WITH LIBERTY TO MONITOR ALL

How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy

HUMAN RIGHTS WATCH

ACLU
AMERICAN CIVIL LIBERTIES UNION

HUMAN RIGHTS WATCH

With Liberty to Monitor All

How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy

Printed in the United States of America
ISBN: 978-1-62313-1814
Cover design by Rafael Jimenez

Human Rights Watch defends the rights of people worldwide. We scrupulously investigate abuses, expose the facts widely, and pressure those with power to respect rights and secure justice. Human Rights Watch is an independent, international organization that works as part of a vibrant movement to uphold human dignity and advance the cause of human rights for all.

Human Rights Watch is an international organization with staff in more than 40 countries, and offices in Amsterdam, Beirut, Berlin, Brussels, Chicago, Geneva, Goma, Johannesburg, London, Los Angeles, Moscow, Nairobi, New York, Paris, San Francisco, Sydney, Tokyo, Toronto, Tunis, Washington DC, and Zurich.

For more information, please visit our website: http://www.hrw.org

JULY 2014

978-1-62313-1814

With Liberty to Monitor All

How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy

Summary

For much of its history, the United States has held itself out as a model of freedom, democracy, and open, accountable government. Freedoms of expression and association, as well as rights to a fair trial, are protected by the Constitution, and US officials speak with pride of the freedom of the media to report on matters of public concern and hold government to account for its actions. Yet, as this report documents, today those freedoms are very much under threat due to the government's own policies concerning secrecy, leak prevention, and officials' contact with the media, combined with large-scale surveillance programs. If the US fails to address these concerns promptly and effectively, it could do serious, long-term damage to the fabric of democracy in the country.

Specifically, this report documents the effects of large-scale electronic surveillance on the practice of journalism and law, professions that enjoy special legal protections because they are integral to the safeguarding of rights and transparency in a democracy. To document these effects, we interviewed 92 people, including 46 journalists and 42 lawyers, about their concerns and the ways in which their behavior has changed in light of revelations of large-scale surveillance. We also spoke to current and former senior government officials who have knowledge of the surveillance programs to understand their perspective, seek additional information, and take their concerns into account in our analysis.

Whether reporting valuable information to the public, representing another's legal interests, or voluntarily associating with others in order to advocate for changes in policy, it is often crucial to keep certain information private from the government. In the face of a massively powerful surveillance apparatus maintained by the US government, however, that privacy is becoming increasingly scarce and difficult to ensure. As a result, journalists and their sources, as well as lawyers and their clients, are changing their behavior in ways that undermine basic rights and corrode democratic processes.

Revelations of Large-Scale Surveillance

The United States government today is implementing a wide variety of surveillance programs that, thanks to developments in its technological capacity, allow it to scoop up personal information and the content of personal communications on an unprecedented scale. Media reports based on revelations by former National Security Agency (NSA)

contractor Edward Snowden have recently shed light on many of these programs. They have revealed, for example, that the US collects vast quantities of information—known as "metadata"—about phone calls made to, from, and within the US. It also routinely collects the content of international chats, emails, and voice calls. It has engaged in the large-scale collection of massive amounts of cell phone location data. Reports have also revealed a since-discontinued effort to track internet usage and email patterns in the US; the comprehensive interception of all of phone calls made within, into, and out of Afghanistan and the Bahamas; the daily collection of millions of images so the NSA can run facial recognition programs; the acquisition of hundreds of millions of email and chat contact lists around the world; and the NSA's deliberate weakening of global encryption standards.

In response to public concern over the programs' intrusion on the privacy of millions of people in the US and around the world, the US government has at times acknowledged the need for reform. However, it has taken few meaningful steps in that direction.

On the contrary, the US—particularly the intelligence community—has forcefully defended the surveillance programs as essential to protecting US national security. In a world of constantly shifting global threats, officials argue that the US simply cannot know in advance which global communications may be relevant to its intelligence activities, and that as a result, it needs the authority to collect and monitor a broad swath of communications. In our interviews with them, US officials argued that the programs are effective, plugging operational gaps that used to exist, and providing the US with valuable intelligence. They also insisted the programs are lawful and subject to rigorous and multi-layered oversight, as well as rules about how the information obtained through them is used. The government has emphasized that it does not use the information gleaned from these programs for illegitimate purposes, such as persecuting political opponents.

The questions raised by surveillance are complex. The government has an obligation to protect national security, and in some cases, it is legitimate for government to restrict certain rights to that end. At the same time, international human rights and constitutional law set limits on the state's authority to engage in activities like surveillance, which have the potential to undermine so many other rights.

The current, large-scale, often indiscriminate US approach to surveillance carries enormous costs. It erodes global digital privacy and sets a terrible example for other countries like India, Pakistan, Ethiopia, and others that are in the process of expanding their surveillance capabilities. It also damages US credibility in advocating internationally for internet freedom, which the US has listed as an important foreign policy objective since at least 2010.

As this report documents, US surveillance programs are also doing damage to some of the values the United States claims to hold most dear. These include freedoms of expression and association, press freedom, and the right to counsel, which are all protected by both international human rights law and the US Constitution.

Impact of Surveillance on Journalists

For journalists, the surveillance programs and a government crackdown on unregulated contact between officials and the press have combined to constrict the flow of information concerning government activity. An increase in the frequency of leak prosecutions, as well as the government's implementations of programs—such as the Insider Threat Program—aimed at discouraging officials from sharing information outside the government, have raised the stakes for officials who might consider even talking to journalists.

Large-scale surveillance dramatically exacerbates those concerns by largely cutting away at the ability of government officials to remain anonymous in their interactions with the press, as any interaction—any email, any phone call—risks leaving a digital trace that could subsequently be used against them. This is particularly worrisome in light of changes to US law that allow intelligence information to be used more easily in criminal investigations, potentially allowing law enforcement to circumvent traditional warrant requirements.

Journalists told us that officials are substantially less willing to be in contact with the press, even with regard to unclassified matters or personal opinions, than they were even a few years ago. This can create serious challenges for journalists who cover national security, intelligence and law enforcement, and who often operate in a gray area—working with information that is sensitive but not necessarily classified, and

speaking with multiple sources to confirm and piece together the details of a story that may be of tremendous public interest.

In turn, journalists increasingly feel the need to adopt elaborate steps to protect sources and information, and eliminate any digital trail of their investigations—from using high-end encryption, to resorting to burner phones, to abandoning all online communication and trying exclusively to meet sources in person.

Journalists expressed concern that, rather than being treated as essential checks on government and partners in ensuring a healthy democratic debate, they now feel they may be viewed as suspect for doing their jobs. One prominent journalist summed up what many seemed to be feeling as follows: "I don't want the government to force me to act like a spy. I'm not a spy; I'm a journalist."

This situation has a direct effect on the public's ability to obtain important information about government activities, and on the ability of the media to serve as a check on government. Many journalists said it is taking them significantly longer to gather information (when they can get it at all), and they are ultimately able to publish fewer stories for public consumption. As suggested above, these effects stand out most starkly in the case of reporting on the intelligence community, national security, and law enforcement—all areas of legitimate—indeed, extremely important—public concern.

Impact of Surveillance on Lawyers

Lawyers face a different challenge. They have a professional responsibility to maintain the confidentiality of information related to their clients on pain of administrative discipline. They also rely on the ability to exchange information freely with their clients in order to build trust and develop legal strategy, which is especially important in the realm of criminal defense. Increased government surveillance undercuts these longstanding and central elements of the practice of law, creating uncertainty as to whether lawyers can ever provide true confidentiality while communicating electronically with clients.

Lawyers we interviewed for this report expressed the greatest concern about situations where they have reason to think the US government might take an intelligence interest in a case, whether it relates to the activities of foreign governments or a drug or

terrorism prosecution. As with the journalists, lawyers increasingly feel under pressure to adopt strategies to avoid leaving a digital trail that could be monitored; some use burner phones, others seek out technologies they feel may be more secure, and others reported traveling more for in-person meetings. Some described other lawyers expressing reluctance to take on certain cases that might incur surveillance, though by and large the attorneys interviewed for this report seemed determined to do their best to continue representing clients. Like journalists, some felt frustrated, and even offended, that they were in this situation. "I'll be damned if I have to start acting like a drug dealer in order to protect my client's confidentiality," said one.

The result is the erosion of the right to counsel, a pillar of procedural justice under human rights law and the US Constitution.

Uncertainty and Secrecy

Uncertainty is a significant factor shaping the behavior of both journalists and lawyers. The combination of the sheer number of surveillance programs, the complexity of the underlying legal regimes, and the lack of clarity as to their scale and scope renders it practically impossible for any layperson to discern which forms of communication and data storage are secure and when they may be reasonably subject to surveillance. Compounding matters, the government has failed fully to disclose the rules governing its collection and use of information under the surveillance regime. Piecemeal access to this information only creates greater doubt.

The US government has an obligation to defend national security, yet many of its surveillance practices go well beyond what may be justified as necessary and proportionate to that aim. Instead, these practices are undermining fundamental rights and risk changing the nature of US democracy itself. It is time for the US to carry out significant reforms of its surveillance programs and other policies contributing to the harms documented in this report.

Human Rights Watch and the ACLU strongly urge the United States to:

- end large-scale surveillance practices that are either unnecessary or broader than necessary to protect national security or an equally legitimate goal;

- strengthen the protections provided by targeting and minimization procedures;
- disclose additional information about surveillance programs to the public;
- reduce government secrecy and restrictions on official contact with the media; and
- enhance protections for national-security whistleblowers.

Methodology

This report is based on interviews with 92 people in the United States, including journalists, lawyers, and current and former US government officials.[1] Because of the sensitive nature of the questions asked, many interview subjects spoke on background, preferring that their comments not be attributed to them by name. A couple elected to speak entirely off the record. Many of the interviews took place in or around New York City or Washington, DC. A large number were conducted by telephone, though it was not always possible to determine whether interviewees may have felt uncomfortable speaking entirely candidly over the phone.

We spoke with 46 journalists representing a wide range of news organizations, including both larger and smaller media outlets. The major outlets include the *New York Times*, the *Wall Street Journal*, the *Washington Post*, the *Los Angeles Times*, the Associated Press, Reuters, *McClatchy*, *The New Yorker*, National Public Radio, and ABC News. Most interview subjects either formerly covered or currently cover the US intelligence community, national security, or law enforcement. Most work in print, but some also work in television or radio. A few are or were editors or news executives. A significant number of the journalists are highly decorated; as a group, the interviewees for this report have won at least a dozen Pulitzer Prizes and many other prestigious journalism awards.

We interviewed 42 practicing attorneys, working in a variety of areas: criminal defense lawyers (including public defenders both at the federal and state level, and private defense attorneys representing a wide range of clients, including people charged with terrorism, drug, and financial crimes); judge advocates serving in the military and representing detainees at Guantanamo Bay; and lawyers engaged in complex civil litigation, representation of multinational corporations, and representation of foreign sovereigns.

Finally, we interviewed five current or former senior government officials with knowledge of the US government's surveillance programs or related policies. These include a senior official within the intelligence community and a senior official within the Federal Bureau of Investigation (FBI). We repeatedly requested interviews with senior officials at the National Security Agency (NSA), but after initially stating they would consider our request, the agency's representatives ceased replying to our correspondence.

[1] Note that the totals of each of the separate categories do not add up to 92 because at least one subject offered comments as a member of multiple groups.

I. Background: US Surveillance, Secrecy, and Crackdown on Leaks

> There are limits to the public's right to know in national security [contexts], but many [people within the] intelligence community know that if we followed strict rules on [classified information], there'd be no discussion of national security at all.
>
> —Steve Engelberg, editor-in-chief of ProPublica, January 30, 2014

In December of 2005, the *New York Times* reported that the NSA had been conducting warrantless surveillance on Americans since shortly after the terrorist attacks of September 11, 2001.[2] According to the *Times*, President Bush had authorized the NSA to listen in on phone calls and gather emails of US persons without warrants. A federal judge found that the warrantless wiretapping program blatantly violated both the US Constitution and the federal law governing surveillance for foreign intelligence and international counterterrorism purposes, the Foreign Intelligence Surveillance Act of 1978 ("FISA").[3] That law established a court, the Foreign Intelligence Surveillance Court ("FISC" or "FISA Court"), specifically designed to issue such warrants.[4] FISA included specific provisions governing surveillance of three types of communications, which we define here as follows: "domestic communications" (which originate and terminate inside the United States), "international communications" (which originate or terminate inside the United States, but not both), and "foreign-to-foreign communications" (which both originate and terminate outside the United States).

Over the next several years, a series of stories revealed further details about the NSA's spying activities.[5] The Bush administration over time imposed more restrictions on the

---

[2] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times,* December 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all (accessed July 8, 2014).

[3] *Am. Civil Liberties Union v. Nat'l Sec. Agency*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *vacated on jurisdictional grounds*, 493 F.3d 644 (6th Cir. 2007).

[4] "Bush Administration's Warrantless Wiretapping Program," *Washington Post*, February 12, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051500999.html (accessed July 8, 2014) (noting that the program was not subject to court oversight).

[5] For a chronology of the surveillance revelations during this period, see G. Alex Sinha, "NSA Surveillance Since 9/11 and the Human Right to Privacy," *Loyola Law Review*, vol. 59 (2013), pp. 880-885.

warrantless wiretapping program, and some portions of the program were eventually authorized under FISC orders.[6]

However, these restrictions prompted Congress to broaden FISA, including by allowing programmatic surveillance without court oversight over specific targets.[7] Further news reports surfaced, suggesting the NSA's surveillance activities continued to broaden in scope, potentially to a problematic degree.[8] Nevertheless, the public debate died down significantly.

The current chapter in the NSA saga began on June 5, 2013, when the *Guardian* published a secret FISC order from April of 2013.[9] The order instructed the US telecommunications provider Verizon to turn over to the government (on a daily basis, for three months) the records on all calls in its systems. Specifically, the article noted that "the numbers of both parties on a call are handed over, as is location data, call duration, unique identifiers, and the time and duration of all calls."[10] Many refer to the information Verizon had been ordered to turn over as "metadata"—data about communications or transactions, rather than the content of communications themselves (that is, the specific words uttered). Although the *Guardian* article described the collection of metadata rather than the content of phone conversations, it once again breathed life into the NSA controversy, illustrating

---

[6] In January of 2007, President Bush announced changes to the controversial warrantless spying program, adding a role for the FISA Court. Dan Eggen, "Court Will Oversee Wiretap Program," *Washington Post*, January 18, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/01/17/AR2007011701256.html (accessed July 8, 2014). For more information, see also Office of the Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, " Unclassified Report on the President's Surveillance Program," July 10, 2009, http://www.justice.gov/oig/special/s0907.pdf (accessed July 16, 2014), p. 30.

[7] In modifying the legal framework, Congress initially passed (and President Bush signed) the Protect America Act in 2007. That law expired in 2008, however, and Congress did not renew it. Instead, later the same year, Congress passed the FISA Amendments Act (FAA), which was renewed again in 2012 and remained in effect as of the time of this report's publication. The FAA dramatically expanded the government's authority to conduct warrantless surveillance of international communications (including communications originating or terminating inside the United States). For more details, see Sinha, "NSA Surveillance Since 9/11 and the Human Right to Privacy," *Loyola Law Review*, pp. 883-888.

[8] For a description of the relevant legislative changes and subsequent surveillance revelations, see Sinha, "NSA Surveillance Since 9/11 and the Human Right to Privacy," *Loyola Law Review*, pp. 883-892.

[9] Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *Guardian*, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (accessed July 8, 2014).

[10] Ibid. Subsequent reports, including the Privacy and Civil Liberties Oversight Board report on Section 215, found that under current practice, cell phone location data is not in fact collected. See Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," January 23, 2014, http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf (accessed July 8, 2014), pp. 22-23.

through a rare, primary document that the NSA's call-records program was remarkably broad and indiscriminate.

Within days, former NSA contractor Edward Snowden came forward as the source of the document.[11] Snowden, concerned by the NSA's surveillance activities, had collected a large number of NSA files before leaving his position as a contractor for the agency, and shared them with members of the press. Since the *Guardian* article, a flood of subsequent stories have appeared in different media outlets, many apparently based on documents provided by Snowden. Collectively, they confirm much of what had been alleged before and reveal much more, illuminating the contours of a powerful and growing surveillance apparatus run by the US government. Specific reports have detailed a variety of surveillance programs aimed at different sorts of electronic information and communications, including the large-scale collection of:

- metadata related to domestic phone calls;[12]
- the actual content of Americans' international chats, emails, and voice calls, as well as electronic documents shared internationally;[13]
- business records related to Americans' international money transfers (for a program run by the CIA);[14]
- massive amounts of cell phone location data;[15]

---

[11] Glenn Greenwald et al., "Edward Snowden: the whistleblower behind the NSA surveillance revelations," *Guardian*, June 9, 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (accessed July 8, 2014).

[12] Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *Guardian*, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (accessed July 14, 2014).

[13] The key programs revealed are called "PRISM" and "Upstream." Dominic Rush and James Ball, "PRISM Scandal: tech giants flatly deny allowing NSA direct access to servers," *Guardian*, June 6, 2013, http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining (accessed July 8, 2014); "NSA slides explain the PRISM data-collection program," *Washington Post*, June 6, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (accessed July 8, 2014).

[14] Charlie Savage and Mark Mazzetti, "C.I.A. Collects Global Data on Transfers of Money," *New York Times*, November 14, 2013, http://www.nytimes.com/2013/11/15/us/cia-collecting-data-on-international-money-transfers-officials-say.html?_r=0 (accessed July 8, 2014).

[15] The program revealed is called "CO-TRAVELER." Barton Gellman and Ashkan Soltani, "NSA tracking cellphone locations worldwide, Snowden documents show," *Washington Post*, December 4, 2013, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (accessed July 8, 2014).

- a since-discontinued program to track Americans' internet usage and emailing patterns;[16] and
- address books and contact lists from personal email and chat accounts around the world.[17]

There also have been reports that the government has eased the rules on sharing information gathered through surveillance (both internally, among different agencies, and with other governments),[18] and that it is secretly using information gathered through surveillance purportedly conducted for intelligence purposes in standard criminal investigations.[19] A further report detailed a government system for gathering all of an unnamed country's phone calls (including calls made to and from the US, and calls made by Americans from or within the country).[20]

Legal Authorities Governing Surveillance

The US government conducts different types of surveillance in different contexts. For example, federal law enforcement agents might seek a warrant from a judge to conduct targeted surveillance of a particular person suspected of a crime.[21]

---

[16] Orin Kerr, "Problems with the FISC's Newly-Declassified Opinion on Bulk Collection of Internet Metadata," post to "Lawfare" (blog), November 19, 2013, http://www.lawfareblog.com/2013/11/problems-with-the-fiscs-newly-declassified-opinion-on-bulk-collection-of-internet-metadata/ (accessed July 8, 2014).

[17] Barton Gellman and Ashkan Soltani, "NSA collects millions of e-mail address books globally," *Washington Post*, October 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html (accessed July 14, 2014).

[18] Charlie Savage and Laura Poitras, "How a Court Secretly Evolved, Extending U.S. Spies' Reach," *New York Times,* March 11, 2014, http://www.nytimes.com/2014/03/12/us/how-a-courts-secret-evolution-extended-spies-reach.html?_r=0 (accessed July 8, 2014).

[19] John Shiffman and Kristina Cooke, "Exclusive: U.S. directs agents to cover up program used to investigate Americans," Reuters, August 5, 2013, http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 (accessed July 8, 2014).

[20] The program is called "MYSTIC," and it employs a search tool called "RETRO." Barton Gellman and Ashkan Soltani, "NSA surveillance program reaches 'into the past' to retrieve, replay phone calls," *Washington Post,* March 18, 2014, http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (accessed July 8, 2014). Later reporting revealed that as of 2013, MYSTIC was operable in five countries, gathering voice data in the Bahamas and one other unnamed country, and gathering phone metadata in Mexico, Kenya, and the Philippines. Ryan Devereaux, Glenn Greenwald and Laura Poitras, "Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas," *The Intercept*, May 19, 2014, https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (accessed July 8, 2014). On May 23, Wikileaks revealed the unnamed country in the first report to be Afghanistan. "WikiLeaks statement on the mass recording of Afghan telephone calls by the NSA," May 23, 2014, https://wikileaks.org/WikiLeaks-statement-on-the-mass.html (accessed July 8, 2014).

[21] Under the 4th Amendment to the US Constitution, in order for the government to conduct a search of "persons, houses, papers, and effects," the government must demonstrate to a judge probable cause that a search would reveal evidence of a crime or contraband. See U.S. Const. amend. IV.

The surveillance programs at issue in this report are generally introduced in the name of national security or intelligence rather than criminal law enforcement. Instead of trying to piece together facts about events that have already occurred, they aim to inform the government broadly and—in theory—help prevent future events like terrorist attacks. The programs disclosed by Snowden operate on a much larger scale than more traditional surveillance methods used for law enforcement purposes—collecting hundreds, thousands, or millions of records at a time. By its nature, large-scale surveillance often implicates the interests of many people who are not suspected of any wrongdoing.

Large-scale surveillance by the US government proceeds under a variety of legal authorities. The main authorities known to the public as of July 2014 are Section 215 of the USA PATRIOT Act (PATRIOT Act), Section 702 of the Foreign Intelligence Surveillance Act (FISA), and Executive Order 12,333.[22] In addition to these tools, the FBI also has the power to collect significant amounts of information relevant to national security investigations—without judicial oversight and sometimes in large quantities—using National Security Letters (NSLs).[23]

Surveillance under Section 215 of the PATRIOT Act

The phone call metadata program revealed by the *Guardian* in June 2013 operates under Section 215 of the PATRIOT Act (Section 215), which allows for the collection of "tangible things" or business records that are "relevant" to an authorized investigation.[24] A major point of controversy concerning Section 215 is that the FISA Court has clearly adopted a weak standard for relevance (and seemingly not in line with Congress's intent) if it has concluded that Verizon should turn over metadata of *all* domestic calls on a rolling basis.

---

[22] Section 215 and Section 702 are provisions of federal law, passed by Congress and signed by the president. USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Section 215; FISA Amendments Act of 2008, H.R. 6304, Title VII, Section 702. Executive orders are different; although they also have the force of law, and are subject to judicial review, the president can sign (or change or revoke) them unilaterally to help guide the operations of the Executive Branch. For the applicable executive order, see Executive Order 12,333, "United States Intelligence Activities," December 4, 1981, http://www.archives.gov/federal-register/codification/executive-order/12333.html (accessed July 9, 2014).

[23] NSLs operate like subpoenas except that they are not issued by judges. An FBI agent can issue them to seek metadata and other non-content information from third parties, without prior judicial authorization. Controversially, NSLs can be written to bar the recipient from discussing that he or she has been asked for information. While various forms of NSLs have existed for years, their use increased with the passage of the USA PATRIOT Act in 2001. None of the Snowden revelations as of July 2014 concerned NSLs in any significant way.

