section offers some preliminary conclusions about the conditions under which a technology user's actions might constitute a waiver of his or her privacy protections under Article 17 of the ICCPR, and the duties of the governments that are parties to the ICCPR to support the choices of individuals who take measures to secure their digital data. Per the Vienna Convention on the Law of Treaties, "[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[58] When that approach alone "[l]eaves the [treaty's] meaning ambiguous or obscure," or "[l]eads to a result which is manifestly absurd or unreasonable," then "[r]ecourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion."[59] Application of these principles often permits and may at times require that a state's treaty obligations evolve with changing circumstances. As Eirik Bjorge has recently put it, "The wording [of a treaty] is important because it may lead us to ascertaining the intention of the parties, not because it is somehow an end in and of itself."[60] An evolutionary reading of a treaty may therefore "be required by good faith."[61] For the reasons laid

[57] It is noteworthy, for example, that the ten reports the first UN Special Rapporteur on privacy is scheduled to produce between 2017 and 2021 do not appear designed to address this subject at all. *See* Office of the High Commissioner for Human Rights, "Planned Thematic Reports and call for consultations," www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx.

[58] Vienna Convention on the Law of Treaties, art. 31.

[59] Ibid., art. 32. To the extent that this chapter has focused on the United States, it is significant that the US accepts the Vienna Convention as informing interpretation of its treaty obligations. *See* E. Criddle, "The Vienna Convention on the Law of Treaties in U.S. Treaty Interpretation" (2004) 44 *Virginia Journal of International Law* 431, 443.

[60] E. Bjorge, *The Evolutionary Interpretation of Treaties* (Oxford: Oxford University Press, 2014), p. 189.

[61] Ibid., p. 190.

out below, the right to privacy reveals that the ICCPR is precisely the sort of treaty that requires an evolutionary reading.

A *Waiver Should Be Understood Narrowly under the ICCPR*

The text of Article 17 is the starting point in determining the conditions for waiver. As noted above, the covenant prohibits "arbitrary or unlawful interference" with four distinct but potentially overlapping items: privacy, family, home, and correspondence. Challenging questions arise immediately simply from the relationships among these categories. For example, privacy is distinctively diffuse relative to the other items; the concept of privacy neither encompasses everything about one's correspondence, family, and home, nor is it fully exhausted by those three domains. The language of Article 17 therefore immediately invites the possibility that certain information will warrant protection under more than one category. That possibility is even more complex than it appears at first glance because the protections under the different categories may not be symmetrical.

For example, whether state interference with a particular piece of information intrudes upon my privacy would seem to depend, at least in part, on my attitude toward that information or my previous choices about whether to publicize it. In other words, if I publicize certain information widely enough, then interference with that information is not, by definition, an interference with my privacy. By contrast, e-mail, text messages, and instant messages are almost certainly "correspondence" under the covenant, irrespective of whether I intend them to be private, and thus interference with these items could trigger Article 17 even if I had shared those e-mails, texts, or messages with many correspondents. By listing "correspondence" as its own protected category – separately from "privacy" – interference with correspondence could require an assessment of non-arbitrariness and lawfulness by default.[62]

This asymmetry may lead to irregular outcomes when assessing whether an individual has waived the protections of Article 17. Suppose a state takes the position that the interception of an unencrypted e-mail sent by me does not count as an interference with my privacy because the lack of encryption renders the e-mail non-private. Even so, the e-mail could still be protected under Article 17 as correspondence. By contrast, an analogous transaction that does not fall under the secondary protection of the "correspondence," "home," or "family" categories – say, storing certain work information unencrypted in the cloud – might not qualify for Article 17 protection at all. Those results may seem counterintuitive, raising further questions about whether "privacy" as a category should be understood as a catchall designed only to extend the protections of Article 17 to sensitive domains other than

[62] The fact that someone has made correspondence public may, of course, bear on the question of whether interference with that correspondence is arbitrary or unlawful.

https://doi.org/10.1017/9781316838952.012 Published online by Cambridge University Press

one's correspondence, family, and home, rather than offering a separate layer of support that overlaps with those enumerated categories. In any event, how to untangle the relationships among these categories is exactly the sort of question this chapter argues is in need of an authoritative answer.

Notwithstanding such questions, however, and based on the covenant's object and purpose, it appears that covenant protections should generally be rounded up rather than down. The main objective of the covenant is described in broad terms in the preamble, which offers a sweeping account of the value of the rights it protects. Under the terms of the covenant, the enumerated rights "derive from the inherent dignity of the human person"; people must be able to enjoy those rights to achieve "the ideal of free human beings … [living] in freedom from fear and want."[63] Although it can be tempting to link the spread of digital technologies and the rise of social media with a devaluation of privacy and conclude that attitudes toward privacy have shifted with technological advancement, that is neither obviously true nor especially relevant.[64] The object and purpose of the covenant would be undermined by permitting the casual or unintentional waiver of a core right simply because many people use digital technologies insecurely. Indeed, when only a minuscule, elite subset of the population is actually capable of safely maneuvering around technological vulnerabilities – and, even then, imperfectly – the appropriate conclusion is not that everyone else has chosen insecurity, but rather that security is too difficult to attain. Conditioning enjoyment of the right to privacy under the ICCPR on the secure use of digital technologies would render the right meaningless.

Among the implications of this conclusion is that strict application of the US third-party doctrine is likely incompatible with the ICCPR. Digital technologies nearly always involve the provision of information (whether content or metadata, for those who accept the distinction) to a third party. Were any disclosure to a third party enough to eliminate a user's privacy interest, users would lose privacy protections for nearly all of the information they store or transmit in digital form. Even if the doctrine only applied to metadata, it would be unacceptably broad under the

[63] ICCPR, preamble.

[64] Numerous opinion polls have been taken since the Snowden revelations, which appear to show that a majority of Americans continue to value privacy in a variety of contexts, even as they are willing to permit certain intrusions for the sake of protecting national security. *See, e.g.*, M. Madden and L. Rainie, "Americans' Attitudes About Privacy, Security and Surveillance," Pew Research Center, www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/; University of Southern California Annenberg School for Communication and Journalism, "Is online privacy over?," http://annenberg.usc.edu/news/around-usc-annenberg/online-privacy-over-findings-usc-annenberg-center-digital-future-show;
L. Cassani Davis, "How Do Americans Weigh Privacy Versus National Security?," *The Atlantic*, www.theatlantic.com/technology/archive/2016/02/heartland-monitor-privacy-security/459657/; L. Rainie and M. Duggan, "Privacy and Information Sharing," Pew Research Center, www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

covenant, especially because metadata can be as revealing as content, but is more poorly understood by the public at large (and therefore may be less voluntarily shared).

In the recent Supreme Court case where Justice Sotomayor questioned the wisdom of the third-party doctrine, Justice Samuel Alito contemplated the possible effects of new technology on privacy rights. He wrote:

> Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.[65]

Depressing as these comments may be for privacy advocates, they are at least comprehensible in the context of a system that accepts the third-party doctrine. But that doctrine is questionable in the digital age, and it may never have taken root under the present circumstances. Many people *do* maintain some sort of subjective expectation of privacy in information they share with a third party. One might properly comprehend that an e-mail provider has access to one's e-mail content without also believing one's e-mails could just as well have been sent to *other* third parties, such as foreign governments searching for intelligence. The same is true for digital banking activity or text messages or any other manner of nonpublic transaction that is only possible with the assistance of a third party. In the abstract, and in the digital age, that expectation is not objectively unreasonable either – at least not obviously so.

Moreover, the third-party doctrine plays out differently under the covenant as compared to the US Constitution. Even beyond the wrinkle identified above with respect to the four types of interests protected by Article 17, there are a number of relevant differences between the rights to privacy guaranteed, respectively, by the covenant and the Fourth Amendment. For one, Article 17 makes no explicit reference to reasonableness or subjective expectations, unlike the Fourth Amendment to the Constitution, which bans, *inter alia*, "unreasonable searches and seizures." Article 17 also applies more broadly than the Fourth Amendment; whereas the Fourth Amendment specifically regulates US government action, Article 17 bans a variety of privacy interferences by government actors and also obliges governments to protect rights holders against interferences from private actors. Incorporating recognition of these points into an applicable waiver standard is essential to ensuring that the protections of Article 17 keep pace with technological change, thereby staying true to the object and purpose of the covenant.