[24] Human Rights Watch, "Comments for the Review Group on Intelligence and Communications Technologies," October 11, 2013, http://www.hrw.org/news/2013/10/11/human-rights-watch-comments-review-group-intelligence-and-communications-technologie.

Surveillance under Section 702 of FISA

Section 702 of FISA (Section 702) is a provision of federal law, created by the FISA Amendments Act (FAA), that permits the Executive Branch to issue year-long warrants for collecting the content of international communications and other data of persons reasonably believed to be outside the US, specifically to acquire broadly-defined foreign intelligence information. The FISA Court periodically approves the government's "minimization procedures," as well as "targeting procedures" designed to ensure surveillance is targeted at non-US persons outside the US, but it does not issue specific warrants nor approve specific targets of surveillance.[25] Subject to minimization, the government can collect and use the international communications or internationally-shared data of Americans under Section 702. The government relies on Section 702 to collect communications from US service providers as well as to monitor fiber optic cables as they enter the United States, and both forms of surveillance involve the collection of US persons' communications.[26] The targeting and minimization procedures that have been made public so far provide almost no protections for non-US persons under these programs.[27]

Surveillance under Executive Order 12,333

Executive Order 12,333 took effect when President Reagan signed it in 1981.[28] It has been updated from time to time, but it remains the primary executive order addressing US

---

[25] The ACLU has summarized the implications of the various provisions in the FAA, including noting the breadth of permissible surveillance. For example, "[u]nlike surveillance under traditional FISA, surveillance under the FAA is not predicated on probable cause or individualized suspicion. The government's targets need not be agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Rather, the FAA permits the government to target any foreigner located outside the United States so long as the programmatic purpose of the surveillance is to acquire 'foreign intelligence information.'" See Submission of Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union Foundation to Privacy and Civil Liberties Oversight Board, Public Hearing on Section 702 of the FISA Amendments Act, March 19, 2014, http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf (accessed July 9, 2014), p. 5. Further, "[n]othing in the Act requires the government even to inform the court who its surveillance targets are (beyond to say that the targets are outside the United States), what the purpose of its surveillance is (beyond to say that a "significant purpose" of the surveillance is foreign intelligence), or which Americans' privacy is likely to be implicated by the acquisition." See ibid., p. 9. Much information can be swept in "incidentally" in searches for information relating to targeted individuals, including communications of people who have no connection with the intelligence target.

[26] Rush and Ball, "PRISM Scandal," *Guardian*, http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining; "NSA slides explain the PRISM data-collection program," *Washington Post*, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[27] A report from July of 2014 revealed that "ordinary internet users, American and non-American alike, far outnumber legally targeted foreigners in communications intercepted by the [NSA] from U.S. digital networks." Barton Gellman, Julie Tate, and Ashkan Soltani, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," *Washington Post*, July 5, 2014, http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html (accessed July 16, 2014).

[28] Executive Order 12,333 is available online at http://www.archives.gov/federal-register/codification/executive-order/12333.html.

intelligence activities, especially those undertaken abroad. Like the minimization procedures discussed above, Executive Order 12,333 also provides some protections for US persons,[29] requiring (when it comes to US persons) that the intelligence community "use the least intrusive techniques feasible."[30] Yet the US government is reported to be conducting large-scale surveillance under 12,333, such as "secretly breaking into the main communications links that connect Yahoo and Google data centers around the world."[31] It appears, then, that the government has the power to collect large amounts of information even on US persons through the executive order.[32]

Privacy Protections under Existing US Surveillance Programs

US officials have argued that they have put effective mechanisms in place to protect privacy. They have pointed to two types of protections: "minimization" procedures and oversight mechanisms.

Minimization Procedures

The government has in various contexts adopted policies called "minimization procedures," which are designed to limit its collection and use of information pertaining to "United States persons" (US persons) whether they are inside or outside the US.[33] In theory, minimization limits the collection or use of information on US persons; it does not appear to apply to any broad category of non-US person, or provide safeguards for their data or

---

[29] Executive Order 12,333, Part 1.1(d): Goals. Specifically, the order notes that agencies and departments should build in "full consideration of the rights of United States persons" while attempting to maximize the benefit of the country's intelligence efforts. Ibid.

[30] Ibid., Part 2.4: Collection Techniques. The order does not provide much protection for non-US persons, except to limit searches of their personal property by the CIA. Ibid.

[31] Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden Documents say," *Washington Post*, October 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (accessed July 9, 2014).

[32] For more information on Executive Order 12,333, see Mark Jaycox, Electronic Frontier Foundation, "Three Leaks, Three Weeks, and What We've Learned About the US Government's Other Spying Authority: Executive Order 12333,", November 5, 2013, https://www.eff.org/deeplinks/2013/10/three-leaks-three-weeks-and-what-weve-learned-about-governments-other-spying (accessed July 9, 2014).

[33] US citizens, lawful permanent residents of the US, companies incorporated in the US, and "unincorporated association[s] a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence" all count as "US persons." 50 U.S. Code § 1801 (i). The minimization procedures published by the *Guardian* in June of 2013 indicate that the definition of "US person" used by the NSA derives from the original language of the Foreign Intelligence Surveillance Act of 1978 (FISA). "Procedures used by NSA to minimize data collection from US persons: Exhibit B, full document," *Guardian*, June 20, 2013, http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document (accessed July 8, 2014), p. 2. For the original FISA definition, see 50 U.S. Code § 1801(i).

communications. Not all of the government's minimization procedures are public, however, so it is impossible to know their full extent.[34]

Some of the surveillance programs also operate under some measure of court supervision—most notably, the FISC and its appellate counterpart, both composed of federal judges. However, those courts operate in secrecy and do not have any structures in place that would offer meaningful opposition or any kind of counterweight to government requests for approval of surveillance programs. Nor are most FISC orders made public. Indeed, the bulk collection of metadata under Section 215 was authorized by the FISC in secret, and the public did not know about it until years later.

The agencies involved in conducting surveillance also have internal positions for the purpose of promoting accountability, such as inspectors general or privacy and civil liberties officers, though it is unclear what role—if any—they have played in checking the surveillance programs revealed over the past year. Executive bodies such as the Privacy and Civil Liberties Oversight Board (PCLOB) also have some power to exercise oversight, but their recommendations are not binding.[35]

Both the US House of Representatives and the Senate have standing Committees on Intelligence and on the Judiciary, which are designed, in theory, to provide oversight over the intelligence community's activities. However, much of what these committees do is itself secret. Moreover, effective oversight requires that the intelligence community candidly share information with these committees. As Senator Ron Wyden, from the Senate Intelligence Committee, has noted, senior officials have repeatedly made misleading statements about their activities in congressional hearings.[36] Senate

---

[34] We have submitted a Freedom of Information Act Request seeking remaining minimization procedures. To read the request, see Appendix.

[35] A number of individuals and groups have recently criticized the oversight of the intelligence community as inadequate, highlighting, for example, the limited role for the FISA Court, the lack of public transparency, and the strength of the PCLOB. See, e.g., Human Rights Watch, "Comments to the Privacy and Civil Liberties Oversight Board (PCLOB)", August 1, 2013, http://www.hrw.org/news/2013/08/01/comments-human-rights-watch-privacy-and-civil-liberties-oversight-board-pclob; letter from Human Rights Watch to President Obama Urging Surveillance Reforms, January 16, 2014, http://www.hrw.org/news/2014/01/16/letter-president-obama-urging-surveillance-reforms; Jameel Jaffer, "Obama's NSA Proposal Reveals Broken Oversight System," *Guardian*, March 25, 2014, https://www.aclu.org/blog/national-security/obamas-nsa-proposal-reveals-broken-oversight-system (accessed July 9, 2014); ACLU, "Support Oversight of the Secret FISA Court," https://www.aclu.org/support-oversight-secret-fisa-court (accessed July 9, 2014).

[36] Ron Wyden, "Statement at Senate Intelligence Committee's Open Hearing," January 29, 2014, http://www.wyden.senate.gov/news/press-releases/wyden-statement-at-senate-intelligence-committees-open-hearing (accessed July 9, 2014).

Intelligence Committee Chairman Dianne Feinstein has also noted that the intelligence community has failed fully to inform the committee about its surveillance activities.[37]

The Current Surveillance Debate

The Snowden revelations have prompted domestic and international debates about whether and how to reform US surveillance practices. Among US policymakers, most of that debate has focused on the impact of surveillance on privacy rights of US persons. The US government's perspective is that its surveillance activities are lawful and necessary to protect US national security.

Even so, in response to public pressure, both President Barack Obama and the US Congress have expressed some willingness to consider reforms. In August of 2013, President Obama created the Review Group on Intelligence and Communications Technologies (President's Review Group).[38] The group issued a report in December of 2013, recommending a series of reforms to US surveillance practices.[39] The PCLOB has also held hearings on the surveillance programs, recommending its own changes to Section 215 in a report it released in January of 2014.[40] The PCLOB issued a second report in July of 2014, recommending more modest changes to Section 702.[41]

---

[37] Diane Feinstein, "Statement on Intelligence Collection of Foreign Leaders," October 28, 2013, http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=61f9511e-5d1a-4bb8-92ff-a7eaa5becaco (accessed July 9, 2014).

[38] "About the Review Group on Intelligence and Communications Technologies," Office of the Director of National Intelligence, accessed July 9, 2014, http://www.dni.gov/index.php/intelligence-community/review-group.

[39] See Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," December 12, 2013, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed July 9, 2014).

[40] Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf. Both Human Rights Watch and the ACLU (working in conjunction with Amnesty International) submitted comments to the PCLOB, and provided someone to testify before the PCLOB as well. Human Rights Watch, "Comments of Human Rights Watch to the Privacy and Civil Liberties Oversight Board (PCLOB)," August 1, 2013, http://www.hrw.org/news/2013/08/01/comments-human-rights-watch-privacy-and-civil-liberties-oversight-board-pclob; ACLU, "Submission to the PCLOB on US Surveillance and Human Rights Law," April 16, 2014, https://www.aclu.org/national-security-technology-and-liberty/submission-pclob-us-surveillance-and-human-rights-law (accessed July 9, 2014).

[41] Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," July 2, 2014, http://www.pclob.gov/All%20Documents/Report%200n%20the%20Section%20702%20Program/PCLOB-Section-702-Report-PRE-RELEASE.pdf (accessed July 9, 2014).

In January of 2014, President Obama gave a speech in which he acknowledged the legitimacy of some concerns about government surveillance.[42] He vowed to make certain changes, such as shifting the storage of information from the bulk domestic metadata program to private companies.[43]

Most recently, Congress has debated legislation that would make some adjustments to Section 215 of the USA PATRIOT Act. In May of 2014, the House passed a version of what has been known as the "USA FREEDOM Act." An initial draft of the bill contained provisions that would have constituted a significant step towards ending bulk collection of US persons' phone records and metadata, but the version that the House finally passed was significantly watered down.[44] Many of the bill's original sponsors and supporters now question whether the current version would prevent large-scale collection of business records or metadata in practice, defeating the objective of the bill.[45] As of July 2014, the Senate was contemplating similar legislation. Both bills are limited in that they fail significantly to address US surveillance under authorities other than Section 215.[46] As of this writing, there has yet to be any significant tightening of the legal authorities that facilitate an astonishing scale of government collection of metadata and communications content. Even were the USA FREEDOM Act to become law in some form, massive and largely indiscriminate collection of content appears set to continue under Section 702 and Executive Order 12,333.

More broadly, however, the debates in Congress and among relevant members of the Executive Branch have failed to account for a variety of costs of large-scale surveillance programs, including not only the implications of surveillance for individuals' privacy rights,

---

[42] "Obama's Speech on N.S.A. Phone Surveillance," *New York Times*, January 17, 2014, http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html?_r=0 (accessed July 9, 2014). For commentary on that speech, see "Statement on US President Obama's surveillance speech," Human Rights Watch news release, January 17, 2014, http://www.hrw.org/news/2014/01/17/statement-us-president-obama-s-surveillance-speech.

[43] He also imposed certain interim limits on the querying of that information, including requiring judicial oversight and limiting searches of targets' contacts to those linked by two degrees of separation rather than three.

[44] In part this was a result of last-minute changes shortly before the vote. Andrea Peterson, "NSA reform bill passes House, despite loss of support from privacy advocates," *Washington Post*, May 22, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/22/nsa-reform-bill-passes-house-despite-loss-of-support-from-privacy-advocates/ (accessed July 9, 2014). See also "US Senate: Salvage Surveillance Reform," Human Rights Watch news release, May 22, 2014, https://www.hrw.org/news/2014/05/22/us-senate-salvage-surveillance-reform.

[45] Peterson, "NSA reform bill passes House," *Washington Post*, http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/22/nsa-reform-bill-passes-house-despite-loss-of-support-from-privacy-advocates/.

[46] The USA Freedom Act, as passed by the House, would modify a bulk phone metadata program authorized under Section 215 of the USA PATRIOT Act, and includes some provisions on NSLs. It does not significantly address various other authorities, like Section 702 of FISA, or Executive Order 12,333, which appear to lie behind most of the surveillance programs revealed thus far in the Snowden documents.

both inside and outside the US, but also the "chilling" or inhibiting effect surveillance can have on the exercise of freedoms of expression and association. Indeed, early research indicates that the revelations in 2013 and continuing to date have begun to have a chilling effect on private individuals' electronic communications practices and activities.[47] And, as this report documents, surveillance can have a profound impact on the practice of journalism and law.

The Broader Context: Government Secrecy and the Crackdown on Leaks

The increase in US government surveillance has come at the same time as an increase in criminal investigations and prosecutions of leaks, as well as the establishment of new government programs to prevent leaks of information or otherwise restrict government officials' contact with the media.[48] These steps have raised further concerns over public access to information, particularly as many journalists, advocates, and even some members of Congress and the Executive Branch believe the government over-classifies information, prohibiting access to much information that is not actually sensitive.[49]

Over-Classification

The power to classify US government information rests with the president, the vice president, the heads of federal agencies, and anyone else designated by the president, though only certain types of information may be classified.[50] Three levels of classification are available—top secret, secret, and confidential—calibrated to the seriousness of the

---

[47] E.g., Stephen Cobb, "New Harris poll shows NSA revelations impact online shopping, banking, and more," *We Live Security*, April 2, 2014, http://www.welivesecurity.com/2014/04/02/harris-poll-nsa-revelations-impact-online-shopping-banking/ (accessed July 9, 2014); Alex Marthews and Catherine Tucker, "Government Surveillance and Internet Search Behavior," unpublished paper, March 24, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564 (accessed July 9, 2014).

[48] The meaning of the term "leak" may vary by context, so for simplicity, we will use the term broadly to include the unauthorized disclosure of government information to the press, even if that information is not sensitive, as well as the release (whether authorized by a high-level official or not) of classified information without prior declassification. On this definition, "instant declassification"—the idea that a high-level official can properly declassify information simply by making it public—would still count as a leak. For more on "instant declassification," see Jennifer K. Elsea, Congressional Research Service, "The Protection of Classified Information: The Legal Framework," December 17, 2002, http://legalresearchplus.files.wordpress.com/2013/01/rs21900.pdf (accessed July 9, 2014), pp.11-14.

[49] E.g., Elizabeth Goitein and David M. Shapiro, Brennan Center for Justice, New York University School of Law, "Reducing Overclassification Through Accountability," October 5, 2011, http://www.brennancenter.org/publication/reducing-overclassification-through-accountability (accessed July 9, 2014); Human Rights Watch interview with Dana Priest, national security reporter at the *Washington Post*, Washington, DC, December 17, 2013; Human Rights Watch interview with Jane Mayer, staff writer for *The New Yorker*, Washington, DC, January 16, 2014.

[50] Executive Order 13,526 provides the current guidelines for the federal government's classification and declassification of information. Elsea, Congressional Research Service, "The Protection of Classified Information," http://legalresearchplus.files.wordpress.com/2013/01/rs21900.pdf, p. 3.

expected harm to protected government interests like national security from publication of the information.[51]

In classifying information, officials are supposed to designate the length of time for which the information is expected to remain sensitive; in theory, much of the information that is currently classified should at some point become available to the public.[52] Of over 95 million classification decisions made by the federal government in 2012, however, the vast majority were "derivative" rather than "original"—meaning they involved reclassifying information that had previously been marked as classified.[53]

Officials found to have leaked classified information may face a number of penalties, ranging from administrative sanctions to criminal prosecution.[54] The Obama administration has pursued eight prosecutions of officials for allegedly releasing information to the press—an unprecedented number.[55] By contrast, since 1917 (when the Espionage Act—the law under which most leakers have been prosecuted—took effect), all previous administrations pursued three leak prosecutions combined.[56]

"Insider Threats"

In response to the leaks of information to Wikileaks by former US soldier Chelsea Manning, in October 2011, President Obama implemented the "Insider Threat Program" (or "ITP").[57]

---

[51] Ibid.

[52] Ibid., p. 4.

[53] Information Security Oversight Office, "Annual Report to the President 2012," http://www.archives.gov/isoo/reports/2012-annual-report.pdf (accessed July 9, 2014), pp. 4, 7. For more, see David E. Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information," *Harvard Law Review*, vol. 127 (2013), p. 575.

[54] Elsea, Congressional Research Service, "The Protection of Classified Information," http://legalresearchplus.files.wordpress.com/2013/01/rs21900.pdf, pp. 10-11.

[55] Leonard Downie Jr. with reporting by Sara Rafsky, Committee to Protect Journalists, "The Obama Administration and the Press," October 10, 2013, https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php (accessed July 9, 2014) (documenting the various leak prosecutions pursued by the Obama administration). At the same time, the administration continues to benefit from selective, authorized leaks to the press. For an in-depth look at the US government's handling of leaks, see Pozen, "The Leaky Leviathan," *Harvard Law Review*, p. 512. Note that the Obama administration inherited two of its eight prosecutions from the Bush administration.

[56] These are the widely accepted numbers, and the recent spike is not in dispute; however, there may be room for some disagreement at the margins. See Pozen, "The Leaky Leviathan," *Harvard Law Review*, p. 537.

[57] Marisa Taylor and Jonathan S. Landay, "Obama's crackdown views leaks as aiding enemies of U.S.," *McClatchy*, June 20, 2013, http://www.mcclatchydc.com/2013/06/20/194513/obamas-crackdown-views-leaks-as.html (accessed July 9, 2014); "National Insider Threat Taskforce," Office of the National Counterintelligence Executive, accessed July 9, 2014, http://www.ncix.gov/nittf/index.php.

The program requires training of federal employees to beware of insider threats—colleagues who may be inclined to leak classified information.[58] Failure to report suspicious activity by colleagues can result in hefty penalties, including loss of security clearance and criminal charges.[59] One guide on insider threats, prepared by the Defense Security Service—an agency of the Department of Defense that provides security support to various defense and federal agencies—lists a government worker's "exploitable behavior traits" and attempting to work in private as "potential espionage indicators."[60]

While the point of the program is ostensibly to limit leaks of classified information,[61] the ITP covers a wide range of government agencies (including, for example, the Peace Corps and the Department of Agriculture), and it makes clear that it sets out only minimum standards.[62] Agencies thus have flexibility to crack down widely, with potential implications for the ability of employees safely to discuss even unclassified matters with the press. Indeed, *McClatchy* reported that several agencies have already applied the policy to justify protecting such information.[63]

In reporting on sensitive areas, journalists often work with information that is not itself classified. Skilled journalists often assemble fragments of a story bit by bit without ever requiring a source to provide protected information. As a result, increased restrictions on the discussion of even unclassified information make it harder for journalists to gather the pieces of information that compose the whole picture.

---

[58] Taylor and Landay, "Obama's crackdown views leaks as aiding enemies of U.S.," *McClatchy*, http://www.mcclatchydc.com/2013/06/20/194513/obamas-crackdown-views-leaks-as.html. Technically, the policy does not define "insider threats" in relation to classified information specifically, but the program is designed to protect classified information. See Office of the National Counterintelligence Executive, "National Insider Threat Policy," http://www.ncix.gov/nittf/docs/National_Insider_Threat_Policy.pdf (accessed July 9, 2014), p. 5.

[59] Taylor and Landay, "Obama's crackdown views leaks as aiding enemies of U.S.," *McClatchy*, http://www.mcclatchydc.com/2013/06/20/194513/obamas-crackdown-views-leaks-as.html#.Uccy--vmVHl.

[60] Defense Security Service, "Insider Threats: Combating the ENEMY within your organization," http://www.dss.mil/documents/ci/Insider-Threats.pdf (accessed July 9, 2014), p. 2.

[61] Office of the National Counterintelligence Executive, "National Insider Threat Policy," http://www.ncix.gov/nittf/docs/National_Insider_Threat_Policy.pdf, p. 1. The policy applies to "all executive branch departments and agencies with access to classified information, or that operate or access classified computer networks; all employees with access to classified information, including classified computer networks (and including contractors and others who access classified information, or operate or access classified computer networks controlled by the federal government); and all classified information on those networks." Ibid.

[62] Office of the National Counterintelligence Executive, "National Insider Threat Policy," http://www.ncix.gov/nittf/docs/National_Insider_Threat_Policy.pdf, p. 5.

[63] Taylor and Landay, "Obama's crackdown views leaks as aiding enemies of U.S.," *McClatchy*, http://www.mcclatchydc.com/2013/06/20/194513/obamas-crackdown-views-leaks-as.html#.Uccy--vmVHl.

Limiting Intelligence Officials' Contact with the Media

Within the intelligence community, recent rules go even further. Director of National Intelligence James Clapper issued Intelligence Community Directive 119 in March of 2014, prohibiting intelligence community employees from all unauthorized contact with the press and requiring employees to report unauthorized or unintentional press contact on certain topics.[64] The Office of the Director of National Intelligence also updated its press rules (through ODNI Instruction 80.04) in April of 2014, requiring "pre-publication review" of certain information that any member of the intelligence community makes available to the public.[65] The range of topics that trigger pre-publication review include those that "discuss … operations, business practices, or information related to the ODNI, the IC, or national security," and the rules do not distinguish between classified or unclassified information, or between information that is private and information that is already in the public domain.[66] Steve Aftergood, Director of the Federation of American Scientists' Project on Government Secrecy, observed that the "newly updated Instruction will no doubt inhibit informal contacts between ODNI employees and members of the general public, as it is intended to do."[67]

[64] Hadas Gold and Josh Gerstein, "Clapper signs strict new media directive," *Politico*, April 21, 2014, http://www.politico.com/blogs/media/2014/04/clapper-signs-strict-new-media-directive-187162.html (accessed July 9, 2014).

[65] Steven Aftergood, "ODNI Requires Pre-Publication Review of All Public Information," *Secrecy News*, May 8, 2014, at http://fas.org/blogs/secrecy/2014/05/odni-prepub/ (accessed July 9, 2014).

[66] Ibid.

[67] Ibid.

II. The Impact of Surveillance on Journalists

> Every national security reporter I know would say that the atmosphere in which professional reporters seek insight into policy failures [and] bad military decisions is just much tougher and much chillier.
> — Steve Coll, staff writer for *The New Yorker* and Dean of the Graduate School of Journalism at Columbia University, February 14, 2014

Numerous US-based journalists covering intelligence, national security, and law enforcement describe the current reporting landscape as, in some respects, the most difficult they have ever faced. "This is the worst I've seen in terms of the government's efforts to control information," acknowledged Jonathan Landay, a veteran national security and intelligence correspondent for *McClatchy Newspapers*.[68] "It's a terrible time to be covering government," agreed Tom Gjelten, who has worked with National Public Radio for over 30 years.[69] According to Kathleen Carroll, senior vice president and executive editor of The Associated Press, "We say this every time there's a new occupant in the White House, and it's true every time: each is more secretive than the last."[70] Journalists are struggling harder than ever before to protect their sources, and sources are more reluctant to speak. This environment makes reporting both slower and less fruitful.

Journalists interviewed for this report described the difficulty of obtaining sources and covering sensitive topics in an atmosphere of uncertainty about the range and effect of the government's power over them. Both surveillance and leak investigations loomed large in this context—especially to the extent that there may be a relationship between the two. More specifically, many journalists see the government's power as menacing because they know little about when various government agencies share among themselves information collected through surveillance, and when they deploy that information in leak investigations.[71] "[Government officials have been] very squishy about what they have and

---

[68] Human Rights Watch interview with Jonathan Landay, national security and intelligence correspondent for *McClatchy Newspapers,* Washington DC, December 12, 2013.

[69] Human Rights Watch telephone interview with Tom Gjelten, correspondent with NPR, March 18, 2014.

[70] Human Rights Watch interview with Kathleen Carroll, Senior Vice President and Executive Editor of The Associated Press, New York, New York, May 8, 2014.

[71] E.g., Human Rights Watch interviews with Jonathan Landay, December 12, 2013, and an investigative journalist for a major outlet, New York, New York, January 23, 2014.

[what they] will do with it," observed James Asher, Washington Bureau Chief for *McClatchy Co.*, the third largest newspaper group in the country.[72] One Pulitzer Prize-winning reporter for a newspaper noted that even a decrease in leak prosecutions is unlikely to help, "unless we [also] get clear lines about what is collectable and usable."[73]

Others agreed. "I'm pretty worried that NSA information will make its way into leak investigations," said one investigative journalist for a major outlet.[74] A reporter who covers national defense expressed concern about the possibility of a "porous wall" between the NSA and the Department of Justice, the latter of which receives referrals connected to leak investigations.[75] Jonathan Landay wondered whether the government might analyze metadata records to identify his contacts.[76] A national security reporter summarized the situation as follows: "Do we trust [the intelligence] portion of the government's knowledge to be walled off from leak investigations? That's not a good place to be."[77]

While most journalists said that their difficulties began a few years ago, particularly with the increase in leak prosecutions, our interviews confirmed that for many journalists large-scale surveillance by the US government contributes substantially to the new challenges they encounter. The government's large-scale collection of metadata and communications makes it significantly more difficult for them to protect themselves and their sources, to confirm details for their stories, and ultimately to inform the public.

In the 1970s, many journalists spoke with sources by phone, and the government already had the technological capacity to tap those calls if it so chose. But traditional forms of wiretapping or physical surveillance were time consuming and resource intensive. Today, so many more transactions are handled electronically that there exists a tangible, easy-to-store, easy-to-access record of a much larger proportion of any given person's life: banking transactions, internet browsing, driving habits (though EZ Pass records, license plate cameras, and GPS systems), cell phone location and activity, emailing patterns, and more. Metadata can reveal intimate details about people, such as religious affiliations, medical

---

[72] Human Rights Watch interview with James Asher, Washington Bureau Chief for *McClatchy Co.*, Washington DC, December 12, 2013.

[73] Human Rights Watch interview with a reporter, Washington, DC, December 17, 2013.

[74] Human Rights Watch interview with an investigative journalist for a major outlet, New York, New York, January 23, 2014.

[75] Human Rights Watch interview with a reporter who covers national defense issues, Washington DC-area, January 16, 2014.

[76] Human Rights Watch interview with Jonathan Landay, December 12, 2013.

[77] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

diagnoses, and the existence of private relationships. Meanwhile, as more transactions have become digitalized, the government has acquired a much greater technical capacity to gather, store, analyze, and sift through electronic data.

Even with rapidly evolving techniques for conducting research and contacting sources, journalists expressed concern that widespread government surveillance constrains their ability to investigate and report on matters of public concern, and ultimately undermines democratic processes by hindering open, informed debate.

Losing Sources

One of the most common concerns journalists expressed to us was that their sources were drying up.[78] According to James Asher, "[Before] you'd start pulling the curtain back and more people would come forward. Many fewer people are coming forward now."[79]

Journalists expressed diverse views as to when and why reporting conditions began to deteriorate. Some pointed to the attacks of September 11, 2001 and the subsequent expansion in the amount of information considered sensitive for national security purposes.[80] Others emphasized a cluster of stories that appeared in the media in 2005, including the first reports of the NSA's domestic surveillance programs and confirmation of black sites in Poland.[81] The most common explanation, however, was a combination of increased surveillance and the Obama Administration's push to minimize unauthorized leaks to the press (both by limiting government employees' contact with journalists, such as through the Insider Threat Program, and by ramping up prosecutions of allegedly unauthorized leaks, as described above).[82] That trend generates fear among both sources

---

[78] See also Leonard Downie Jr. with reporting by Sara Rafsky, Committee to Protect Journalists, "The Obama Administration and the Press," October 10, 2013, https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php (accessed July 9, 2014) (also documenting these concerns).

[79] E.g., Human Rights Watch interview with James Asher, Washington DC, December 12, 2013.

[80] E.g., Human Rights Watch telephone interview with Tim Weiner, reporter for the *New York Times*, January 31, 2014; Human Rights Watch interview with Barton Gellman, senior fellow at The Century Foundation, New York, New York, February 10, 2014.

[81] Human Rights Watch telephone interview with Philip Bennett, Professor at Duke University and former managing editor of the Washington Post, February 26, 2014; Human Rights Watch telephone interview with Tom Gjelten, March 18, 2014. Bennett said there is "no doubt in my mind" that a cluster of national security stories in 2005 rattled the government, and prompted it to crack down on the press. Gjelten reported beginning an extended leave from reporting in March of 2005. He encountered a radical shift in source cooperation upon his return in December of 2007. "[It was] like a whole different world."

[82] These views are not mutually exclusive, and some journalists subscribed to multiple theories. Some journalists also reported limited concern about the effect of large-scale electronic surveillance by the US government or said that they had not observed a chilling effect, though that view was uncommon and in some cases reflected the journalist's coverage areas. E.g., Human Rights Watch interview with a reporter covering the Supreme Court, Washington DC, January 15, 2014; Human

and journalists about the consequences of communicating with one another—even about innocuous, unclassified subjects.[83]

Even sources who are not sharing classified information risk losing their security clearances and ability to work. Steve Engelberg, the editor-in-chief of ProPublica, described the security clearance that a source holds as their "driver's license in the intelligence community."[84] According to him, "[It's] easy to lose it, at which point you can't work."[85] As a result, loss of a security clearance is a "big sanction."[86] Scott Horton, who writes on national security for *Harper's Magazine*, sees the risks to sources as a very real and tangible threat to their willingness to speak to reporters and to ensure effective reporting:

> Reveal details about government activity and you may lose almost everything: your clearance, your position, and your pension. You may have to hire an attorney, and you may have your reputation destroyed in the press by their own counter-leaks, making it impossible to get a new job.[87]

Yet while loss of one's security clearance, job, or pension can be serious enough, the risk of prosecution for leaking has never been higher.[88] "It is not lost on us, or on our sources, that there have been eight criminal cases against sources [under the current administration] versus three before [under all previous administrations combined]," observed Charlie Savage, a Pulitzer Prize-winning reporter for the *New York Times*.[89] That

---

Rights Watch interview with an investigative journalist most recently covering (among other things) state-level politics, Washington DC, January 17, 2014; Human Rights Watch telephone interview with Mark Bowden, author and Distinguished Writer in Residence at The University of Delaware, January 21, 2014.

[83] Again, for more, see Downie Jr. with reporting by Rafsky, Committee to Protect Journalists, "The Obama Administration and the Press," https://www.cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php.

[84] Human Rights Watch interview with Stephen Engelberg, editor-in-chief of ProPublica, New York, January 30, 2014.

[85] Ibid.

[86] Ibid. *McClatchy* calls this a "career-killing penalty." Marisa Taylor and Jonathan S. Landay, "Obama's crackdown views leaks as aiding enemies of U.S.," *McClatchy*, June 20, 2013, http://www.mcclatchydc.com/2013/06/20/194513/obamas-crackdown-views-leaks-as.html#.Uccy--vmVHl (accessed July 14, 2014).

[87] Human Rights Watch interview with Scott Horton, writer on national security for *Harper's Magazine*, New York, New York, January 13, 2014.. For more on the costs associated with leak prosecutions, see also David E. Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information," *Harvard Law Review*, vol. 127 (2013), p. 553.

[88] Agencies are also making many referrals to the Department of Justice that do not become full prosecutions. Human Rights Watch interview with Peter Finn, National Security Editor at the *Washington Post*, Washington DC, December 17, 2013. For some statistics on the number of leak investigation referrals, see Steven Aftergood, "'Crimes Reports' and the Leak Referral Process," *Secrecy News*, Dec. 17, 2002, http://www.fas.org/blogs/secrecy/2012/12/crimes_reports/ (accessed July 11, 2014). Newer statistics are difficult to locate.

[89] Human Rights Watch telephone interview with Charlie Savage, reporter for the *New York Times*, March 14, 2014.

spike sends a message, even when prosecutions do not end in convictions. "I understand why they do it," noted another Pulitzer Prize-winning reporter.[90] "Even the cases that blow up in [the government's] face have the intended effect."[91]

In February of 2014, Stephen Kim, who faced a leak prosecution, described the costs of the process:

> This has been a huge blow for me and for my entire family. I had to give up a job that I had liked. It also destroyed my marriage. My family had to spend all of the money they had saved up and even sell their house to pay my legal fees. I hardly have any remaining assets.[92]

Although Kim eventually pleaded guilty to unauthorized disclosure of classified information, his description of the harm to himself and his family represents the setbacks anyone prosecuted might face, irrespective of the ultimate disposition of the case. Thomas Drake, who was also prosecuted by the Obama administration for leaking information to the press, reported similar costs.[93] The government dropped all of its major counts against Drake right before his trial was scheduled to begin, in exchange for a guilty plea to a minor misdemeanor, triggering harsh criticism from the judge for putting Drake through "four years of hell."[94]

While sources' employers sometimes have legitimate reasons for discouraging conversations about certain matters with the press, the stakes and the consequences have increased substantially in recent years, making conversations about declassified or innocuous subjects not worth the risk. One journalist described a source who was eventually fired when his or her employer found signs of the source's initial contact with journalists a year earlier, even though the source had not leaked classified information.[95]

---

[90] Human Rights Watch interview with a reporter, Washington, DC, December 17, 2013.

[91] Ibid.

[92] Steven Aftergood, "Stephen Kim Leak Case Heats Up," October 23, 2013, *Secrecy News,* http://fas.org/blogs/secrecy/2013/10/kim-heat/ (accessed July 11, 2014). Kim was a contractor with the State Department who was accused of leaking classified information to Fox News reporter James Rosen in 2009. The information, derived from a top-secret intelligence report, described North Korea's intentions to perform nuclear tests.

[93] For more on Drake's case, see PBS interview with Thomas Drake, Frontline, December 10, 2013, http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-thomas-drake/ (accessed July 16, 2014).

[94] Scott Shane, "No Jail Time in Trial Over N.S.A. Leak," *New York Times*, July 15, 2011, http://www.nytimes.com/2011/07/16/us/16leak.html (accessed July 11, 2014). The judge also called the government's conduct "unconscionable." See also Pozen, "The Leaky Leviathan," *Harvard Law Review*, p. 553 (discussing the Drake case).

[95] Human Rights Watch interview with Peter Finn, December 17, 2013.

At the same time, the fact that senior government officials themselves routinely appear to authorize "leaks" of classified information has bred cynicism about the government's claims that these prosecutions are merely about enforcing the law. "Of course, leaks that help the government are sanctioned," observed Brian Ross, chief investigative correspondent for ABC News.[96] Bart Gellman, senior fellow at The Century Foundation, and the winner of multiple Pulitzer Prizes, argued that official, sanctioned leaks reveal much more classified information than unofficial ones.[97]

Yet, beyond the leak investigations and administrative efforts to prevent leaks, many journalists said that the government's increased capacity to engage in surveillance—and the knowledge that it is doing so on an unprecedented scale—has made their concerns about how to protect sources much more acute and real.

> "That's what Snowden meant for me. There's a record of everywhere I've walked, everywhere I've been."
> —A national security reporter

In fact, some believed that surveillance may be a direct cause of the spike in leak investigations. "It used to be that leak investigations didn't get far because it was too hard to uncover the source, but with digital tools it's just much easier, and sources know that." observed Bart Gellman.[98] Peter Maass, a senior writer at *The Intercept*, concurred: "Leak investigations are a lot easier because you leave a data trail calling, swiping in and out of buildings, [and] walking down a street with cameras. It's a lot easier for people to know where you're going and how long you're there."[99] Charlie Savage raised a similar point: "[E]lectronic trails mak[e] it easier to figure out who's talking to reporters. That has made it realistic [to investigate leaks] in a way that it wasn't before."[100] Peter Finn, the National

---

[96] Human Rights Watch interview with Brian Ross, Chief Investigative Correspondent for ABC News, New York, New York, February 11, 2014. Law professor David Pozen calls this view "jaundiced but not unfounded." Pozen, "The Leaky Leviathan," *Harvard Law Review*, p. 562. One reporter for a newspaper similarly criticized what he sees as a "double standard in the government's pursuit of [leak] prosecutions." Human Rights Watch interview with a reporter, Washington, DC, December 17, 2013. Phil Bennett, a former managing editor of the *Washington Post* and now a professor at Duke University, recalled then Vice-President Dick Cheney disclosing a torrent of classified information to Bob Woodward just weeks after 9/11 that portrayed the continued terrorist threat to the country as high and describing the administration's aggressive response without "triggering a leak investigation or explaining on what authority he was making the disclosures." Human Rights Watch telephone interview with Philip Bennett, February 26, 2014.

[97] Human Rights Watch interview with Barton Gellman, February 10, 2014.

[98] Human Rights Watch interview with Barton Gellman, February 10, 2014.

[99] Human Rights Watch telephone interview with Peter Maass, senior writer at *The Intercept*, March 26, 2014.

[100] Human Rights Watch telephone interview with Charlie Savage, March 14, 2014.

Security Editor at the Washington Post, expressed concern that "the government's ability to find the source will only get better."[101]

A national security reporter made the link even clearer, stating that the Snowden revelations show that "[w]hat we're doing is not good enough. I used to think that the most careful people were not at risk, [that they] could protect sources and keep them from being known. Now we know that isn't the case."[102] He added, "That's what Snowden meant for me. There's a record of everywhere I've walked, everywhere I've been."[103] Peter Maass voiced a similar concern: "[The landscape] got worse significantly after the Snowden documents came into circulation. If you suspected the government had the capability to do mass surveillance, you found out it was certainly true."[104]

Journalists repeatedly told us that surveillance had made sources much more fearful of talking. The Snowden revelations have "brought home a sense of the staggering power of the government," magnifying the fear created by the increasing number of leak investigations.[105] Accordingly, sources are "afraid of the entire weight of the federal government coming down on them."[106] Jane Mayer, an award-winning staff writer for *The New Yorker*, noted, "[t]he added layer of fear makes it so much harder. I can't count the number of people afraid of the legal implications [of speaking to me]."[107] One journalist in Washington, DC, noted, "I think many sources assume I'm spied on. [I'm] not sure they're right but I can't do anything about their presumption."[108] As a result, she said, some remaining sources have started visiting her house to speak with her because they are too fearful to come to her office.[109] One national security reporter estimated that intelligence reporters have the most skittish sources, followed by journalists covering the Department of Justice and terrorism, followed by those on a military and national security beat.[110]

---

[101] Human Rights Watch interview with Peter Finn, December 17, 2013. Note that Finn spoke on his own behalf, and not for the Washington Post.

[102] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

[103] Ibid.

[104] Human Rights Watch telephone interview with Peter Maass, March 26, 2014.

[105] Human Rights Watch interview with Peter Finn, December 17, 2013.

[106] Human Rights Watch interview with Marisa Taylor, investigative reporter for *McClatchy Newspapers*, Washington DC, January 16, 2014.

[107] Human Rights Watch interview with Jane Mayer, staff writer for *The New Yorker*, Washington, DC, January 16, 2014.

[108] Human Rights Watch interview with a reporter in Washington, DC, (date withheld).

[109] Email from a reporter in Washington DC to Human Rights Watch, June 5, 2014.

[110] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

As a result, journalists report struggling to confirm even unclassified details for stories, and have seen trusted, long-standing sources pulling back. "I had a source whom I've known for years whom I wanted to talk to about a particular subject and this person said, 'It's not classified but I can't talk about it because if they find out they'll kill me' [figuratively speaking]."[111] Several others have reported the sudden disappearance of formerly reliable sources, or the reluctance of sources to discuss seemingly innocuous and unclassified matters.[112] One decorated intelligence and national security journalist indicated that even retired sources are increasingly reluctant to speak.[113] Though firing or revocation of security clearances no longer worries them, they fear prosecution, and "now [they] have to worry that their communications can be reached on a basis far short of probable cause."[114]

Though losing developed sources has proved frustrating to numerous journalists with whom we spoke, a number suggested that the largest challenge they face is reaching new sources. "Sources don't just materialize," noted Peter Finn. "They often are developed."[115] That requires building trust, which can be a slow and difficult process.

Adding to the challenge of developing sources that are already skittish is the fact that surveillance makes it very difficult for journalists to communicate with them securely. Calling or emailing can leave a trail between the journalist and the source; and it can be difficult to get casual contacts to take more elaborate security measures to communicate. "[H]ow do you even get going?" asked Bart Gellman, referring to the challenge of making first contact with a new would-be source without leaving a trace. "By the time you're both ready to talk about more delicate subjects, you've left such a trail that even if you start using burner phones or anonymous email accounts you're already linked."[116] A national security reporter noted, "[Ideally,] you bump into people. [That's] tough to arrange, though, without [creating a] record…. [You] find yourself using phone and email to set up a chance to talk. If that's completely forbidden, then we are really in trouble."[117] As a result,

---

[111] Human Rights Watch interview with Jonathan Landay, December 12, 2013.

[112] E.g., Human Rights Watch interviews with Steven Aftergood, Director, Federation of American Scientists' Project on Government Secrecy, Washington DC, December 11, 2013, and Peter Finn, December 17, 2013.

[113] Human Rights Watch interview with a journalist (name, location, and date withheld).

[114] Human Rights Watch interview with a journalist (name, location, and date withheld).

[115] Human Rights Watch interview with Peter Finn, December 17, 2013.

[116] Human Rights Watch interview with Barton Gellman, February 10, 2014.

[117] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

according to Peter Finn, "both parties want to move faster toward a more direct relationship that requires less electronic contact."[118]

Yet approaching sources in person from the outset can also be quite difficult. The time and effort required physically to locate specific sources can be prohibitive. Moreover, some sources simply do not want reporters to know their identities, so they "won't necessarily want to meet face to face initially."[119] That can push journalists back toward more conventional—and traceable—methods of making contact.[120] This sort of situation can leave reporters feeling "increasingly frustrated."[121]

A couple of journalists reported trying to make the best of a challenging situation. "In some ways, this environment creates a closer alliance with sources," observed Bart Gellman. "They're being treated as adversaries by people they work for. You use whatever you have."[122] Yet even the journalists who expressed these sorts of views did not regard such new opportunities as offsetting the growing challenges.[123] As a national security reporter summed up the matter, "We're not able to do our jobs if sources are in danger."[124]

Changing Journalistic Practices

In an attempt to protect their sources, their data, and themselves, many journalists reported modifying their practices—their tradecraft—for investigating stories, communicating with sources, and protecting their notes. The fact that journalists are profoundly altering their tradecraft is evidence of the impact of surveillance on their profession.

Yet significant uncertainty about which methods are effective, exacerbated by continued uncertainty about the scope and legal limits of US surveillance operations, leads to a variety of different approaches. Some journalists have changed their practices in response to specific tips they have received from government officials. "I was warned by someone at the Pentagon that it was easy to track my calls because I used the same number all the time,"

---

[118] Human Rights Watch interview with Peter Finn, December 17, 2013.

[119] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

[120] Ibid.

[121] Ibid.

[122] Human Rights Watch interview with Barton Gellman, February 10, 2014.

[123] E.g., Human Rights Watch telephone interview with Peter Maass, March 26, 2014.

[124] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

reported a national security journalist.[125] Now he uses burner phones.[126] Brian Ross relayed a different tip he received: Start all international calls with, "I'm a US citizen. Aren't you?"[127] (Ross' tip refers to a prohibition against the "targeting" of US citizens for surveillance under Section 702.)[128] Others develop their techniques with the support of security experts.[129] Still others are operating blindly—speculating as to what works and what does not. As one investigative reporter put it put it, "You don't know what you're up against; you just take the precautions you can."[130]

We found three broad types of changes in journalists' behavior, all aimed at obscuring parts of the reporting process: increasing use of advanced privacy-enhancing technology, decreasing reliance on electronic tools, and modified use of conventional methods of protecting information and sources. Journalists often employ a combination of measures from all three categories.

> "At that point, why have a computer at all?" he wondered. "You could just go to the store and buy an Olivetti typewriter."
> —Steve Coll

Advanced Privacy and Security Technology

A significant number of journalists reported using various forms of encryption software for their communications with sources or colleagues, including emails, chats, texts, and phone calls, though it is far from clear how effective these methods are in the long run.[131] While proper use of encryption can protect the contents of communications, it will not obscure the identity of the correspondents, or the fact that they are communicating. As a result, if the government were to collect metadata concerning emailing patterns (as it did until 2011), then even encrypting domestic emails would only offer partial protection.[132]

---

[125] Ibid.

[126] Ibid.

[127] Human Rights Watch interview with Brian Ross, February 11, 2014.

[128] "Procedures used by NSA to minimize data collection from US persons: Exhibit B – full document," *Guardian*, June 20, 2013, http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document (accessed July 11, 2014).

[129] Human Rights Watch interview with Barton Gellman, February 10, 2014.

[130] Human Rights Watch interview with an investigative reporter, Washington, DC, November 19, 2013.

[131] Human Rights Watch interviews with multiple journalists (names, locations, and dates withheld).

[132] By using encryption in combination with the software Tor, some journalists may be able to hide their communication patterns in a way that encryption alone does not.