[65] *United States v. Jones*, 132 S. Ct. 945, 962 (2012) (Alito J., concurring).

https://doi.org/10.1017/9781316838952.012 Published online by Cambridge University Press

B *States Should Support – and Certainly Should Not Interfere with – Active Steps Taken by Individuals to Protect Their Data*

Under the ICCPR, states are bound both "to respect and [to] ensure" the rights in the covenant.[66] It has become common to describe those obligations by reference to the "respect, protect, and fulfill" framework, which in the context of privacy essentially captures the idea that states must avoid actively infringing on privacy rights, protect those rights from infringement by others, and take positive steps to support individual realization of privacy rights.[67] Recent discussions of privacy tend to focus on the negative obligations of states – the obligation not to violate privacy by engaging in improper surveillance, for example. But the positive obligations of states must remain part of the conversation as well.

By analogy, consider the human right to health, which is protected by the International Covenant on Economic, Social and Cultural Rights (ICESCR).[68] The ICESCR guarantees "the right of everyone to the enjoyment of the highest attainable standard of physical and mental health."[69] Properly understood, the right is not an entitlement *to be healthy*, but rather a right to have the state take adequate steps to facilitate the health of its population.[70] A state's full compliance with its obligations to ensure the right to health would not prevent members of its population from making poor health choices. Nevertheless, parties to the ICESCR are obligated to undertake measures to promote the health of their people.[71] Those measures might include reasonable efforts by the state to guarantee access to key resources for promoting health, such as by providing meaningful access to adequate medical care and nutrition.[72] They could also include the provision of information that facilitates informed health choices, such as nutrition labels on food packaging or disclosures about the side effects of various medical treatments.[73]

[66] *See* ICCPR, art. 2(1).

[67] *See, e.g.*, U.N. Office of the High Commissioner for Human Rights, "International Human Rights Law," www.ohchr.org/EN/ProfessionalInterest/Pages/InternationalLaw.aspx.

[68] ICESCR, art. 12. The right is also suggested in the Universal Declaration of Human Rights, although somewhat less directly. *See* UDHR, art. 25.

[69] Note that the United States has not ratified the ICESCR, and therefore the right to health does not exert the same binding force on the US as the right to privacy does.

[70] UN Office of the High Commissioner for Human Rights and World Health Organization, "The Right to Health: Fact Sheet No. 31," at 5, www.ohchr.org/Documents/Publications/Factsheet31.pdf.

[71] States would also have negative obligations with respect to the right to health, such as to refrain from directly undermining the health of their populations (for example, by stripping large segments of the population of health insurance or polluting the drinking water).

[72] *See* ibid., at 3.

[73] *See* ibid.

Similarly, a state can properly ensure the right to privacy even as some of its citizens compromise their rights through poor choices about how to handle their own data.[74] The human right to privacy entitles one to protect certain information from invasion not just by one's own government, but by foreign governments, corporations, hackers, identity thieves, and most anyone else. As noted above, governments that have ratified the ICCPR are obligated to protect individuals from such other actors who might intrude on the right, and to facilitate the efforts of individuals who seek out tools to secure their own information.

This obligation to ensure the right to privacy has several implications. It means governments should work with tech companies to repair known software flaws rather than secretly hoarding those exploits and allowing their populations to be rendered vulnerable. It means governments should seek to prevent or discourage the hacking of personal information rather than tolerating or encouraging those hacks. It means governments should offer resources to educate the public on good technological hygiene – for example, managing passwords for their online accounts or securing their mobile devices – rather than making it easier for companies to collect and sell their digital information, such as their web browsing histories. And it means governments should support the development and use of technologies that make it genuinely possible for individuals to secure their information, such as end-to-end encryption for messaging services. At the very least, it certainly means states may not actively prevent people from accessing and using reasonable security and encryption tools.