Journalists also reported using special devices or software to encrypt and store data securely.[133] A couple endorsed the use of air-gapped computers—computers that never connect to the internet, or any unsecured network—for particularly sensitive material.[134] Steve Coll noted, however, that securing a computer to such a degree significantly limits its utility. "At that point, why have a computer at all?" he wondered. "You could just go to the store and buy an Olivetti typewriter."[135]

Some journalists—including a few working on particularly sensitive materials—declined to discuss their full range of security measures.[136] Another noted that he tries to mask his records of purchases of advanced technology.[137]

On the other hand, some journalists actively avoid encryption, or use it with reservations. One prominent concern is that encryption is not entirely secure.[138] One national security reporter asked, "Will it save you in the end? Isn't the NSA going to crack it, or get someone to give up the code?"[139] Steve Coll noted that he has been "interested in the debate about whether any encryption approach is effective."[140] According to some of the people he has looked to for information on the subject, the biggest worry is not that the NSA will find a way to crack encryption, but rather that one's electronic "hygiene" in using it must be "excellent."[141] In other words, one lapse in protecting encryption passphrases or hardware can provide others with direct access to sensitive data in unencrypted form. Bart Gellman noted similar challenges with Tor: "You forget to launch Tor once before logging onto the account, and you're linked to it."[142]

---

[133] Human Rights Watch interviews with multiple journalists (names, locations, and dates withheld).

[134] E.g., Human Rights Watch interviews with a national security reporter, January 14, 2014 and Steve Coll, February 14, 2014.

[135] Human Rights Watch interview with Steve Coll, February 14, 2014.

[136] Human Rights Watch interviews with Jonathan Landay, December 12, 2013; a national security reporter, Washington, DC, January 14, 2014; and Barton Gellman, February 10, 2014.

[137] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

[138] E.g., Human Rights Watch interview with Steven Aftergood, December 11, 2013.

[139] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

[140] Human Rights Watch interview with Steve Coll, February 14, 2014.

[141] Ibid.

[142] Human Rights Watch interview with Barton Gellman, February 10, 2014. See Section II, The Impact of Surveillance on Journalists, Footnote 132.

Another worry is that encrypting communications might only draw the government's attention.[143] The NSA's minimization procedures that have been made public allow its employees to seek permission from the Attorney General to retain encrypted communications even if they are purely domestic.[144] Scott Shane, an intelligence reporter for the *New York Times*, said that while he has used encryption in the past, he is "skeptical that it is a solution of significance."[145] He noted that encrypted email "wasn't even a speed bump" for prosecutors in some recent leak cases, "who even used that to suggest the source knew he was doing something wrong."[146] Shane was referring to the prosecutions of Thomas Drake. Drake was suspected of leaking information to a reporter about wasteful spending at the NSA, and in their case against him, prosecutors highlighted his use of encrypted email (Hushmail) to communicate with the reporter.[147]

Eric Schmitt, a Pulitzer Prize-winning reporter for the *New York Times* who covers terrorism and national security, had similar misgivings. He observed that while certain sources might be better off using encrypted email, and journalists have begun using it among themselves and with some of their sources, "if you ask … government sources to do it, it brands them."[148] Steve Aftergood suggested the same concern: "Maybe you're drawing more attention to yourself by using it, suggesting the contents are sensitive."[149]

Several journalists highlighted another significant difficulty: In many instances, for encryption to work, both the journalist and the source must have some facility with the same encryption tool. Some journalists expressed doubts about their own ability to master encryption and related technologies.[150] Others noted that many would-be sources

---

[143] E.g., Human Rights Watch interviews with an investigative journalist, Washington, DC, November 19, 2013, and a national security reporter, Washington, DC, January 14, 2014.

[144] Glenn Greenwald and James Ball, "The top secret rules that allow NSA to use US data without a warrant," *Guardian*, June 20, 2013, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant (accessed July 11, 2014).

[145] Human Rights Watch telephone interview with Scott Shane, intelligence reporter for the *New York Times*, April 2, 2014.

[146] Ibid.

[147] "Former NSA Senior Executive Charged with Illegally Retaining Classified Information, Obstructing Justice and Making False Statements," Department of Justice press release, April 15, 2010, http://www.justice.gov/opa/pr/2010/April/10-crm-416.html (accessed July 14, 2014). He was indicted in 2010 on charges related to espionage and obstructing the investigation against him, but after a costly trial, had all charges dropped in exchange for a guilty plea to a misdemeanor for exceeding authorized use of a computer.

[148] Human Rights Watch interview with Eric Schmitt, reporter for the *New York Times*, Washington, DC, January 28, 2014.

[149] Human Rights Watch Interview with Steven Aftergood, December 11, 2013.

[150] At the same time, a growing number of intelligence and national security journalists are posting PGP keys on their Twitter pages, signifying to potential sources that they possess some useful level of technological sophistication.

lack the technical savvy to approach journalists safely,[151] and even that using encrypted methods of communication with typical sources—as opposed to sources who already prefer to use encryption—might "spook" them. "They're going to feel like they're doing something wrong."[152] Jane Mayer added, "Your source has to be really committed [to bother with advanced security measures]."[153]

Most journalists who use advanced technologies indicated that their outlets are willing to cover the financial costs of doing so.[154] Those costs are not overwhelming on the whole; there are open source (free) versions of certain encryption software, such as PGP, while other programs require a manageable subscription fee, like Silent Circle.

However, the use of advanced technologies does impose costs beyond the financial. They can take time to learn, and are often difficult to use. Journalists we spoke with characterized them as "a burden,"[155] "a huge tax on your time,"[156] and "cumbersome and slow."[157] The perceived complexity of learning them imposes a barrier for some journalists.[158] While some outlets actively train select staff in the use of advanced technology,[159] others do not. Several journalists described teaching themselves new technologies on an ad hoc basis under their own initiative.[160]

Decreasing Reliance on Digital Technology

Both sources and journalists alike use a range of third-party service providers, including web-based email, social media services, or cloud-based storage. The revelations of the

---

[151] A couple of journalists flagged the development of secure drop boxes, which allow sources (with online instruction) to submit files to a news outlet without independently learning how to use encryption software. E.g., Human Rights Watch interview with Barton Gellman, February 10, 2014. See, e.g., *The New Yorker* Strongbox, accessed July 14, 2014, http://www.newyorker.com/strongbox/.

[152] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

[153] Human Rights Watch interview with Jane Mayer, January 16, 2014.

[154] Human Rights Watch interviews with Jonathan Landay, December 12, 2013; Peter Finn, December 17, 2013; a national security reporter, Washington, DC January 14, 2014; and Jane Mayer, Washington, DC, January 16, 2014; Human Rights Watch telephone interviews with a reporter who covers law enforcement and national security, February 4, 2014, and a journalist covering Afghanistan, March 18, 2014.

[155] Human Rights Watch interview with Steve Coll, February 14, 2014.

[156] Human Rights Watch interview with Barton Gellman, February 10, 2014.

[157] Human Rights Watch interview with Jane Mayer, January 16, 2014.

[158] Human Rights Watch interview with an investigative journalist for a major outlet, New York, January 23, 2014.

[159] One journalist described having his name on a list to be supplied with some advanced technology by his outlet. Human Rights Watch interview with Eric Schmitt, January 28, 2014.

[160] Human Rights Watch interview with an investigative reporter, Washington, DC, November 19, 2013.

PRISM program[161] brought into stark relief the privacy and security risks associated with using US-based online service providers, who are subject to orders under Section 702 and other national security authorities. The lack of certainty about how data stored by these companies is protected undermines their convenience and cost-effectiveness.

For all of the influence of advanced technologies on the evolution of journalistic tradecraft, many journalists indicated that creating no electronic record is best. Even those who have made significant use of advanced privacy-enhancing technology held this view.[162] As one national security reporter summed it up, "any form of electronic communication just can't be used for sensitive matters."[163] Accordingly, many journalists have ratcheted back their use of technology.

Many journalists reported a strong preference for meeting sources in person in large part for reasons of security.[164] "I don't think there's anything ironclad you can do except [meet] face to face," remarked Jonathan Landay.[165] "Maybe we need to get back to going to sources' houses," added Peter Finn.[166] Indeed, several journalists expressed a marked reluctance to contact certain sources by email or phone.[167] "[We] have to think about how to contact someone without leaving electronic cookies behind," observed Steve Engelberg.[168] "[You] can't call [sources] at work," noted a New York-based investigative journalist. If you have misgivings about using a source's cell phone or personal email, "[the] only thing that's left is to go to their door."[169]

The common view appears to be that meeting face to face with a source is better than calling, which in turn is better than emailing.[170] "Most assume emails can be intercepted or subpoenaed," noted Eric Schmitt. Fewer worried that the government will intercept their

---

[161] For more on the PRISM program, see Section I, Background: US Surveillance, Secrecy, and Crackdown on Leaks, Footnote 13.

[162] E.g., Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

[163] Ibid.

[164] E.g., Human Rights Watch interviews with Martin Knobbe, New York-based correspondent for *Stern Magazine*, New York, New York, January 13, 2014, and a reporter in Washington, DC (date withheld).

[165] Human Rights Watch interview with Jonathan Landay, December 12, 2013.

[166] Human Rights Watch interview with Peter Finn, December 17, 2013.

[167] E.g., Human Rights Watch interviews with a national security reporter, Washington, DC, January 14, 2014, and a New York-based investigative journalist, New York, March 24, 2014.

[168] Human Rights Watch interview with Stephen Engelberg, January 30, 2014.

[169] Human Rights Watch interview with a New York-based investigative journalist, New York, March 24, 2014.

[170] E.g., Human Rights Watch interview with a reporter, Washington, DC, December 17, 2013; Human Rights Watch telephone interview with Scott Shane, April 2, 2014.

domestic calls. "I doubt the NSA can get content of domestic calls without an active investigation," noted one national security reporter, who said he has heard as much from "good sources."[171] Peter Finn concurred: "I don't think they could listen routinely to journalists." (There have been no revelations of large-scale US government eavesdropping on purely domestic phone calls.)

Even so, when forced to call a source, a couple of journalists indicated a preference for using landlines over cell phones, noting how easily one can intercept the contents of a cell phone call.[172] "Almost anybody with the right equipment can eavesdrop on a cellphone call; landlines are more secure from snooping (though of course [the] government … can capture content with [a] wiretap)," observed Peter Maass.[173] Nevertheless, the US government continues to collect metadata information on landlines as well as cell phones, and as Maass noted, "The government doesn't need to know what people are talking about—just *that* they're talking. That can go a long way in supporting the prosecution's case in a leak investigation."[174]

Two journalists also indicated a growing affinity for using postal services to transmit documents rather than electronic means,[175] though a third expressed concern about media reports that the US Postal Service has been photographing all of the mail it handles.[176] Even suggesting that sources use conventional mail rather than other means to communicate can scare away sources, however. Peter Maass described being approached by a would-be source, and urging that person to mail him information rather than sending it electronically. He never heard from the person again, and Maass suspects the reason is that "I made him aware of the danger of being connected to me. As a result, I lost that story."[177]

Several journalists also suggested a preference for avoiding other technologies that create electronic trails or files. One trend is to use cash rather than credit cards when making

---

[171] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

[172] Human Rights Watch interview with Eric Schmitt, January 28, 2014; Human Rights Watch telephone interview with Peter Maass, March 26, 2014; email correspondence with Peter Maass, July 3, 2014.

[173] Human Rights Watch email correspondence with Peter Maass, July3, 2014.

[174] Human Rights Watch telephone interview with Peter Maass, March 26, 2014.

[175] Human Rights Watch interviews with Steven Aftergood, December 11, 2013, and Martin Knobbe, January 13, 2014.

[176] Human Rights Watch interview with an investigative journalist for a major outlet, New York, January 23, 2014. For background, see Ron Nixon, "U.S. Postal Service Logging All Mail for Law Enforcement," *New York Times,* July 3, 2013, http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html (accessed July 14, 2014).

[177] Human Rights Watch telephone interview with Peter Maass, March 26, 2014.

purchases that relate to one's reporting.[178] A couple of journalists also reported avoiding storing data in the cloud.[179] Steve Engelberg noted that he prefers to deal in hard copies and printouts—rather than electronic files—when working on drafts of stories related to national security.[180]

Other Strategies to Protect Sources

In addition to seeking security in a combination of more and less advanced technology, a number of journalists have adapted their use of conventional tools to make it more difficult to track down their sources through surveillance. One approach involves deliberately creating a misleading electronic trail. For example, one journalist described a colleague who calls a large number of possible sources before a story comes out in order to obscure the identities of those who actually provided information.[181] Another reported booking "fake" travel plans for places he never intended to visit.[182]

Journalists and sources have also made creative use of common technologies to hide their interactions. The most common such approach is to use "burner" phones—cell phones with limited identifiable links to the owner, and which one disposes of after a matter of days or weeks. A significant number of journalists described elaborate processes by which they managed to obtain such phones, limit their traceability, and make them operable for a short period.[183]

Others described a variety of similar techniques for sharing information with sources electronically while minimizing the trace left behind. Some detailed the inventive use of email accounts or phones, as well as tricks for hiding purchase records related to reporting activity.[184]

---

[178] E.g., Human Rights Watch interviews with Jonathan Landay, December 12, 2013, and a national security reporter, Washington, DC, January 14, 2014.

[179] Human Rights Watch interviews with an investigative journalist for a major outlet, New York, January 23, 2014, and Stephen Engelberg, January 30, 2014.

[180] Human Rights Watch interview with Stephen Engelberg, January 30, 2014.

[181] Human Rights Watch interview with an investigative reporter, Washington, DC, November 19, 2013.

[182] Human Rights Watch interview with Jonathan Landay, December 12, 2013.

[183] Human Rights Watch interviews with multiple journalists (names, locations, and dates withheld).

[184] Human Rights Watch telephone interview with a journalist covering immigration issues, February 4, 2014; Human Rights Watch interviews with an investigative reporter, Washington, DC, November 19, 2013; Scott Horton, January 13, 2014; and Jonathan Landay, December 12, 2013. Peter Maass described one such common practice from Russia dating back at least 10 years ago. During a visit to Russia around that time, Maass watched an acquaintance borrow a stranger's phone in a restaurant. The acquaintance wanted to make a sensitive call without having it traced back to him. When Maass asked him

Journalists also have made efforts to better protect their information. Due to the traceability of GPS information from cell phones, and the possibility of turning cell phones into listening devices (even if they are off),[185] several journalists reported turning off cell phones or taking out their phone batteries before speaking with people in person, or even leaving phones behind altogether when visiting sources.[186] One journalist reported keeping his files "on a flash drive in [his] pocket all the time," and taking additional precautions with his notes—such as writing them by hand and encoding them.[187] A couple of others have employed codes for discussing stories or sources, whether within an office or otherwise.[188]

The large variety and complexity of these strategies illustrate the fear that journalists and their sources hold of government surveillance. Even in cases where the topic of discussion is innocuous and declassified, journalists and their sources are unable to converse freely, stymying effective reporting. Many of these techniques entail additional costs for journalists— not just the financial costs of additional technology and equipment, but perhaps even more burdensome costs in the time it takes for journalists to go through all the elaborate steps they now need to take to keep their sources protected.

Ongoing Uncertainty about Security

Even with all these burdensome and costly measures, many journalists expressed doubts about their power to protect sources and the level of security they are able to attain.

A national security reporter observed, "[I'm under] no illusion that [my approach] is foolproof, but it's anything to protect [us] somewhat."[189] A number of journalists seemed to recognize that their evolving tradecraft countermeasures are extremely limited. Jonathan Landay noted that certain steps he is inclined to take "may not be very successful, but you

why the stranger would lend his phone so readily, the acquaintance replied, "We all do that now." Human Rights Watch telephone interview with Peter Maass, March 26, 2014.

[185] Liz Klimas, "Report: The FBI Can Remotely Turn on Phone Microphones for Spying," *The Blaze*, August 2, 2013, http://www.theblaze.com/stories/2013/08/02/report-fbi-can-remotely-turn-on-phone-microphones-for-spying/ (accessed July 14, 2014).

[186] E.g., Human Rights Watch interviews with an investigative reporter, Washington, DC, November 19, 2013, and an investigative journalist for a major outlet, New York, January 23, 2014.

[187] Human Rights Watch interview with Scott Horton, January 13, 2014.

[188] Human Rights Watch interviews with Brian Ross, February 11, 2014, and Jonathan Landay, December 12, 2013.

[189] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

do whatever you can think of."[190] Brian Ross was also skeptical of some of his steps, such as using codes within the office to discuss more sensitive matters. "We're not very good at it; we're not trained in cyphers and codes."[191]

Not a single journalist we spoke with believed they could defeat the most focused efforts by the government to discern their activities. "If the government wants to get you, they will," noted Adam Goldman, a Pulitzer Prize-winning reporter with the *Washington Post*. "We don't have the technology [that] they do," added Jonathan Landay.[192] While there are a number of steps one can take to limit exposure to large-scale electronic surveillance, observed Bart Gellman, "if a first-rate intelligence agency decides to target you specifically and invest serious resources, there's nothing you can do"[193] Accordingly, he described his tradecraft techniques as an attempt "to raise the cost of surveillance."[194]

Another prominent journalist wondered whether the US government might fill its intelligence gaps on US persons by acquiring information—including, potentially, on journalists—from friendly foreign governments.[195] Indeed, it is publicly known that the US has an intelligence sharing agreement with the UK, Canada, Australia, and New Zealand—a group of countries collectively called the "Five Eyes"[196]—and has worked closely with various other intelligence services.[197] As described in the next section, the US is known to have received intelligence about a US law firm's communications with its client from the Australian intelligence service.[198] One senior intelligence official we spoke with noted that the US government can accept (though not solicit) intelligence about US persons from other governments even where the US is not permitted to gather that intelligence itself.[199]

---

[190] Human Rights Watch interview with Jonathan Landay, December 12, 2013.

[191] Human Rights Watch interview with Brian Ross, February 11, 2014.

[192] Human Rights Watch interview with Jonathan Landay, December 12, 2013.

[193] Human Rights Watch interview with Barton Gellman, February 10, 2014.

[194] Ibid.

[195] Human Rights Watch interview with a journalist (name, location, and date withheld).

[196] Patrick Donahue and John Walcott, "U.S. Offered Berlin 'Five Eyes' Pact. Merkel Was Done With It," *Bloomberg*, July 12, 2014, http://www.bloomberg.com/news/2014-07-11/berlin-spying-prompted-u-s-offer-too-late-to-sway-merkel.html (accessed July 14, 2014).

[197] Maria McFarland Sanchez-Moreno, "What is the NSA Sharing with Other Countries?," *Al Jazeera America*, January 24, 2014, http://america.aljazeera.com/opinions/2014/1/what-is-the-nsa-sharingwithothercountrieso.html (accessed July 14, 2014).

[198] James Risen & Laura Poitras, "Spying by N.S.A. Ally Entangled U.S. Law Firm," *New York Times,* Feb. 15, 2014, http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0 (accessed July 14, 2014).

[199] For more on related statements by the same official, see Section IV, The Government's Rationale for Surveillance.

A national security reporter put it this way: "It's difficult, if you're using any electronic communications, to do something that DOJ with a subpoena or the NSA couldn't figure out. But you want to make the initial leak investigation more difficult to preclude a more sweeping inquiry."[200] For example, burner phones "won't thwart the NSA," he argued.[201] "They'll know [the phone is] always near [other phones linked to me.] But for sensitive calls, it'll hopefully thwart the initial leak investigation."[202] A Pulitzer Prize-winning reporter for a major newspaper agreed: "It's really hard to leave zero trail and do your job."[203]

Impact on News Coverage, Public Accountability, and the Quality of Democratic Debate

Increased surveillance, combined with the tightening of measures to prevent both leaks and (more broadly) government officials' contact with the media, may be having a profoundly detrimental impact on public discourse. There are good reasons to believe that recent developments are reducing the amount and quality of news coverage of matters of public concern. They are also affecting the role that journalists have typically played in holding government to account for its actions, particularly when it comes to the intelligence sector.

Impact on News Coverage

Several journalists we spoke with asserted that the new challenges they face significantly impede news coverage of matters of great public concern.[204] Many journalists emphasized the extra time entailed by the new techniques they're employing to protect their sources and communications.[205] "It's a tax on my time," noted Bart Gellman. "I could do double the work if I weren't spending so much effort on encryption and a secure workflow between networked and air-gapped machines."[206] Part of the delay results from using more advanced privacy and security technologies, which may involve trade-offs with convenience, and ensuring that sources do the same. Part of the delay also comes from the scaled back use of electronic communications or digital technology. "Mail is slow,"

---

[200] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

[201] Ibid.

[202] Ibid.

[203] Human Rights Watch interview with a reporter for a major newspaper, Washington, DC, December 17, 2013.

[204] E.g., Human Rights Watch interview with Jane Mayer, January 16, 2014.

[205] E.g., Human Rights Watch interviews with a reporter, Washington, DC, December 17, 2013, and Adam Goldman, reporter with the *Washington Post*, Washington, DC, January 28, 2014.

[206] Human Rights Watch interview with Barton Gellman, February 10, 2014

observed Martin Knobbe, a New York-based correspondent for Stern Magazine. "It can take two weeks to get an okay to meet someone [using mail]."[207] All things considered, "[i]t absolutely slows down coverage," claimed Marisa Taylor.[208]

"Stories that could have been done have a much higher uphill climb," observed Steve Engelberg.[209] With staff limitations, it is not always possible to undertake that climb simply because a story looks interesting or promising. "We have to pick our spots. It takes thought."[210] While the additional time that goes into stories can also yield more nuance, these extra challenges arise at an inopportune time. Print-centered news outlets have struggled over the last several years, and may have fewer resources than in the past.[211]

Additionally, many journalists said the amount of information provided or confirmed by sources is diminishing. For one, sources are becoming less candid over email and phone. "I definitely see a trend of sources speaking at a different level of candor face to face [as compared to over the phone]," noted a national security reporter.[212] As a result, he acknowledged spending more time physically near where his sources work.[213] Others also confirmed traveling more (and spending the money that goes with that), or facing the difficult choice of how to pursue information if travel is not an option.[214]

As one might expect, sources are less willing to discuss sensitive matters, even where it is not clearly classified. "[There is] much greater reluctance from sources to talk about sensitive stuff," asserted Scott Shane.[215] "There just isn't a bright line between classified and not…. There's a huge gray area. That's where the reporting takes place. [But s]ources are increasingly unwilling to enter that gray zone."[216]

---

[207] Human Rights Watch interview with Martin Knobbe, January 13, 2014.

[208] Human Rights Watch Interview with Marisa Taylor, January 16, 2014.

[209] Human Rights Watch interview with Stephen Engelberg, January 30, 2014.

[210] Ibid.

[211] Human Rights Watch interview with James Asher, December 12, 2013.

[212] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

[213] Ibid.

[214] Ibid. Human Rights Watch interviews with Jane Mayer, January 16, 2014; Martin Knobbe, January 13, 2014; and Eric Schmitt, January 28, 2014. Human Rights Watch telephone interview with a reporter who covers law enforcement and national security, February 4, 2014.

[215] Human Rights Watch telephone interview with Scott Shane, April 2, 2014.

[216] Ibid.

Yet the effect is still broader. As a Pulitzer Prize-winning reporter put it, "People are increasingly scared to talk about anything."[217] According to Jonathan Landay, source reluctance extends "even [to] something like, 'Please explain the rationale for this foreign policy.' That's not even dealing with classified material; that's just educating readers."[218] Landay added, "There's [also] a much greater constraint on the ability to get explanatory information about the views of people dealing with real issues before they get into the political levels of the government. That's not classified. That's not secret. At worst, that's embarrassing."[219] Jane Mayer put it differently. "What you're losing now is spontaneity."[220] As a result, we are "not getting spur-of-the-moment stories." She also emphasized the motives of many government sources: "Most of these leaks are just criticism, frankly. [My sources] are very patriotic on the whole…. They're not enemies of the state."[221]

> "Most of these leaks are just criticism, frankly. [My sources] are very patriotic on the whole…. They're not enemies of the state."
> — Jane Mayer

Bart Gellman put the size of the challenge into context: "I don't feel like there's a drought, but there are more challenges."[222] Steve Engelberg agreed, noting that the surveillance revelations have "added a layer of complexity" to national security reporting, but have not shut it down completely.[223]

The net result is a less informed public. It is "absolutely" the case that less information is reaching the American people, according to James Asher. Kathleen Carroll agreed. While she does not necessarily see a connection between leak investigations and surveillance, she also expressed concern over sources feeling especially skittish, noting that "People have to work harder, it takes longer, and you […] won't have as many stories [until the landscape changes]."[224]

---

[217] Human Rights Watch interview with a reporter, Washington, DC, December 17, 2013.
[218] Human Rights Watch interview with Jonathan Landay, December 12, 2013.
[219] Ibid.
[220] Human Rights Watch interview with Jane Mayer, January 16, 2014.
[221] Human Rights Watch interview with Jane Mayer, January 16, 2014
[222] Human Rights Watch interview with Barton Gellman, February 10, 2014.
[223] Human Rights Watch interview with Stephen Engelberg, January 30, 2014.
[224] Human Rights Watch interview with Kathleen Carroll, May 8, 2014.

Impact on the Press's Ability to Serve as a Check on Government Abuse

In recent decades, the press has played an important role in checking government, and in particular, the intelligence community.[225] That has not always been the case. Betty Medsger, a former *Washington Post* reporter whose series of stories in 1971 first revealed the FBI's targeting of dissenters, recalled that there was "very little investigative work" before her articles appeared.[226] Even her FBI stories derived from documents stolen by activists, rather than through Medsger's cultivation of sources inside the intelligence community. "I was given these files. I didn't have clever techniques. Nobody was trying to develop inside sources until then."[227]

Tim Weiner, a Pulitzer Prize-winning reporter for the *New York Times*, who also won a National Book Award for his history of the CIA, offered an earlier timeline for the development of investigative journalism on the intelligence community, observing that "serious investigative reporting into the CIA started in the mid-1960's, and then seriously expanded a decade later."[228] Phil Bennett elaborated:

> The growth of the intelligence community and of a more critical, more adversarial press occurred in tandem, on overlapping timelines. Although there have been state secrets since the founding of the Republic, the current institutional structure that manufactures and protects those secrets emerged near the end of World War II and the beginning of the Cold War. For the most part, at first journalists did little to contest the government's monopoly on secrets. But the Vietnam War led some journalists to see secrecy as a tool for the government to deceive the public. The Pentagon Papers case ratified this view. Disclosing government secrets then became a central part of the birth of modern investigative reporting. This has carried over to the digital era.[229]

---

[225] Human Rights Watch email correspondence with Tim Weiner, July 2, 2014.

[226] Human Rights Watch interview with Betty Medsger, former *Washington Post* reporter, New York, New York, January 24, 2014.

[227] Ibid.

[228] Human Rights Watch email correspondence with Tim Weiner, July 10, 2014. Weiner has written several books, including *Legacy of Ashes: The History of the CIA*, (New York: Anchor Books, 2008).

[229] Human Rights Watch email correspondence with Phil Bennett, July 10, 2014.

Ultimately, the government's own investigations into the intelligence community in the mid-1970s—most famously among them, the Church Committee in the Senate—provided a sound basis for ongoing and active investigative work by journalists on the intelligence community ever since.[230] Those inquiries revealed significant and widespread misconduct by the intelligence community dating back decades. By offering the public significant and early insight into objectionable practices by the FBI, Medsger's stories formed a major part of the environment that gave rise to those investigations,[231] complementing pressure resulting from the Vietnam War and Seymour Hersh's 1974 reporting on the CIA.[232]

> "This is not a bunch of bratty journalists trying to undermine legitimate government operations."
> — Kathleen Carroll

But coverage of the intelligence community has recently (once again) become more challenging to undertake. "It seems to me that at some point it became very difficult again to cover these institutions and get inside sources," Medsger observed.[233]

Many journalists who spoke to us expressed a strong commitment to their work, and were unwilling to be dissuaded from continued efforts to cover increasingly difficult beats. "I'm not in any way going to stop reporting," remarked Adam Goldman. "In most cases, I am not the vulnerable one," added Steve Aftergood.[234] Peter Maass also identified a silver lining: "Even though it's harder, it's also very exciting. We're being given an amazing opportunity to do exciting work that could help shape society for years to come."[235]

Nevertheless, the effects that surveillance and leak investigations have had on coverage are working to undermine effective democratic participation and governance.

---

[230] Medsger's stories appeared in 1971, the Watergate scandal occurred in 1972, Seymour Hersh published some major revelations about the CIA's activities in 1974, and in 1975, both the executive and the legislative branches launched investigations into the intelligence community. For more on the chronology of these events, see G. Alex Sinha, "NSA Surveillance Since 9/11 and the Human Right to Privacy," *Loyola Law Review*, vol. 59 (2013), pp. 871-873. For more on the story behind Medsger's reporting, see Betty Medsger, *The Burglary: The Discovery of J. Edgar Hoover's Secret FBI*, (New York: Alfred A. Knopf, 2014).

[231] Human Rights Watch interview with Betty Medsger, January 24, 2014.

[232] Human Rights Watch email correspondence with Tim Weiner, July 2, 2014.

[233] Human Rights Watch interview with Betty Medsger, January 24, 2014.

[234] Human Rights Watch Interview with Steven Aftergood, December 11, 2013.

[235] Human Rights Watch telephone interview with Peter Maass, March 26, 2014.

"What makes government better is our work exposing information," argued Dana Priest, a Pulitzer Prize-winning national security reporter at the *Washington Post*.[236] "It's not just that it's harder for me to do my job, though it is. It also makes the country less safe. Institutions work less well, and it increases the risk of corruption. Secrecy works against all of us."[237] Charlie Savage added, "National security journalism is especially important for a functioning, democratically accountable system."[238] Steve Coll agreed as well, noting, "There's a real loss to the public, the voters."[239]

> "…[a]s an American reporter, I should not be uneasy about the government targeting me to figure out my sources."
> — Scott Shane

For James Asher, "The role of the press is to be challenging and critical."[240] It is thus inherently important for journalists to seek out certain information that the government treats as sensitive and, when appropriate, share it with the public. Kathleen Carroll also emphasized the responsibility typically demonstrated by journalists who work on national security topics. "This is not a bunch of bratty journalists trying to undermine legitimate government operations," she argued. Moreover, though she believes "that a government's actions on behalf of the people it serves should be public, [m]ost news organizations [including her outlet, the Associated Press] will recognize that certain things the government is doing need to remain secret, at least for now. The disputes take place because the government idea of what should remain secret is much more sweeping."[241]

Dana Priest defined the problem as follows:

> The government is getting the balance between guarding information and making it public wrong. They think anything classified should stay secret…. The question for me is what really needs to stay secret. The rules for that were set for the nuclear era. We have a new era now with old rules. The government should reverse it, and start by asking, 'What needs to be secret?'[242]

---

[236] Human Rights Watch interview with Dana Priest, national security reporter at the *Washington Post*, Washington, DC, December 17, 2013.
[237] Ibid.
[238] Ibid.
[239] Human Rights Watch interview with Steve Coll, February 14, 2014.
[240] Human Rights Watch interview with James Asher, December 12, 2013.
[241] Human Rights Watch interview with Kathleen Carroll, May 8, 2014.
[242] Human Rights Watch interview with Dana Priest, December 17, 2013.

A couple of journalists also expressed principled resistance to the prospect of undertaking so many evasive maneuvers to do their work. Scott Shane argued that "[a]s an American reporter, I should not be uneasy about the government targeting me to figure out my sources."[243] Another reporter, who covers law enforcement and national security, noted that the need for additional secrecy has forced him to "start to act like a criminal."[244] Brian Ross articulated a similar sentiment: "There's something about using elaborate evasion and security techniques that's offensive to me—that I should have to operate as like a criminal, like a spy."[245] Adam Goldman, though he was less inclined to connect surveillance and leak investigations, also shared that view: "I don't want the government to force me to act like a spy. I'm not a spy; I'm a journalist."[246] He added, "What are we supposed to do? Use multiple burners? No email? Dead drops? I don't want to do my job that way. You can't be a journalist and do your job that way."[247]

"I don't want the government to force me to act like a spy. I'm not a spy; I'm a journalist… What are we supposed to do? Use multiple burners? No email? Dead drops? I don't want to do my job that way. You can't be a journalist and do your job that way."
— Adam Goldman

Certain statements by government officials have, indeed, suggested that journalists who report leaked information are engaged in criminal behavior. In January of 2014, Director of National Intelligence James Clapper called on "[Snowden] and his accomplices to facilitate the return of the remaining stolen documents that have not yet been exposed…."[248] As Snowden is not known to have had the assistance of others in obtaining the documents he later provided to the media, many interpreted that comment to refer to the reporters who had published stories based on the documents.[249]

---

[243] Human Rights Watch telephone interview with Scott Shane, April 2, 2014.

[244] Human Rights Watch telephone interview with a reporter who covers law enforcement and national security, February 4, 2014.

[245] Human Rights Watch interview with Brian Ross, February 11, 2014.

[246] Human Rights Watch interview with Adam Goldman, January 28, 2014.

[247] Ibid.

[248] Hadas Gold, "Clapper refers to Snowden 'accomplices'," *Politico*, January 29, 2014, http://www.politico.com/blogs/media/2014/01/clapper-alludes-to-snowden-accomplices-182264.html (accessed July 14, 2014).

[249] Ibid.

Republican Representative Mike Rogers made another such remark only days later.[250] Rogers, Chairman of the House's Permanent Select Committee on Intelligence (the primary House body tasked with oversight of the intelligence community), criticized journalist Glenn Greenwald for working with news outlets that paid for stories based on the Snowden documents.[251] Rogers accused Greenwald of "selling his access to information," specifically "[f]or personal gain." He concluded, "A thief selling stolen information is a thief."

One former government official we interviewed made a similar comparison between leakers and burglars (though without directly criticizing journalists who receive and publish leaked information).[252] Scott Shane responded to that analogy at some length:

> Informing Americans about the national security programs that they pay for and are carried out in their name is impossible without government officials who are willing to speak with reporters about them, within limits. The hard part, of course, is judging the proper limits. To compare the exchange of information about sensitive programs between officials and the media, which has gone on for decades, to burglary seems to miss the point. Burglary is not part of a larger set of activities protected by the Constitution, and at the heart of our democracy. Unfortunately, that mindset is sort of the problem.[253]

Several journalists likened the current reporting atmosphere to what one might find in more authoritarian countries. Peter Maass noted that he has worked under threat of surveillance abroad while covering the Soviet Union, the Balkans, and North Korea, and has thus been exposed to the need for evasion in reporting.[254] But he is "horrified and outraged" that the same concerns now apply here in the US.[255] Jonathan Landay reported that a number of his sources for a story in Jordan were called in for questioning after they spoke with him. "But I expect that to happen in

---

[250] Josh Gerstein, "Intelligence chairman accuses Glenn Greenwald of illegally selling stolen material," *Politico*, February 4, 2014, http://www.politico.com/story/2014/02/intelligence-chairman-argues-selling-snowden-docs-a-crime-103100.html (accessed July 14, 2014).

[251] Ibid.

[252] For more on this comparison, see Section IV, The Government's Rationale for Surveillance.

[253] Human Rights Watch telephone interview with Scott Shane, April 2, 2014.

[254] Human Rights Watch telephone interview with Peter Maass, March 26, 2014.

[255] Ibid.

Jordan."[256] A national security reporter noted that the US government now causes him more concern than other governments that we expect to do surveillance. "A year ago, in our line of business, we were more worried about the Chinese government snooping to get an edge by collecting what we weren't reporting. Now it's a distant second to our own government."[257]

[256] Human Rights Watch interview with Jonathan Landay, December 12, 2013.

[257] Human Rights Watch interview with a national security reporter, Washington, DC, January 14, 2014.

III. The Impact of Surveillance on Lawyers and Their Clients

> I found it shocking to think that the US is doing this [surveillance]—and I was at DOJ before.
> —A lawyer specializing in international dispute resolution at an international firm, April 1, 2014

Recent media reports confirm that large-scale electronic surveillance by the US government has been sweeping up vast amounts of private data and communications. That includes confidential information related to ongoing legal matters, and privileged communications between attorneys and their clients. Duty-bound to protect that information, and strategically disadvantaged if unable to do so, many attorneys describe surveillance as undermining their ability to advocate on behalf of their clients.[258]

At the most general level, as described by Maureen Franco, the federal public defender for the west district of Texas, "The Snowden stories confirm widely held suspicions and make us more nervous about using electronic communications."[259] Worries about surveillance vary from one area of legal practice to another, but they are particularly pronounced among attorneys who defend clients from charges related to terrorism—including federal defenders who are assigned to such cases rather than choosing them. Yet attorneys in other areas expressed significant concern as well, including defense attorneys who handle drug cases, and even attorneys doing international or civil work. Specifically, lawyers expressed concern over their ability to satisfy their professional duty of confidentiality, maintain their attorney-client relationships, and effectively represent their clients.

---

[258] Much information related to ongoing legal matters is confidential in the sense that attorneys must not reveal it without the client's informed consent. This includes communications between attorneys and clients, the reasoning behind strategic decisions made pertaining to the case, and information an attorney learns about his client during the representation. The attorney-client privilege is narrower than the duty of confidentiality; it applies to specific sorts of communications, especially (but not exclusively) between attorneys and their clients. The privilege manifests itself primarily as a rule of evidence: privileged communications cannot be introduced in legal proceedings without the client's consent. Respect for client confidentiality and the attorney-client privilege enables clients to trust their attorneys and facilitates open communication.

[259] Human Rights Watch telephone interview with Maureen Franco, federal public defender for the west district of Texas, March 14, 2014.

Like journalists, attorneys are uncertain about whether it is even possible to protect their communications from government surveillance, and are confused about what steps they can—and may even be obligated—to take. The result is a less robust relationship between some attorneys and their clients, and a legitimate concern about the impact on due process rights in the criminal context.

Uncertainty and Confusion among Lawyers over How to Respond to Large-Scale US Surveillance

The legal community, perhaps even more so than the media, is plagued by uncertainty and confusion over the implications for their work of surveillance of the scope revealed during the last year. Part of that uncertainty derives from the widespread sense that we have yet to learn the full extent of the government's surveillance powers, and what steps the intelligence community is taking to avoid scooping up attorney-client communications.[260] Part may also reflect the unsettled legal landscape regarding whether attorneys who are surveilled have legal recourse.[261]

The US government has stated that it applies certain minimization procedures to protect attorney-client communications.[262] Indeed, some of those procedures—which appear to limit NSA monitoring of communications under Section 702, if they are between someone under indictment in the US and their lawyer—were made public in June 2013 as part of one of the earliest *Guardian* stories based on the Snowden documents.[263]

---

[260] As one American Bar Association (ABA) publication put it, "[G]iven the secretive nature of the NSA, as well as the United States Foreign Intelligence Surveillance Court that oversees its surveillance warrants, lawyers can't even be sure of what is and what is not legal." Victor Li, ABA Journal, "Tools for lawyers worried that NSA is eavesdropping on their confidential conversations," March 30, 2014, http://www.abajournal.com/news/article/tools_for_lawyers_worried_that_nsa_is_eavesdropping_on_their_confidential_c/?utm_source=maestro&utm_medium=email&utm_campaign=tech_monthly (accessed July 14, 2014).

[261] In 2013, in a case that predated the Snowden revelations, the Supreme Court denied standing to people who felt obliged to change their practices to guard against surveillance undertaken pursuant to one specific legal authority, Section 702, because they could not demonstrate that their communications had actually been collected. For that ruling and its rationale, see generally *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138 (2013). New challenges are underway based on the Snowden revelations and related acknowledgments of surveillance by the government.

[262] Letter from NSA Director General Keith Alexander to ABA President James Silkenat, March 10, 2014, http://www.americanbar.org/content/dam/aba/images/abanews/nsa_response_03102014.pdf (accessed July 14, 2014).

[263] "Procedures used by NSA to minimize data collection from US persons: Exhibit B – full document," *Guardian*, June 20, 2014, http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document (accessed July 14, 2014), pp. 4-5.

But it is far from clear whether analogous procedures exist that apply to US surveillance under other authorities. Moreover, these procedures are little comfort to the many lawyers who represent individuals or companies not now under criminal indictment in the United States.[264] Indeed, in February 2014, new documents revealed that the communications of US-based law firm Mayer Brown with its client, the government of Indonesia, came under surveillance by an Australian intelligence agency, which in turn provided resulting intelligence to the United States.

The report prompted a letter from James R. Silkenat, president of the American Bar Association, to the NSA, expressing concern about reports of surveillance intruding on the attorney-client relationship.[265] Then-NSA Director General Keith Alexander responded, essentially restating public information concerning the NSA's rules.[266] For example, Alexander noted that the NSA stops monitoring communications when they are discovered to be between someone "known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment" (though it keeps the portion of the exchange it has already gathered).[267] The NSA also seeks individualized review by the Office of General Counsel before disseminating to other agencies or offices "information constituting U.S. person privileged communications [such as those that arise between a person and his attorney]."[268]

A number of lawyers indicated that it is difficult to know what to make of the current landscape, and they are only beginning to confront the implications of large-scale electronic surveillance for their work. In reflecting about the risks posed by surveillance, Tom Durkin, a leading national security defense attorney, began to express worries about

---

[264] Nicolas Niarchos, "Has the NSA Wiretapping Violated Attorney-Client Privilege?," *The Nation,* February 4, 2014, http://www.thenation.com/article/178225/has-nsa-wiretapping-violated-attorney-client-privilege (accessed July 14, 2014).

[265] Letter from ABA President James Silkenat to NSA Director General Keith Alexander and NSA General Counsel Rajesh De, February 20, 2014, http://www.americanbar.org/content/dam/aba/uncategorized/GAO/2014feb20_privilegedinformation_l.authcheckdam.pdf (accessed July 14, 2014).

[266] Letter from NSA Director General Keith Alexander to ABA President James Silkenat, March 10, 2014, http://www.americanbar.org/content/dam/aba/images/abanews/nsa_response_03102014.pdf. The ABA acknowledged General Alexander's response in a short public statement. American Bar Association, "ABA president responds to NSA letter regarding attorney-client privilege," March 11, 2014, http://www.americanbar.org/news/abanews/aba-news-archives/2014/03/aba_president_respon.html (accessed July 14, 2014).

[267] Letter from NSA Director General Keith Alexander to ABA President James Silkenat, March 10, 2014, http://www.americanbar.org/content/dam/aba/images/abanews/nsa_response_03102014.pdf, p. 3.

[268] Ibid., 2.

his metadata records for the first time during an interview with us: "I never thought about whether I wanted to leave a metadata trail until" he gave it some consideration at that moment.[269] He argued that it is too soon to comprehend the full range of implications of the Snowden revelations for the practice of law.[270] On the other hand, another litigator, who runs a private practice representing international clients, noted how significant the revelations have been for him: "I think everyone is starting to think about this."[271] It takes time, however, because "we're used to a world with sacrosanct communications between lawyers and clients."[272]

Many attorneys were very concerned about surveillance, even if not necessarily up to date on recent developments. The following remarks are indicative of this anxiety. A federal defender who has been working on a terrorism matter noted: "I get the sense that once you represent someone accused of terror-related charges, someone in the government is always going to be interested."[273] The defender added, "Everyone kind of jokes uncomfortably about it, particularly with the NSA stuff that's been coming out."[274] Linda Moreno, a defense attorney specializing in national security and terrorism cases, cited reports from "former CIA and FBI consultants" as the basis for part of her concern: "In their collection of metadata, I've been informed that the NSA filters for trigger words [like 'Osama bin Laden,' 'jihad,' and 'Islam']. In my law practice, those are words used in my discussions with colleagues, experts, and potential witnesses."[275]

A significant number of the lawyers who spoke with Human Rights Watch expressed worries about surveillance by the US government. Overall, criminal defense attorneys appear to be the most anxious. Much like journalists, they serve a crucial role in a democratic society, and one that is singled out for its importance in the US Constitution.[276]

---

[269] Human Rights Watch telephone interview with Tom Durkin, national security defense attorney, March 6, 2014.

[270] Ibid.

[271] Human Rights Watch telephone interview with a litigator with a private practice representing international clients, April 7, 2014.

[272] Ibid.

[273] Human Rights Watch telephone interview with a federal defender handling a terrorism case, April 3, 2014.

[274] Ibid.

[275] Human Rights Watch telephone interview with Linda Moreno, defense attorney specializing in national security and terrorism cases, March 12 and in-person interview, New York, New York, March 20, 2014.

[276] One group of criminal defense attorneys operates under especially difficult circumstances in this respect. Attorneys defending detainees held at Guantanamo Bay, Cuba, have faced extreme difficulty in trying to protect the confidentiality of communications with their clients. All phones at the military base at Guantanamo are subject to surveillance; in February 2013 defense attorneys discovered listening devices disguised as smoke detectors in attorney client meeting rooms; all meetings with clients are monitored with cameras; in late January 2013, during a different Guantanamo hearing, the judge

Interestingly, despite reports that Mayer Brown, a major corporate law firm, has had some of its confidential client information collected through surveillance by an NSA ally, concerns about surveillance did not appear as pronounced among the corporate lawyers with whom we spoke. One factor behind the disparity appears to be that large firms have been concerned about surveillance by other governments for a long time, and have had the financial resources to develop systems for protecting their information. For example, one information security officer at a major international firm indicated that the threat of large-scale electronic surveillance by the US government does not trigger any special security measure the firm does not already take to protect against other governments or independent hackers.[277] A partner in the litigation department at another large firm reported the same thing.[278] As indicated below, however, concerns about large-scale electronic surveillance have started to work their way into practice areas handled by some corporate firms, such as international arbitration.