States seeking to clear the way for aggressive surveillance might prefer simply to push their obligations aside. Consider once more the example of the United States, which has publicly opposed the proposals of technology companies to provide encryption as standard for various services.[75] In particular, law enforcement officials like former FBI Director James Comey have strenuously resisted "end-to-end" encryption as a default for various forms of communication, pressuring companies that offer such encryption to alter their "business model."[76] Similarly, former Director of National Intelligence James Clapper complained that the Snowden revelations accelerated personal use of encryption, which he claimed was "not a good thing."[77] Even President Barack Obama publicly stated opposition to

[74] There is something of an asymmetry between the right to privacy and the right to health, in that it may be less likely that a state would seek to limit the latter to advance an alternate interest, like national security.

[75] *See* J. Comey, "Encryption, Public Safety, and 'Going Dark'," Lawfare, www.lawfareblog.com/encryption-public-safety-and-going-dark; T. Schleifer, "FBI director: We can't yet restrain ISIS on social media," CNN, www.cnn.com/2015/06/18/politics/fbi-social-media-attacks/.

[76] D. Froomkin and J. McLaughlin, "Comey Calls on Tech Companies Offering End-to-End Encryption to Reconsider 'Their Business Model'," *The Intercept*, https://theintercept.com/2015/12/09/comey-calls-on-tech-companies-offering-end-to-end-encryption-to-reconsider-their-business-model/.

[77] J. McLaughlin, "Spy Chief Complains That Edward Snowden Sped Up Spread of Encryption by 7 Years," *The Intercept*, https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/.

unbreakable encryption.[78] Moreover, as of 2011, the NSA had a policy of treating encrypted communications collected under one of its surveillance authorities as worthy of special scrutiny,[79] a point of concern for various privacy advocacy groups.[80] Although there were reports of serious debates within the Obama administration on encryption policy,[81] the public criticisms of encryption from prominent officials and the evidence that encrypted communications are viewed with suspicion by the government are discouraging. They are also legally relevant to the state's duty to ensure the right to privacy, for they aim to limit the use, availability, or utility of tools that help individuals secure that right for themselves.

V CONCLUSION

This chapter advocates for a serious conversation about waiving the human right to privacy. Many other elements of the right are appropriately on the table already, being dissected, debated, reinterpreted, and applied to novel circumstances. All essential questions about the right to privacy should be folded into that discussion. Privacy issues will only grow more significant as digital technologies and the surveillance programs that track them become more sophisticated and ubiquitous. It is important that we get these issues right, and now is the time to ensure that we do.

It bears emphasizing that a universally accepted standard for waiving the human right to privacy may prove to be elusive, especially given that states like the United States may contribute to the debate by drawing on excessively broad standards from their own domestic legal precedents. Moreover, an acceptable standard may prove to be challenging to implement in any event, and its creation would in no way diminish the importance of questions already being addressed, such as the definitions of the terms in Article 17 or the proper limitations on the right. Nevertheless, waiver has broad implications for the legality of common state practices; the persistence of questions about its application only sows doubt where clarity is essential.

[78] J. McLaughlin, "Obama Wants Nonexistent Middle Ground on Encryption, Warns Against 'Fetishizing Our Phones'," *The Intercept*, https://theintercept.com/2016/03/11/obama-wants-nonexistent-middle-ground-on-encryption-warns-against-fetishizing-our-phones/.

[79] *See* "Exhibit B: Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended," at 9, www.aclu.org/files/assets/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf.

[80] *See, e.g.*, K. Opsahl and T. Timm, "In Depth Review: New NSA Documents Expose How Americans Can Be Spied on Without a Warrant," Electronic Frontier Foundation, www.eff.org/deeplinks/2013/06/depth-review-new-nsa-documents-expose-how-americans-can-be-spied-without-warrant.

[81] *See* S. Sorcher and J. Eaton, "What the US government really thinks about encryption," *The Christian Science Monitor*, www.csmonitor.com/World/Passcode/2016/0525/What-the-US-government-really-thinks-about-encryption.