More broadly, a number of legal organizations have begun to wrestle with questions surrounding the impact of surveillance on attorneys. These include the American Bar Association (ABA),[279] the New York City Bar Association,[280] the National Association of

---

learned that some unknown government agency was monitoring the courtroom feed and could pick up conversations, even at a whisper, between attorneys and their clients at defense tables; and in mid-April last year, an enormous number of prosecution and defense files disappeared from the server that both legal teams are required to use to process the highly classified documents in the case. Human Rights Watch telephone interview with Michael Schwartz, Air Force JAG who does work before the Guantanamo commissions, March 11, 2014; Laura Pitter, "Listening In," *Foreign Policy*, February 21, 2013, http://www.foreignpolicy.com/articles/2013/02/20/listening_in_guantanamo (accessed July 16, 2014); Jane Sutton, "Vanishing files delay Guantanamo hearings in 9/11 case," Reuters, April 17, 2013, http://www.reuters.com/article/2013/04/17/us-usa-guantanamo-delay-idUSBRE93GoYT20130417 (accessed July 16, 2014). As a result of these and other obstacles to protecting attorney client confidences, Guantanamo attorneys had been forced to modify their practices independently of concerns about large-scale electronic surveillance. It is all the more striking that some of these attorneys have felt the need to modify their practices even further in light of the Snowden revelations. E.g., Human Rights Watch telephone interviews with James Connell III, defense attorney for one of the Guantanamo detainees, March 18, 2014, and Jason Wright, Army JAG who does work before the Guantanamo commissions, March 31, 2014.

[277] Human Rights Watch email correspondence with an information security officer at a major international law firm based in Los Angeles, California, April 8, 2014.

[278] Human Rights Watch telephone interview with a partner in the litigation department of a large firm, March 25, 2014.

[279] The ABA Journal published an article on the tools available to lawyers to protect against surveillance. Victor Li, "Tools for lawyers worried that NSA is eavesdropping on their confidential conversations," http://www.abajournal.com/news/article/tools_for_lawyers_worried_that_nsa_is_eavesdropping_on_their_confidential_c/?utm_source=maestro&utm_medium=email&utm_campaign=tech_monthly. The ABA Litigation Journal also designated an entire issue to questions of surveillance. See generally ABA Litigation Journal, Spring 2014 issue, available at http://www.americanbar.org/publications/litigation_journal/2013-14/spring.html (accessed July 14, 2014).

[280] Brief for Association of the Bar of the City of New York as Amici Curiae Supporting Plaintiffs-Appellants, *ACLU v. Clapper*, Case No. 13 Civ. 3994 (WHP) (Mar. 13, 2014), https://www.aclu.org/sites/default/files/assets/clapper-ca2-bar-of-city-of-ny-amicus.pdf (accessed July 14, 2014).

Criminal Defense Lawyers (NACDL),[281] and the National Lawyers Guild.[282] Nevertheless, as described further below, they have yet to reach a consensus around the precise implications of surveillance for lawyers' professional responsibilities—and this lack of consensus highlights broader uncertainty.[283]

The Implications of Surveillance for the Professional Responsibilities of Lawyers

Lawyers practicing in the United States operate in a heavily regulated environment. They must comply with various rules of professional responsibility or risk penalties that can include suspension or even the loss of their license to practice law. Those rules generally include the obligation to maintain the confidentiality of information related to the representation of their clients, which attorneys regard as a core value of their profession.[284] Increasing surveillance by the US government introduces a serious ethical problem for attorneys, who are often professionally obligated to protect the contents of their communications, the nature of their legal research, and even the fact that they are communicating with a particular person or traveling to a particular place.[285]

For example, the American Bar Association maintains a set of Model Rules of Professional Conduct (Model Rules)—carefully sculpted guidelines that form influential, baseline standards for various jurisdictions that admit and regulate lawyers. The Model Rules stipulate that attorneys "shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[286] While lawyers have long been expected not to disclose

---

[281] The NACDL has held webinars on legal issues related to the introduction of surveillance information as evidence in criminal prosecutions. NACDL, "NACDL Hosts Educational Webinars on NSA and FISA," November 25, 2013, http://www.nacdl.org/enewsissue.aspx?fid=48707 (accessed July 14, 2014).

[282] The National Lawyers Guild put out a report in the spring of 2014 on its long history with government surveillance, and the effects of surveillance on the legal profession. Traci Yoder, National Lawyers Guild, "Breach of Privilege: Spying on Lawyers in the United States," April 2014, https://www.nlg.org/resource/reports/breach-privilege-spying-lawyers-united-states (accessed July 14, 2014).

[283] For more on the professional responsibilities of lawyers operating under the threat of surveillance, see The Implications of Surveillance for the Professional Responsibilities of Lawyers, Section III.

[284] Human Rights Watch interview with Stephen Gillers, Elihu Root Professor of Law at NYU School of Law, New York, New York, April 7, 2014; Human Rights Watch telephone interview with Ron Kuby, criminal defense and civil rights lawyer, March 7, 2014.

[285] Affirmation of Professor Stephen Gillers, *Ctr. for Constitutional Rights v. Bush*, Case No. 06-cv-313 (June 30, 2006), https://www.eff.org/document/gillers-affirmation (accessed July 14, 2014).

[286] American Bar Association Model Rules, Rule 1.6(c): Confidentiality of Information, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html (accessed July 14, 2014).

confidential client information without consent, the ABA modified the language of the applicable rule in 2012 to impose an explicit obligation on attorneys to take *positive steps* to protect the confidentiality of information concerning their clients and cases.[287]

According to Andrew Perlman, a professor at Suffolk University Law School who served as chief reporter of the ABA's Commission on Ethics 20/20 and directs Suffolk's Institute on Law Practice Technology and Innovation, the rule change followed general concerns about cybersecurity.[288] Perlman noted, however, that the wording of the rule is open-ended because the nature of security threats is constantly evolving. The obligation to protect client information applies across the board, and large-scale electronic surveillance can trigger the rule.[289]

"My take is that lawyers—especially those with clients whose legal matters may be of interest to the government—have legitimate concerns about government surveillance," Perlman noted.[290] Those concerns, he added, are especially pronounced for attorneys dealing with clients located outside the United States.[291] Stephen Gillers, Elihu Root Professor of Law at NYU School of Law, and a widely recognized expert on legal ethics, agreed. As early as 2007, Gillers argued that mere knowledge that the government could collect and apparently was collecting Americans' international communications without a specific warrant, and without meeting the conventional criminal standard of probable cause, was enough to preclude certain lawyers working on terror defense cases from using email, fax, and phone communications with people abroad.[292]

Yet, according to Gillers, "Obligations are [even] stronger on lawyers now [since the Snowden revelations]."[293] Since 2007, the public has learned more about the enormous power of the US government's surveillance apparatus and some media reports have made clear that the US government has collected at least some confidential legal information. For example, in February 2014, reports surfaced that the government had—under FISA

---

[287] American Bar Association, "August 2012 Amendments to ABA Model Rules of Professional Conduct," http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_house_action_compilation_redline_105a-f.authcheckdam.pdf (accessed July 14, 2014), pp. 5-7.

[288] Human Rights Watch telephone interview with Andrew Perlman, Professor at Suffolk University Law School, March 14, 2014.

[289] Ibid. See also Affirmation of Professor Stephen Gillers, *Center for Constitutional Rights v. Bush*, Case No. 06-cv-313 (June 30, 2006).

[290] Human Rights Watch telephone interview with Andrew Perlman, March 14, 2014.

[291] Ibid.

[292] Affirmation of Professor Stephen Gillers, *Center for Constitutional Rights v. Bush*, Case No. 06-cv-313 (June 30, 2006), paras. 3, 8.

[293] Human Rights Watch interview with Stephen Gillers, April 7, 2014.

Court orders—wiretapped defense attorneys representing individuals accused of terrorism charges.[294] Even though the communications were privileged, the narrow minimization rules did not apply, so the government was able to listen to the recordings of the calls.[295] The same month, as noted above, another report based on a document provided by Edward Snowden revealed that a US-based corporate law firm, Mayer Brown, "was monitored while representing [the Indonesian] government in trade disputes with the United States."[296] More specifically, the Australian Signals Directorate, the Australian analog for the NSA, surveilled communications between the Indonesians and their American lawyers, and then offered to share what it had collected with the NSA.[297]

Perlman emphasized that the new rule lays out a "reasonableness test";[298] and the commentary elaborating on the ABA rule identifies several factors that lawyers must weigh in discerning the measures they are reasonably expected to undertake to protect their communications.[299] Those factors include (but are not limited to):

> the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[300]

Attorneys handling certain types of cases—such as those representing defendants in terrorism-related cases, foreign sovereigns, or major corporations whose business has significant implications for US economic interests—have legitimate reason for thinking the government may be especially interested in their communications. The risk of the collection and review of confidential case information by US government agents appears

---

[294] Niarchos, "Has the NSA Wiretapping Violated Attorney-Client Privilege?" *The Nation,* http://www.thenation.com/article/178225/has-nsa-wiretapping-violated-attorney-client-privilege.

[295] Ibid.

[296] James Risen and Laura Poitras, "Spying by N.S.A. Ally Entangled U.S. Law Firm," *New York Times,* February 15, 2014, http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0 (accessed July 14, 2014).

[297] Ibid.

[298] Human Rights Watch telephone interview with Andrew Perlman, March 14, 2014.

[299] American Bar Association, "August 2012 Amendments to ABA Model Rules of Professional Conduct," http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_house_action_compilation_redline_105a-f.authcheckdam.pdf (accessed July 14, 2014), p. 7.

[300] Ibid.

higher when handling such matters, imposing on them heightened professional responsibilities.

Attorneys handling cases that would seem to be of little interest to the government have a reason to be concerned as well, however, as they still must avoid needlessly exposing confidential information to unauthorized parties. "Even if you aren't doing sensitive work, you should be concerned about how much [information] is gathered," said Jonathan Hafetz, an associate professor of law at Seton Hall University School of Law.[301] With the US government acquiring and retaining so much electronic data, many ways of communicating or storing information that would have been acceptable in the past are now known to be insufficient to preserve confidentiality.

One of the major concerns attorneys expressed to us relates to the scope of their professional responsibilities under the current surveillance regime.[302] As a result of recent surveillance revelations, a couple of attorneys reported feeling duty-bound to warn their clients that information related to their case may not remain private. Linda Moreno noted, "Given the now publicly admitted revelations that there is no privacy in communications, including those between attorneys and their clients, I feel ethically obligated to tell all clients that I can't guarantee anything [they] say is privileged … or will remain confidential."[303] Similarly, Nancy Hollander, who focuses on criminal defense including in national security contexts, has begun including a bolded auto-signature in her work-related emails with the same effect: "Warning: Based on recent news reports, it is possible that the NSA is monitoring this communication."[304] Overall, however, without a clear sense of the boundaries of US government surveillance, and the effectiveness of various countermeasures, it is difficult to discern what steps lawyers might be obliged to take to protect their information.

[301] Human Rights Watch telephone interview with Jonathan Hafetz, Associate Professor of law at Seton Hall University School of Law, March 13, 2014. Hafetz noted that he became concerned after initial reports about NSA domestic surveillance in 2005, and that his concerns have only grown with the Snowden revelations.

[302] Human Rights Watch telephone interviews with Rob Feitel, defense attorney, March 7, 2014; and an experienced criminal defense attorney, March 10, 2014; Human Rights Watch telephone interview with Linda Moreno, March 12, 2014 and in-person interview, March 20, 2014; Human Rights Watch telephone interview with Jonathan Hafetz, March 13, 2014.

[303] Human Rights Watch telephone interview with Linda Moreno, March 12, 2014 and in-person interview, March 20, 2014.

[304] Email from Nancy Hollander, attorney, to Human Rights Watch, June 24, 2014.

Gillers cautioned lawyers about the use of phone, email, and text communications, noting that when it comes to electronic data, "it doesn't matter what the vehicle is."[305] An experienced criminal defense attorney observed similarly that, based on what we knew about US government surveillance programs before the Snowden leaks, overseas travel (instead of international electronic communication) was likely ethically required for attorneys handling certain types of cases.[306] Now, he argued, "Lawyers have to assume any electronic communication they have is going to be intercepted."[307] Although the risk that poses will vary with the nature of the communications, and might be mitigated in some instances by security measures, lawyers need to treat the likely collection of electronic communications as a "fact of life."[308]

Perlman did not go quite as far. In a March 2014 article, Perlman noted that the challenges of securing one's electronic communications may (for now) create a gap between best practices and ethical obligation.[309] In an interview with us, he suggested that using encrypted email is probably not yet universally required of all lawyers. An attorney might, however, face discipline for removing from his office and subsequently losing an unencrypted flash drive containing highly sensitive client information.[310]

Significantly, the standard shifts with growing common awareness of the risks of certain forms of communication or file storage. Losing an unencrypted flash drive could result in discipline because, according to Perlman, "[i]n light of what we know, [carrying one around is] just too dangerous," and further, "it's easy to avoid the risk."[311] The documents taken by Edward Snowden have demonstrated that an increasing number of electronic transactions are insecure, so "[a]s encryption gets easier, that might be something that becomes necessary, both as a matter of best practices and ethics," Perlman observed.[312] James Connell III, a defense attorney for one of the Guantanamo detainees, agrees: "[It] won't be long before some bar association says you can't . . .

---

[305] Human Rights Watch interview with Stephen Gillers, April 7, 2014.

[306] Human Rights Watch telephone interview with an experienced criminal defense attorney, March 10, 2014.

[307] Ibid.

[308] Ibid.

[309] Andrew Perlman, "Protecting Client Confidences in a Digital Age: The Case of the NSA," *JURIST - Forum*, March 4, 2014, http://jurist.org/forum/2014/03/andrew-perlman-client-confidences.php (accessed July 14, 2014).

[310] Human Rights Watch telephone interview with Andrew Perlman, March 14, 2014.

[311] Ibid.

[312] Ibid.

send unencrypted emails."[313] The same is undoubtedly true for other security measures as well.

Damage to Attorney-Client Trust

One major concern expressed by attorneys is that their inability to guarantee the privacy of their conversations makes it much harder to build trust with their clients. "Normally to build trust you don't want to start with a cautionary statement," observed Shane Kadidal, senior managing attorney of the Guantanamo Global Justice Initiative at the Center for Constitutional Rights.[314] "If your clients see you uncomfortable communicating, they may resist telling you everything," added one federal defender handling a terrorism case. "It just chills the conversation."[315]

"Clients don't tend to come to us with a deep sense of the social compact," noted Ron Kuby, a prominent criminal defense and civil rights lawyer. "They need to be persuaded [to trust their lawyer]." That trust can be essential to the proper functioning of the adversarial process, and it is especially difficult to develop in criminal defense work. Kuby pointed out that many clients who have been charged with an offense are primed to be mistrustful.[316] Nancy Hollander reported increasingly skittish behavior by her clients, describing one who "won't bring his phone to my office."[317] Kuby confirmed that his clients have been less comfortable speaking by phone over the last few years, and he attributes that in part to growing awareness of surveillance by the US government. "It used to be that I could assure them that the government lacked the resources to focus on them. But these days it does have the resources—it can focus on everyone."[318]

Josh Dratel, a renowned criminal defense attorney who has handled a number of terrorism cases, noted a similar phenomenon, pointing out that mistrust of the US government is especially high among people who do not originate in the US.[319] He cannot diminish that

---

[313] Human Rights Watch telephone interview with James Connell III, March 18, 2014.

[314] Human Rights Watch interview with Shane Kadidal, senior managing attorney of the Guantanamo Global Justice Initiative at the Center for Constitutional Rights, New York, New York, March 6, 2014.

[315] Human Rights Watch telephone interview with a federal defender handling a terrorism case, April 3, 2014.

[316] Human Rights Watch telephone interview with Ron Kuby, March 7, 2014.

[317] Human Rights Watch skype interview with Nancy Hollander, April 9, 2014.

[318] Human Rights Watch telephone interview with Ron Kuby, March 7, 2014.

[319] Human Rights Watch telephone interview with Josh Dratel, a criminal defense attorney who has handled numerous terrorism cases, October 11, 2013.

mistrust among his clients "without lying."[320] Large-scale surveillance actually "licenses paranoia among outsiders," significantly affecting how they interact with the legal system, including their own defense attorney. They are less likely, for example, to share essential information with their lawyers.[321] "As a result, I can help them less," he concluded.[322]

Impact on Attorneys' Ability to Effectively Represent Clients

Some attorneys reported feeling forced to change their practices because the government's access to information about their communication patterns (including the contents of some of their work-related exchanges) compromises their strategy.[323] This concern is especially pronounced in contexts where the US government is an opposing legal party, such as in federal criminal cases. In those cases, the government has a genuine interest in the legal strategies employed against it, and the technical ability to gain insight into that strategy by searching through the many electronic records it holds.

The worry here is not so much that the government will explicitly introduce private, strategic communications in court—the attorney-client privilege recognized in US courts largely precludes that possibility[324]—but rather that the government appears to have the power to discern and prepare in advance for the strategy an opposing attorney designs for a case. In general, "it would be a huge advantage to the government" to have access to such information,[325] particularly since defense attorneys do not have any prospect of gaining similar access to the prosecution's information.

Some attorneys also raised concerns about the safety of individuals they might seek to contact in preparing their defenses. For example, Major Jason Wright, an Army JAG who does work before the Guantanamo commissions noted,[326] "We are fearful that our communications with witnesses abroad are monitored," and thus that attempts to build

---

[320] Ibid.

[321] Ibid.

[322] Ibid.

[323] E.g., Human Rights Watch telephone interviews with an experienced criminal defense attorney, March 10, 2014; Human Rights Watch telephone interview with Linda Moreno, March 12, 2014 and in-person interview, March 20, 2014; Human Rights Watch telephone interviews with Jonathan Hafetz, March 13, 2014, and a federal defender based on the West Coast, March 20, 2014.

[324] E.g., Human Rights Watch telephone interview with an experienced criminal defense attorney, March 10, 2014.

[325] Ibid.

[326] "JAG" stands for "Judge Advocate General," and in this context refers to those who serve in the legal branch of the US armed forces.

their case "might put people in harm's way."[327] "Every person you're touching, you're potentially poisoning," agreed Ahmed Ghappour, a law professor at UC Hastings who directs the Liberty, Security, and Technology Clinic.[328]

A clinical law professor who handles national security matters also raised a related pedagogical concern: it might not be in the long-term interests of law students to appear on the radar of the NSA, and that might well happen if they spend a few months on a national security case while in a law school clinic.[329] Without additional detail about what information the government collects, and how it deploys that information, it is difficult to know how to assess these sorts of risks.

Finally, some attorneys expressed the broader concern that large-scale electronic surveillance—by introducing a further, massive power asymmetry between the government and its legal opponents—undermines the adversarial process, a core element of the US criminal justice system.[330] In addition to the possibility that surveillance can give the government insight into opponents' legal strategies, it also provides an enormous but opaque tool for the government to gather evidence against defendants. Because some of this evidence gets collected through sensitive programs, or is considered classified, defendants may never learn how the evidence was obtained and, therefore, be unable to challenge its acquisition as unlawful.[331]

Changing Legal Practices

Many lawyers have long been suspicious about the security of certain forms of communication, even before recent revelations of large-scale electronic surveillance by the US government. "I always assume my phone conversations are being monitored," reported Ron Kuby.[332] Tom Durkin said he had "assumed for years, because of the people I've

[327] Human Rights Watch telephone interview with Jason Wright, March 31, 2014.

[328] Human Rights Watch telephone interview with Ahmed Ghappour, Professor of law at UC Hastings, October 8, 2013.

[329] Human Rights Watch interview with a clinical law professor who handles national security matters, New York, March 19, 2014.

[330] Human Rights Watch telephone interview with Tom Durkin, March 6, 2014.

[331] Human Rights Watch telephone interview with Josh Dratel, October 11, 2013. For more on the government's use of evidence acquired through FISA or the FAA, see Human Rights Watch and Columbia Law School Human Rights Institute, *Illusions of Justice: Human Rights Abuses in US Terror Prosecutions*, http://hrw.org/node/126101, pp. 96-106.

[332] Human Rights Watch telephone interview with Ron Kuby, March 7, 2014.

represented" that the government had access to many of his conversations.[333] And email in particular is problematic because it can so easily be forwarded to third parties.[334]

Nevertheless, a significant number of the lawyers who spoke to us have reduced their reliance on electronic means of communicating or storing data specifically in response to concerns about ongoing surveillance programs. Several emphasized avoiding putting information into emails or discussing matters over the phone.[335] As Linda Moreno put it, "On the phone, we are constrained in our discussions with witnesses and even co-counsel on cases, mindful of government monitoring."[336] One clinical law professor who handles national security matters insists that students working on those cases only perform work from inside a secure clinic office, minimizing the chance that they will save or transmit confidential information insecurely.[337]

"Only a foolish person understands your communications can be intercepted and does nothing about that …It's no different from locking your office door."
—Rob Feitel

Accordingly, lawyers face a choice similar to the one confronting journalists. Some have attempted to increase the security of their electronic tools; others have tried to forgo digital communications or storage tools altogether; and still others have attempted to combine both approaches. Whatever the preferred strategy, a number of attorneys indicated that they must try to do something. "Only a foolish person understands your communications can be intercepted and does nothing about that," observed Rob Feitel, a former federal prosecutor who spent 22 years in the Department of Justice and who now specializes in defense work arising from international and complicated drug cases. "It's no different from locking your office door."[338]

---

[333] Human Rights Watch telephone interview with Tom Durkin, March 6, 2014.

[334] Ibid.

[335] E.g., Human Rights Watch telephone interviews with a New York-based national defense litigator, October 2, 2013; Josh Dratel, October 11, 2013; and a leading national security defense attorney, March 6, 2014; Human Rights Watch interview with Shane Kadidal, March 6, 2014; Human Rights Watch telephone interviews with Rob Feitel, March 7, 2014, and Ron Kuby, March 7, 2014.

[336] Human Rights Watch telephone interview with Linda Moreno, March 12, 2014 and in-person interview, March 20, 2014.

[337] Human Rights Watch interview with a clinical law professor who handles national security matters, New York, March 19, 2014.

[338] Human Rights Watch telephone interview with Rob Feitel, March 7, 2014.

As a result of their growing concerns about surveillance, several attorneys reported encrypting their email or other forms of electronic communications.[339] One lawyer described using air-gapped computers and more secure networks.[340] Another described how his law office maintains its own servers in large part to retain additional control over its data. While there are multiple reasons for his organization to maintain its own servers, some not obviously related to surveillance, this attorney noted that all of those reasons (including surveillance) blend together here because "the [government] is the adversary we're worried about."[341]

Not all of the attorneys we spoke with trust encryption. One noted that it can draw the government's attention to one's communications but may slow down attempts to understand the content.[342] Another suggested that before the Snowden leaks, he might have considered technological solutions to the challenge of protecting communications.[343] He has even used encrypted phone calls in the past, which at the time "seemed over the top."[344] But now he is skeptical that such tools would even work. "Post-Snowden, I think we have to assume there's no encryption the NSA can't beat," he argued, adding, "I don't want a false sense of security."[345]

One defense attorney reported relying exclusively on one particular form of communication that he considered more secure than others for privileged communications with remote clients.[346] "I don't send any information by email, attachment, or phone. I don't use Gchat or What'sApp for anything but 'Hi, what's up?' I don't even talk on Skype."[347]

As with journalists, it is not only the contents of attorneys' communications that matter; it can be important to protect even the fact that they are in contact with particular people. Further, it is not always possible to use advanced electronic security to correspond with the necessary parties, such as when communicating with clients, witnesses, or even co-

---

339 Human Rights Watch interviews with multiple lawyers (names, locations, and dates withheld).

340 Human Rights Watch interview with a lawyer (name, location, and date withheld).

341 Human Rights Watch email correspondence with a lawyer (name, location, and date withheld), June 26, 2014.

342 Human Rights Watch interview with an attorney (name, location, and date withheld). For more on why this is not an idle worry, see Jacob Appelbaum et al., "NSA targets the privacy conscious," *Das Erste*, July 3, 2014, http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html (accessed July 14, 2014).

343 Human Rights Watch interview with a lawyer (name, location, and date withheld).

344 Ibid.

345 Ibid.

346 Human Rights Watch telephone interview with a defense attorney (date withheld).

347 Ibid.

counsel who lack the appropriate resources or technical sophistication.[348] Many attorneys believe that the only secure way to handle such communications is face-to-face.

Many lawyers also reported conducting more meetings in person—sometimes significantly more, and not just with clients, but with co-counsel and witnesses as well.[349] A lawyer specializing in international dispute resolution at an international firm noted that surveillance has intimidated some of her foreign clients, who, as a result, prefer not to communicate remotely, and instead "will only exchange sensitive information in secure rooms in embassies or outside the US."[350] She reported having to travel more to accommodate that preference.[351]

> "[It] seems romantic the first time you do it, but after that it's just a pain in the ass."
> — criminal defense attorney

Yet travel is both expensive and time-consuming, and thus is not always a viable option. Describing the prospect of traveling more to avoid vulnerable long-distance communications, one experienced criminal defense attorney observed, "[It] seems romantic the first time you do it, but after that it's just a pain in the ass."[352] "I can't just jump on a plane and go visit witnesses in order to insure some type of confidentiality," added Linda Moreno, noting that many of her cases have an international component.[353] Tom Durkin highlighted the same problem; describing a colleague who travels to Europe in order to speak face-to-face securely, he observed, "That's a luxury we don't often have."[354]

Having co-counsel located in the US may not be materially better from a strategic point of view when lawyers do not trust the security of their domestic communications. Moreno elaborated:

---

[348] Human Rights Watch interview with a clinical law professor who handles national security matters, New York, March 19, 2014.

[349] E.g., Human Rights Watch interview with Shane Kadidal, March 6, 2014; Human Rights Watch telephone interviews with Rob Feitel, March 7, 2014, and Ron Kuby, March 7, 2014; Human Rights Watch telephone interview with Linda Moreno, March 12, 2014 and in-person interview, March 20, 2014; Human Rights Watch telephone interviews with a lawyer specializing in international dispute resolution at a major international firm, April 1, 2014, and a litigator with a private practice representing international clients, April 7, 2014.

[350] Human Rights Watch telephone interview with a lawyer specializing in international dispute resolution at a major international firm, April 1, 2014.

[351] Ibid.

[352] Human Rights Watch telephone interview with an experienced criminal defense attorney, March 10, 2014.

[353] Human Rights Watch telephone interview with Linda Moreno, March 12, 2014 and in-person interview, March 20, 2014.

[354] Human Rights Watch telephone interview with Tom Durkin, March 6, 2014. Subsequently, Durkin added, "But recently I was forced to do the same." Human Rights Watch telephone interview with Tom Durkin, July 7, 2014.

> I can't tell you how often we [as co-counsel] have to tell each other, "It'll have to wait a month [until I can see you in person]." Just on this trip [to New York, which allowed for the Human Rights Watch interview] my co-counsel on a pending federal case said, "I'll talk to you when you get here." . . . [Still,] sometimes there's an urgency to brainstorming and we just say, we can't run and hide. They're listening to us anyway, but we have to do our work.[355]

Even increased local travel can pose problems. One federal defender handling a terrorism case reported meeting a client in person more frequently to avoid risky electronic communications. Although the client lives in the attorney's area, he works during the week, so in order to discuss the case securely, the attorney must meet him on weekends.[356] While this is less cumbersome than traveling abroad might be, it is yet another burden that disproportionately affects the defense.

> "I'll be damned if I have to start acting like a drug dealer in order to protect my client's confidentiality,"
> — Tom Durkin

On the other hand, a number of criminal defense attorneys expressed principled resistance to modifying their practices to protect against possible intrusion by the US government.

"I'll be damned if I have to start acting like a drug dealer in order to protect my client's confidentiality," asserted Tom Durkin. Another lawyer described the sorts of measures necessary to avoid some forms of government surveillance as "the kinds of techniques that would stand out to me if I wanted to do something illicit."[357] Linda Moreno identified one possible basis for such feelings, noting, "Nobody practiced law like this 15 years ago unless you were a crook."[358] Indeed, James Connell III pointed out that in choosing his security measures, he worries that particularly advanced techniques will look suspicious. "[As much as I want to be secure,] I don't want to look like I'm doing something illegal," he reported. "[There's a] real balance that must be struck."[359] Yet how to strike that balance remains unclear.

---

[355] Human Rights Watch telephone interview with Linda Moreno, March 12, 2014 and in-person interview, March 20, 2014.
[356] Human Rights Watch telephone interview with a federal defender handling a terrorism case, April 3, 2014.
[357] Human Rights Watch email exchange with a litigator with a private practice representing international clients, July 10, 2014.
[358] Human Rights Watch telephone interview with Linda Moreno, March 12, 2014 and in-person interview, March 20, 2014.
[359] Human Rights Watch telephone interview with James Connell III, March 18, 2014.

IV. The Government's Rationale for Surveillance

President Obama has defended his administration's leak investigations as essential to preventing leaks that could endanger US military and intelligence officials,[360] and the government insists that the surveillance programs at the center of the Snowden revelations both comply with the law and protect national security. "I continue to believe that there has been nothing that has come out in the last nine months that is in any way inconsistent with [the claim that everything we do is lawful]," noted one senior intelligence official, who also argued that by and large the programs are valuable for protecting national security.[361]

"These programs are important, vital and lawful," argued Bob Deitz, who served as General Counsel for the NSA from 1998 to 2006, in an interview with us.[362] A senior FBI official concurred, adding, "What's been revealed are intelligence-collection programs that were initially and originally focused on defending the country in a time of war with respect to the enemy that were undertaken in a manner pursuant to the law."

We interviewed five current or former US officials with knowledge of the programs. They generally defended the programs as legal and important for national security. They also showed varying degrees of concern for or interest in the impact that the programs might have on the work of journalists and attorneys. Most were skeptical that the programs have affected journalists and did not appear to have considered seriously the possible effect on attorneys.

The Lawfulness of Current Surveillance Programs

Officials we interviewed argued that the Snowden revelations did not uncover government abuse of its surveillance powers. The senior FBI official observed, "You don't have [evidence of] rampant disregard for the law." He claimed that the programs revealed by

---

[360] On May 16, 2013, Obama offered a public explanation for his interest in stopping leaks of national security information. "Leaks related to national security can put people at risk. They can put men and women in uniform that I've sent into the battlefield at risk. They can put some of our intelligence officers, who are in various, dangerous situations that are easily compromised, at risk. . . . So I make no apologies, and I don't think the American people would expect me as commander in chief not to be concerned about information that might compromise their missions or might get them killed." Joint Conference, President Obama and Prime Minister Erdogan of Turkey, Washington, DC, May 16, 2013, http://www.whitehouse.gov/photos-and-video/video/2013/05/16/president-obama-holds-press-conference-prime-minister-erdogan (accessed July 14, 2014).

[361] Human Rights Watch interview with a senior intelligence official, April 15, 2014 (location withheld).

[362] Human Rights Watch telephone interview with Bob Deitz, General Counsel for the NSA from 1998 to 2006, April 1, 2014.

Snowden are qualitatively different from those described in the findings of the Senate's Church Committee (and its House counterparts) in the mid-1970s. (Those investigations—triggered by news reports of domestic spying by the intelligence community, and by concerns about the Watergate scandal[363]—uncovered widespread abuses by a number of government agencies, including the specific targeting of nonviolent political dissidents.) While the senior FBI official acknowledged that, under the current programs, there have been "mistakes—clear mistakes—that implicate the rights of Americans," he did not regard recent revelations as uncovering willful misconduct.[364] Deitz essentially agreed, insisting that he "wouldn't have spent eight to nine years overseeing lawlessness."

The question of whether the programs fall within the letter of US statutory law has been discussed elsewhere.[365] And whether intelligence officials have engaged in willful misconduct[366] or whether oversight has been adequate[367] are questions that fall outside the scope of this report. However, our research strongly suggests that the US did not design the programs with protection of human rights foremost in mind.

When asked about the role of human rights law in shaping the surveillance activities of the US intelligence community, officials suggested it exists, but is limited. The senior FBI official acknowledged the significance of treaty-based human rights law, noting that "[t]reaties are the supreme law of the land," and adding, "[i]f it's the law, and it applies, we'll enforce it."[368] Yet he also pointed to challenges "operationalizing concepts from international law,"[369] and the comments of other officials suggested that a domestic legal analysis predominates.

---

[363] For more on this sequence of events, see G. Alex Sinha, "NSA Surveillance Since 9/11 and the Human Right to Privacy," *Loyola Law Review*, vol. 59 (2013), pp. 871-873.

[364] Human Rights Watch interview with senior FBI official, Washington, DC, May 12, 2014. The FBI official identified the mistakes as concerning "how NSA processed certain communications," but he did not elaborate.

[365] For more on that discussion, see Brennan Center for Justice, New York University School of Law, "Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs," http://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf (accessed July 14, 2014), p. 3.

[366] For more on that possibility, see Andrea Peterson, "LOVEINT: When NSA officers use their spying power on love interests," *Washington Post*, August 24, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/ (accessed July 14, 2014).

[367] As noted in the Background section above, however, oversight mechanisms for the surveillance programs have received significant criticism recently, in part because various people involved in oversight have themselves expressed concerns. For more on some of that criticism, see Spencer Ackerman, "Fisa court documents reveal extents of NSA disregard for privacy restrictions," *Guardian*, November 19, 2013, http://www.theguardian.com/world/2013/nov/19/fisa-court-documents-nsa-violations-privacy (accessed July 14, 2014).

[368] Human Rights Watch interview with senior FBI official, Washington, DC, May 12, 2014.

[369] Human Rights Watch interview with senior FBI official, Washington, DC, May 12, 2014.

"I don't think that we have historically looked to international human rights law as having a substantial weight of its own, as opposed to … the kind of principles of freedom and dignity and individuality that it's meant to incorporate," noted the senior intelligence official.[370] A former DOJ official said that most of the internal legal assessments would take the form of a "primarily … constitutional analysis"—not an analysis that explicitly takes into account the language of applicable human rights treaties.[371]

Officials repeatedly underscored the level of oversight constraining the American intelligence community. The senior FBI official emphasized "overlapping, extensive oversight by multiple entities," including Congress, the courts, and (at least for the FBI) the Inspector General of DOJ. "I don't think we get enough credit for the work that goes into that [oversight] process," he added.[372] Deitz characterized the US intelligence community as "the most heavily overseen of any … in the world."[373]

The senior intelligence official highlighted the same point, specifically in the context of the surveillance programs described in the Snowden documents. "The [congressional] intelligence committees know all this. They are on top of it and aware of it. We brief them hundreds of times a month on what we're doing and what we're discovering from what we're doing … and contrary to what people think, they push back on us immensely."[374]

The same official also highlighted "a general principle that we can't ask [other governments] to do something that we can't do. That's embodied in Executive Order 12,333."[375] As a result, he noted that "we can't for example, ask GCHQ, 'Hey, could you spy on this American who we are not allowed to spy on?'"[376] When asked if the US government can accept information from other governments that it cannot legally collect on its own, the

---

[370] Human Rights Watch interview with a senior intelligence official, April 15, 2014 (location withheld).

[371] Human Rights Watch telephone interview with former DOJ official, April 10, 2014. The United States takes the position that "[n]othing in [the ICCPR] requires or authorizes legislation, or other action, by the United States of America prohibited by the Constitution of the United States as interpreted by the United States." U.S. reservations, declarations, and understandings, International Covenant on Civil and Political Rights, 138 Cong. Rec. S4781-01 (daily ed., April 2, 1992), http://www1.umn.edu/humanrts/usdocs/civilres.html. The Human Rights Committee criticized this position in the concluding observations of its first review of the United States' compliance with the ICCPR, noting, "The Committee regrets the extent of the State party's reservations, declarations and understandings to the Covenant. It believes that, taken together, they intended to ensure that the United States has accepted only what is already the law of the United States." Report of the Human Rights Committee, A/50/40, October 3, 1995, http://www.un.org/documents/ga/docs/50/plenary/a50-40.htm, para. 279.

[372] Human Rights Watch interview with senior FBI official, Washington, DC, May 12, 2014.

[373] Human Rights Watch telephone interview with Bob Deitz, April 1, 2014.

[374] Human Rights Watch interview with senior intelligence official, April 15, 2014 (location withheld).

[375] Ibid.

[376] Ibid. "GCHQ" refers to Government Communications Headquarters, a British intelligence agency.

official replied, "Sure…. And I don't think there's anything wrong with that."[377] Sharing of that sort could include information on US persons.[378]

Whether the Programs Are Necessary for National Security and Sufficiently Targeted

"Throughout American history, intelligence has helped secure our country and our freedoms," President Obama claimed in his January 2014 surveillance speech.[379] He went on to defend the current surveillance programs as an extension of that tradition. Citing the attacks of September 11, 2001, he elaborated:

> We were shaken by the signs we had missed leading up to the [9/11] attacks—how the hijackers had made phone calls to known extremists and traveled to suspicious places. So we demanded that our intelligence community improve its capabilities, and that law enforcement change practices to focus more on preventing attacks before they happen than prosecuting terrorists after an attack…. And it is a testimony to the hard work and dedication of the men and women of our intelligence community that over the past decade we've made enormous strides in fulfilling this mission.[380]

Officials we spoke with generally shared this view, and also endorsed the scope of the surveillance programs. The senior intelligence official defended them at length, emphasizing that "[w]e don't go out there, and . . . listen to every conversation that Frau Hoffman has with her husband about what kind of bratwurst to bring home for dinner tonight." Instead, he claimed, "[t]he collection is all targeted in some sense at getting things that are legitimate foreign intelligence."[381]

The challenge, he said, is that collecting intelligence to protect national security is a forward-looking exercise, unlike solving crimes. That requires collecting information with some uncertainty as to its ultimate utility. "We don't know necessarily who we're

---

[377] Ibid.

[378] Ibid.

[379] "Obama's Speech on N.S.A. Phone Surveillance," *New York Times*, January 17, 2014, http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html?_r=0 (accessed July 14, 2014).

[380] Ibid.

[381] Human Rights Watch interview with senior intelligence official, April 15, 2014 (location withheld).

looking for or what we're looking for; we may not even know the type of thing we're looking for."[382]

Additionally, "Al-Qaeda communications are flowing along exactly the same pipes as your communications are. So technologically, we need to be able to [identify and sort through those communications]." Naturally, "[i]f you're listening for conversations of bad people, you are going to listen to and intercept some conversations of people who aren't bad people. And that's where the minimization comes in."[383]

As noted in the Background section, agencies that conduct surveillance, like the NSA, will generally operate under a set of "minimization procedures"—broad guidelines shaping the way they can acquire, retain, disseminate, or use information they have the power to collect.[384] For example, the agency might set procedures that instruct employees, in certain circumstances, to redact personally identifying information of US persons found in intercepted communications. Those guidelines can be important because, as the senior intelligence official implied, the government collects a lot of information about people who are not suspected of doing anything wrong. It then sifts through much of that information, based in part on the terms of its minimization procedures. However, the government operates a large number of different surveillance programs, and we do not know the details of most of the minimization procedures that constrain them. Such procedures also seem to provide safeguards only for US persons—and even those appear to be very weak. What little is public about the procedures suggests that they place even fewer constraints on what the government may do with information and communications of non-US persons.

More generally, "I probably couldn't defend every single [bit of] surveillance that is done out there as essential to national security. I think by and large though … it's an apparatus that is set-up to [serve that function]," said the senior intelligence official.[385] As for the bulk metadata program under Section 215, he likened it to a "fire insurance policy" meant to provide a critical capacity that was absent before the 9/11 attacks.[386]

---

[382] Ibid.

[383] Ibid.

[384] For example, according to a senior DOJ official, "the FBI is the component of the Department of Justice that conducts electronic surveillance under FISA and therefore has minimization procedures governing the information that is acquired." Email from senior DOJ official to Human Rights Watch, July 15, 2014.

[385] Ibid.

[386] Ibid.

Officials on Whether the Snowden Disclosures Harmed National Security

While this was not a central focus of our research, it is worth noting that officials did not all agree on the impact that the Snowden disclosures might have had on US national security. Overall, Deitz condemned Snowden's disclosures, claiming that "any professional in the intelligence world will say it's the single most damaging set of leaks [they've ever seen]." The senior intelligence official, while disapproving of the leaks, took a more measured view, arguing that "it's too soon to tell whether [these leaks are] going to have a measurable effect on our ability to protect the nation." He added, "It's only been 9 months since this started, so we can't tell." Still, he claimed that "particular targets have changed their methods of communications because of what's been disclosed." While "it's very hard for us to know what we're not seeing," he argued that less information is available to the intelligence community as a result. NSA director Admiral Michael Rogers made a similar assessment in an interview with the *New York Times*, saying, "'You have not heard me as the director say, 'Oh, my God, the sky is falling.'" Aside from some diminished traffic along certain lines of communication, none of the concerned officials pointed to specific, concrete, and identifiable harms.

Whether the Programs Have a Chilling Effect on the Rights of Journalists, Lawyers, or Others

The officials we spoke with denied that the surveillance programs are intended to chill permissible activity. "I don't think anybody rational has suggested these are intended to chill civil liberties," said the senior intelligence official.[387] They also expressed skepticism that surveillance programs have caused any unintended, objectionable chilling effects.[388]

Officials distinguished between different kinds of chilling. For example, the senior intelligence official separated "rational" and "irrational" chilling.[389] "Journalists who suggest that their lives are at risk and they therefore have to take precautions to avoid

[387] Human Rights Watch interview with senior intelligence official, April 15, 2014 (location withheld).

[388] Human Rights Watch telephone interview with Bob Deitz, April 1, 2014, Human Rights Watch interview with senior intelligence official, April 15, 2014 (location withheld).

[389] Human Rights Watch interview with senior intelligence official, April 15, 2014 (location withheld).

being assassinated by the CIA, or journalists who suggest that they have to be concerned that their conversations are going to be monitored because of their journalism, that's just a fantasy." He added, "It's our assessment that [these programs] are not having and should not have an undue chilling effect, and that frankly, to the extent that people are perceiving the chilling effect now, it's largely due to misperception, sometimes intentionally fostered, about how the programs work."[390]

Deitz made a related but different distinction, dividing legitimate and illegitimate chilling.[391] When asked about the possibility that reporting has become more difficult, Deitz responded, "Leaking is against the law. Good. I want criminals to be deterred."[392] Deitz analogized the chilling of sources to police deterrence of crime, which he called "legitimate" chilling. "Does a cop chill a burglar's inclination to burgle? Yes."[393]

> " I don't think anybody rational has suggested these are intended to chill civil liberties "
> — senior intelligence official

Deitz's comparison of leakers to burglars disregards the pervasive over-classification of information in the United States, and the strong public interest in learning about much of that information. Moreover, it is simply not applicable to much of the work done by journalists covering the government. As noted above, a significant proportion of the reporting that journalists do on sensitive areas involves assembling bits of information that are not classified to begin with.

As to the journalists' worries that information acquired through surveillance could be used in leak investigations, a senior DOJ official largely dismissed concerns over the increase in leak prosecutions pursued by the Obama administration:

> There have been a small number of prosecutions of individuals for unauthorized disclosures of classified information that reflects a very

[390] Ibid.

[391] Human Rights Watch telephone interview with Bob Deitz, April 1, 2014.

[392] Ibid.

[393] Several journalists expected this sort of response, believing that the government actively intends for there to be a chilling effect. E.g., Human Rights Watch interviews with Dana Priest, national security reporter at the *Washington Post*, Washington, DC, December 17, 2013; Human Rights Watch telephone interview with Scott Shane, intelligence reporter for the *New York Times*, April 2, 2014.

> small percentage of the unauthorized disclosures of classified information that have occurred…. I am aware of no change in policy during the Obama Administration seeking to increase investigation and prosecution of unauthorized disclosures of classified information, and any marginal increase in the number of such prosecutions in recent years is not attributable to such a change nor necessarily indicative of future trends in this area.[394]

However, he did acknowledge that "it is possible (though not particularly likely)" that raw intelligence information collected under Section 702 or Executive Order 12,333 "could be identified by FBI as germane to such an investigation or referred to FBI by another agency for such an investigation."[395]

The same official also explained that information collected or derived from electronic surveillance under FISA might make its way into criminal prosecutions as evidence against "an aggrieved person, provided that the aggrieved person and the court or other authority are notified that the government intends to use or disclose such information."[396] Accordingly, he said, "information acquired or derived from FISA is used in some criminal prosecutions related to national security, such as counterterrorism or counterespionage matters, and could be used as well in criminal cases that do not have a nexus to national security."[397]

Though the senior DOJ official indicated that information collected through Section 702 or Executive Order 12,333 is unlikely to be used in leak investigations, the possibility that it could be—and that it could be introduced as evidence—gives real substance to some of the journalists' worries about leaving an electronic trail to their sources, especially where the journalists do research with an international dimension.

---

394 Email from senior DOJ official to Human Rights Watch, July 15, 2014.

395 Ibid. The same official explained that the National Security Division of the Justice Department (NSD), which handles leak investigations, does not itself query such information, though the NSD "is responsible for obtaining authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (FISA) and representing the government before the Foreign Intelligence Surveillance Court." Ibid.

396 Ibid.

397 Ibid.

The Impact on Journalists

The officials were skeptical that surveillance has undermined reporting, or indeed, that anything else has either. "[People argue that] this mass surveillance apparatus is going to cause whistleblowers to dry up and not be willing to talk to reporters and there's absolutely no indication of that in the press at all. There's a steady stream every day of classified information coming out."[398] More broadly, he observed, "We haven't really seen … any measurable change in the journalistic output."[399] As the senior FBI official put it, "The First Amendment seems quite alive and well in America today."[400]

Two officials suggested that journalists have always complained about the challenges of reporting. According to Deitz, "These things rotate through Washington every few years. Nixon had an enemies list. It was a matter of prestige to be on it."[401] The senior intelligence official argued similarly that "this is a constant dynamic, and I think that there is always going to be a flow of information to the press, and the press is always going to be complaining that they're not getting enough of it."[402]

When asked what would constitute sufficient evidence of a chilling effect to cause them concern, both Deitz and the senior FBI official expressed skepticism about the reliability of self-reports by journalists or others. Deitz in particular claimed that people could exploit assertions that they are now constantly on alert for surveillance to advance their interests, observing that "the press is used as much as it uses."[403] He appeared to be suggesting that journalists speaking to us for our research have an incentive to exaggerate their concerns about surveillance. The senior intelligence official responded that "the immediate canary in the mine would be if all of a sudden stories about leaks of classified information stopped appearing in the newspapers."[404] While he argued that he has seen no indication that less information has made its way to the media, he acknowledged that it would be "hard to measure" such a phenomenon.[405]

---

[398] Human Rights Watch interview with senior intelligence official, April 15, 2014 (location withheld).
[399] Ibid.
[400] Human Rights Watch interview with senior FBI official, Washington, DC, May 12, 2014.
[401] Human Rights Watch telephone interview with Bob Deitz, April 1, 2014.
[402] Human Rights Watch interview with senior intelligence official, April 15, 2014 (location withheld).
[403] Human Rights Watch telephone interview with Bob Deitz, April 1, 2014.
[404] Human Rights Watch interview with senior intelligence official, April 15, 2014 (location withheld).
[405] Ibid.

Some journalists independently spoke directly to this point. One suggested that a pair of sizable leaks in recent years—one by Chelsea Manning and one by Edward Snowden—may be obscuring the chilling effect in part, supplying two specific streams of classified information.[406] Indeed, some of the journalists we spoke with indicated that levying hefty penalties against suspected sources weeds out all but the most committed sources, creating an environment more suitable for occasional, massive leaks of highly sensitive information rather than more numerous, smaller disclosures of less sensitive information.[407] As Charlie Savage noted, journalists having more consistent access to a wider range of government agencies may be better for "shed[ding] light on democratic processes" than having a small number of concentrated leaks.[408] The government might prefer that situation as well.

The Impact on Lawyers and Their Clients

Government officials had somewhat less to say regarding the possibility that surveillance has a chilling effect on attorneys and their clients. The senior intelligence official observed that "this is not a new issue for lawyers, how to protect their communications in an electronic age," indicating that he had seen it arise in private practice years ago.[409] He elaborated:

> Should lawyers communicate by email at all with their clients? … [Not doing so] imposes a little additional cost, but … if lawyers weren't taking these kind of precautions beforehand, they probably should have been. So, I don't know how much you can attribute to this particular issue.[410]

While the government does have some minimization procedures in place for attorney-client communications, as previously noted, those procedures do not clearly apply across all programs, and they appear to be limited to cases involving a client under indictment. Moreover, while these rules apply for the most part to direct communication between attorneys and their clients, attorneys are bound to protect information that extends far

---

[406] Human Rights Watch telephone interview with Charlie Savage, reporter for the *New York Times*, March 14, 2014.

[407] E.g. Human Rights Watch interview with James Asher, Washington Bureau Chief for *McClatchy Co.*, Washington, DC, December 12, 2013; Human Rights Watch telephone interview with Charlie Savage, March 14, 2014.

[408] Human Rights Watch telephone interview with Charlie Savage, March 14, 2014.

[409] Human Rights Watch interview with senior intelligence official, April 15, 2014 (location withheld).

[410] Ibid.

beyond their direct communications with clients, including nearly all information related to legal representation.

What the Government Should Do

The revelations of large-scale surveillance by the US have prompted discussion and a few modest steps towards reform by the President and Congress. However, for the most part discussion of reform has been dominated by concerns over intrusion on privacy rights. While the privacy concerns are pressing and important, there has been little public discussion of how the US should act to prevent a chilling of freedoms of the press, expression, and association, or damage to the attorney-client relationship.

As noted above, some of the officials we spoke to denied that there was any sort of inappropriate chilling effect. Those who acknowledged a chilling effect did not seem to think reform of government programs was in order, though two officials noted that the government has an obligation to allay concerns among the public, even if those concerns are grounded in misunderstandings about the government's activity because of inaccurate or overwhelming press reports. When asked about whether the government might have such a duty, the senior intelligence official responded, "Totally. Totally." He added, "If someone wants to write a report that criticizes us for not doing a good enough job of explaining what it is that we do, I'm totally there. I think we have not done a good enough job."[411] The former DOJ official essentially agreed. "It's incumbent on the Executive Branch to put people at ease."[412]

Ultimately, the officials expressed varied responses to this investigation. The senior FBI official voiced an interest in reviewing any evidence of chilling effects on rights that we identified.[413] Deitz, on the other hand, seemed to think the entire project was misguided.[414]

---

[411] Ibid.

[412] Human Rights Watch telephone interview with former DOJ official, April 10, 2014.

[413] Human Rights Watch interview with senior FBI official, Washington, DC, May 12, 2014.

[414] "The problem with organizations [like HRW and the ACLU] is that they're monomaniacs," he said, adding that such groups are blind to "shade[s] of gray" in public policy questions, a result he termed "ridiculous." When our researcher insisted that both organizations genuinely seek to understand the government's stances on these issues, Deitz replied, "Color me skeptical." Human Rights Watch telephone interview with Bob Deitz, April 1, 2014.

V. The Rights at Stake

The US surveillance practices revealed over the last year raise a wide variety of human rights concerns. The issue that probably has received the most attention in public debate so far is the impact of surveillance on the right to privacy of individuals across the globe and in the US, which Human Rights Watch and the ACLU have discussed at length in other reports and submissions.[415] However, the particular patterns described in this report—the effect of surveillance on journalists, attorneys and their clients—raise further concerns about the impact of surveillance on another cluster of related rights: freedoms of expression and association, freedom of the press, the public's right to access information, and the right to counsel.[416]

Rights Affected by Surveillance's Impact on Journalists

Both international human rights law and the US Constitution protect the freedoms of expression and association, as well as the right to privacy.[417] Under both domestic and

---

[415] E.g., Comments of Human Rights Watch to the Privacy and Civil Liberties Oversight Board, August 1, 2013, http://www.hrw.org/sites/default/files/related_material/Comment%20HRW%20PCLOB%20Final%208-1-13_0.pdf; Human Rights Watch, Letter to President Obama Urging Surveillance Reforms, January 16, 2014, http://www.hrw.org/news/2014/01/16/letter-president-obama-urging-surveillance-reforms; Human Rights Watch and the Electronic Frontier Foundation Supplemental Submission to the Human Rights Committee During its Consideration of the Fourth Periodic Report of the United States, February 14, 2014, http://www.hrw.org/news/2014/02/14/human-rights-watch-and-electronic-frontier-foundation-supplemental-submission-human-; Human Rights Watch, Joint Submission to OHCHR Consultation in Connection with General Assembly Resolution 68/167: "The Right to Privacy in the Digital Age," April 1, 2014, https://www.hrw.org/news/2014/04/01/joint-submission-ohchr-consultation-connection-general-assembly-resolution-68167-rig. Privacy and Civil Liberties Oversight Board Public Hearing on Section 702 of the FISA Amendments Act, Submission of Amnesty International & American Civil Liberties Union, March 19, 2014, https://www.aclu.org/sites/default/files/assets/aiusaaclusubmissiontopclob.pdf (accessed July 17, 2014);

American Civil Liberties Union, "Privacy Rights in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights, Draft Report & General Comment," March 2014, https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf (accessed July 17, 2014).

[416] There is a strong and well-recognized connection between privacy and freedom of expression in that inadequate protections for the former can seriously undermine the latter. For sources recognizing that connection, see, e.g., UN Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," Frank La Rue, A/HRC/23/40, April 17, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed July 14, 2014) paras 24-27. The US government's interest in promoting freedom of expression online around the world thus relies significantly on the presence of sufficient privacy protections. For the government's own statement about its interests in promoting freedom of expression online, see US Department of State, "Diplomacy in Action: Internet Freedom," http://www.state.gov/e/eb/cip/netfreedom/index.htm (accessed July 14, 2014).

[417] The US Constitution does not mention privacy by name, but the right finds roots in the 4th Amendment ban on "unreasonable searches and seizures." U.S. CONST. amend. IV.

international law, freedom of expression can also include anonymous speech,[418] and freedom of association can apply both to the freedom of individuals to join and engage with civil society groups and to the right of government officials to interact with members of the press. Moreover, international standards governing freedom of expression protect not just the right to express views for advocacy purposes, but also the right of access to information, including the right to learn about the activities of government, and the right of journalists to pursue information for the public benefit.[419] The same international human rights standards allow limitation of these rights in the interest of national security, but any such restrictions must be necessary to the goal pursued, and proportionate to it.

International Human Rights Law and Standards on Freedom of Expression, Association, and Access to Information

In order for a democratic society to function, and in order for healthy debate over government policies to flourish, people must enjoy the fundamental rights to speak and associate freely, and to acquire information about matters of public concern. Without these, it becomes extremely difficult for the public to have an informed discussion about government policies and practices.

The US ratified the International Covenant on Civil and Political Rights (ICCPR) in 1992, making it binding on the US.[420] The treaty protects the freedom of expression (Article 19), encompassing the freedom of speech that is so prominent in US constitutional law. It also protects the freedom of association (Article 22),[421] and the right to privacy (Article 17).[422] Freedom of expression in the ICCPR also includes "the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers."[423]

---

[418] For more on anonymous speech in human rights law, see UN Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," Frank La Rue, A/HRC/23/40, April 17, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, paras. 88-90.

[419] International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No.16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, ratified by US on June 8, 1992, art. 19.

[420] Ibid. Although the treaty is binding, people cannot bring individual lawsuits based solely on the treaty in US courts.

[421] Ibid., art. 22.

[422] Ibid., art. 17.

[423] Ibid., art. 19. According to Manfred Nowak, no state was in favor of a narrow reading of this article in drafting the treaty, so "there can be no doubt that every communicable type of subjective idea and opinion, of value-neutral news and information, of … political commentary regardless of how critical, … is protected by Art. 19(2)." Manfred Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (Arlington: N.P. Engel, 1993), p. 341. The right also appears in the Universal Declaration of Human Rights (UDHR) and the American Declaration of the Rights and Duties of Man. See Universal Declaration of Human Rights

Additionally, Article 26 of the ICCPR requires equal protection before the law for everyone, regardless of status.[424] As a result, the rights in the ICCPR apply equally to all, including noncitizens. Indeed, the UN Human Rights Committee (HRC), the body established by the ICCPR to review state reports and issue interpretations of the treaty, has reaffirmed that expression, association, and privacy are rights that do not admit of discrimination "between aliens and citizens."[425]

The US has long maintained the position that the ICCPR imposes no extraterritorial obligations on states parties, and thus that the government's obligations under the treaty do not extend beyond its own borders.[426] That position helps the US to justify implementing surveillance programs that are especially invasive of the rights of foreigners located abroad. Yet international bodies, including the HRC[427] and the Office of the High Commissioner on Human Rights,[428] have repudiated the idea that the ICCPR has no extraterritorial reach. Indeed, where a state can project its authority to intercept the electronic communications of persons outside its territory, it carries with it the obligation to respect privacy, freedom of expression, and other associated rights.[429]

(UDHR), adopted December 10, 1948, G.A.Res. 217A(III), U.N. Doc. A/810 at 71 (1948), art. 19; American Declaration of the Rights and Duties of Man, adopted April 1948, Ninth International Conference of American States, art. IV.

[424] ICCPR., art. 26.

[425] UN Human Rights Committee, General Comment 15: The position of aliens under the Covenant, U.N. Doc. HRI/GEN/1/Rev.1 (April 11, 1986), para. 7; see also Submission of Amnesty International USA and the American Civil Liberties Union to Privacy and Civil Liberties Oversight Board, Public Hearing on Section 702 of the FISA Amendments Act, March 19, 2014, https://www.aclu.org/sites/default/files/assets/aiusaaclusubmissiontopclob.pdf (accessed July 14, 2014), p. 13. The Human Rights Committee (HRC) is a group of experts tasked by the UN with monitoring the implementation of the ICCPR. Its General Comments are the most authoritative interpretations of state obligations under the treaty, though states do not always adopt the HRC's views.

[426] For more on the US position, see Harold Koh, Office of the Legal Advisor, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights, October 19, 2010, http://justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf (accessed July 14, 2014), pp. 1-2.

[427] Human Rights Committee, "Concluding observations on the fourth periodic report of the United States of America," CCPR/C/USA/CO/4, April 23, 2014, http://www.refworld.org/docid/5374afcd4.html (accessed July 14, 2014), para. 4, noting, "The Committee regrets that the State party continues to maintain the position that the Covenant does not apply with respect to individuals under its jurisdiction, but outside its territory, despite the interpretation to the contrary of article 2, paragraph 1, supported by the Committee's established jurisprudence, the jurisprudence of the International Court of Justice and State practice.")

[428] UN Human Rights Council, "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights," A/HRC/27/37, June 30, 2014, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (accessed July 14, 2014), para. 34.

[429] Ibid.

In its General Comment 34, the HRC also observed that the freedoms of expression and association are related.[430] The rights to information and to freedom of expression are integral to group advocacy, political organizing, vindication of rights, civil society monitoring, and many other associative activities in a normal democratic society.

Further, the HRC has interpreted the language of Article 19 to establish a "right to access to information held by public bodies."[431] To give effect to the right, the Committee has stated that "States parties should proactively put in the public domain Government information of public interest. States parties should make every effort to ensure easy, prompt, effective and practical access to such information."[432]

There is growing international recognition that the right to seek, receive, and impart information encompasses a positive obligation of states to provide access to official information in a timely and complete manner. For example, the Organization of American States (OAS) has stated that the right of access to official information is a fundamental right of every individual.[433] Moreover, it is internationally recognized that the right of

---

[430] UN Human Rights Committee, General Comment 34, Article 19: Freedoms of opinion and expression, U.N. Doc. CCPR/C/GC/34 (2011), para. 4, (noting "freedom of expression is integral to the enjoyment of the rights to freedom of assembly and association.")

[431] Ibid., paras. 18 and 19.

[432] Ibid., para. 19.

[433] Organization of American States, Declaration of Principles on Freedom of Expression, October 19, 2000, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26&lID=1, prin. 4. For explanatory background on the principles, see Organization of American States, Background and Interpretation of the Declaration of Principles, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=132&lID=1. The Inter-American Commission on Human Rights (IACHR) adopted the declaration at its 108th regular sessions in October 2000. Ibid. In adopting the declaration, the IACHR interpreted Article 13 (freedom of expression) of the American Convention on Human Rights, which the US has signed though not ratified, to include the right of access to official information. Ibid. Other regional and international institutions have made similar statements. For examples of such statements, see, e.g., Joint declaration by Ambeyi Ligabo, U.N. Special Rapporteur on Freedom of Opinion and Expression, Miklos Haraszti, OSCE Representative on Freedom of the Media, and Eduardo Bertoni, OAS Special Rapporteur for Freedom of Expression, December 6, 2004, http://www.cidh.org/Relatoria/showarticle.asp?artID=319&lID=1 (accessed July 14, 2014). See also United Nations Economic and Social Council, Commission on Human Rights, *Civil and Political Rights, Including the Question of Freedom of Expression: The Right to Freedom of Opinion and Expression. Report of the Special Rapporteur, Ambeyi Ligabo, submitted in accordance with Commission resolution 2003/42*, (New York: United Nations, 2003); IACHR, *Report on Terrorism and Human Rights*, OAS/Ser.L./V/II 116, Doc. 5 rev. 1 corr. October 22, 2002, http://www.cidh.org/terrorism/eng/toc.htm (accessed July 14, 2014), para. 281. Although a narrower interpretation of the right of access to information has prevailed in Europe, the European Court of Human Rights, interpreting Article 8 (private and family life) of the European Convention, has found that individuals have the right to obtain information held by the government if such information affects their private lives, and that the government's storage of that information therefore interferes with their rights to privacy and family life guaranteed by the Convention. The European Court has also established that governments may not restrict a person from receiving information that others wish or may be willing to impart. European Court of Human Rights, *Leander v. Sweden*, no. 10/1985/96/144, February 1985, paras. 48 and 74; European Court of Human Rights, *Gaskin v. United Kingdom*, no. 2/1988/146/200, June 1989, para. 49; and European Court of Human Rights, *Guerra and others v. Italy*, no.

access to official information is crucial to ensure democratic control of public entities and to promote accountability within the government.[434]

The Human Rights Committee (HRC) has also specifically emphasized that press freedom—and the ability of the press to obtain information—is essential to ensure freedom of expression and the enjoyment of other rights:

> It constitutes one of the cornerstones of a democratic society. The Covenant embraces a right whereby the media may receive information on the basis of which it can carry out its function. The free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion. The public also has a corresponding right to receive media output.[435]

116/1996/735/932, February 1998, paras. 53 and 60. The European Court's reading finds support in Principle 3 of the Declaration of Principles on Freedom of Expression. Organization of American States, Declaration of Principles on Freedom of Expression, October 19, 2000,http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26&lID=1, prin. 3.

[434] For discussion of these connections, see Organization of American States, Declaration of Principles on Freedom of Expression, http://www.oas.org/en/iachr/expression/showarticle.asp?artID=26&lID=1, prin. 1. In Europe this has been recognized since the early 1980s. Toby Mendel, "Freedom of Information: An Internationally protected Human Right," *Comparative Media Law*, January-June 2003, pp. 13-19, http://www.juridicas.unam.mx/publica/rev/comlawj/cont/1/cts/cts3.htm (accessed July 14, 2014). The Inter-American Court of Human Rights held in 1985 that effective citizen participation and democratic control, as well as a true debate in a democratic society, cannot be based on incomplete information. Understanding freedom of expression as both the right to express oneself, and the right to obtain information, the Inter-American Court of Human Rights held that "freedom of expression is a cornerstone upon which the very existence of a democratic society rests. It is indispensable in the formation of public opinion. It represents, in short, the means that enable the community, when exercising its options, to be sufficiently informed. Consequently, it can be said that a society that is not well informed is not a society that is truly free." Inter-American Court of Human Rights, "Compulsory Membership in an Association prescribed by Law for the Practice of Journalism (Articles 13 and 29 American Convention on Human Rights)," Advisory Opinion OC-5, November 13, 1985, para. 70. The OAS General Assembly has held in 2003, 2004, and 2005 that access to official information is an indispensable requirement for a democracy to work properly, and that states have an obligation to ensure access to information. OAS General Assembly Resolution on Access to Official Information: Strengthening Democracy, AG/Res. 1932 (XXXIII-O/03), June 10, 2003, http://www.oas.org/juridico/english/ga03/agres_1932.htm (accessed July 14, 2014); OAS General Assembly Resolution Access to Official Information: Strengthening Democracy, AG/Res. 2057 (XXXIV-O/04), June 8, 2004, http://www.upd.oas.org/lab/Documents/general_assembly/2004/ag_res_2057_xxxix_O_04_eng.pdf (accessed July 14, 2014); and OAS General Assembly Resolution on Access to Official Information: Strengthening Democracy, AG/RES. 2121 (XXXV-O/05), May 26, 2005, http://www.oas.org/XXXVGA/docs/ENG/2121.doc (accessed July 14, 2014).

[435] UN Human Rights Committee, General Comment 34, Article 19: Freedoms of opinion and expression, U.N. Doc. CCPR/C/GC/34 (2011), para. 13.

The freedom of expression guaranteed by the ICCPR is not absolute. The treaty builds in several possible limitations, including one for the protection of national security.[436] However, any such restrictions must be strictly cabined: as indicated by the text, the right "may … be subject to certain restrictions, but these shall only be such as are provided by law and are necessary … for the protection" of a listed state interest.[437]

As noted by the HRC, this language means that any restrictions on these rights must meet specific conditions: they must be "provided by law"; they must adhere to one of the purposes laid out in Article 19; and "they must conform to the strict tests of necessity and proportionality…. Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated."[438]

Of particular interest, the HRC has also warned about the risks of government overreach in the name of national security, noting that States parties must ensure that provisions to protect national security are not invoked "to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information."[439]

Since the adoption of the ICCPR, civil society groups, governments, and international institutions have also worked together to further develop legal standards that address the apparent tension between access to information and the protection of national security. Those standards, while not binding, are based on developing norms of international law

---

[436] Limitations may also be permissible for the protection of public order, public health or morals, or the rights and freedoms of others. For a list of those limitations, see, e.g., ICCPR, art. 12. Our analysis focuses on the national security exception because that is the public justification for the surveillance programs and the crackdown on leaks. The Human Rights Committee has also acknowledged the national security limitation on the right to freedom of expression. UN Human Rights Committee, General Comment 34, Article 19: Freedoms of opinion and expression, U.N. Doc. CCPR/C/GC/34 (2011), para. 21. Legal scholars argue that the same limitations apply to rights guaranteed by Article 17 (right to privacy), even though the text does not list any exceptions or limitations. As one example, see, e.g. Manfred Nowak, U.N. Covenant on Civil and Political Rights: CCPR Commentary, 2d rev. ed. (Kehl am Rhein: Engel, 2005), p. 381. UN Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," Martin Scheinin, A/HRC/13/37, December 18, 2009, http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf (accessed July 15, 2014); UN Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," Frank La Rue, A/HRC/23/40, April 17, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed July 15, 2014)

[437] ICCPR, art. 19(3), at 52.

[438] UN Human Rights Committee, General Comment 34, Article 19: Freedoms of opinion and expression, U.N. Doc. CCPR/C/GC/34 (2011), para. 22.

[439] Ibid., para. 30.

and state practice, and provide informed, detailed, and legally persuasive guidelines for the interpretation of the proper scope of some of the rights that the ICCPR protects.

One set of such relevant standards, in wide use and grounded in international and comparative law, is the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (Johannesburg Principles).[440] These principles provide that restrictions on expression based on national security "must have the genuine purpose and demonstrable effect of protecting a legitimate national security interest,"[441] which they define as protecting "a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government."[442]

The 2013 Tshwane Principles on National Security and the Right to Information (Tshwane Principles) apply developing interpretation and jurisprudence of national and international bodies to the right to information.[443] The Tshwane Principles provide: "Everyone has the right to seek, receive, use, and impart information held by or on behalf of public authorities, or to which public authorities are entitled by law to have access."[444]

The Tshwane Principles directly address the ICCPR limitations, recognizing that governments may need to keep certain information classified, including information with particularly strong implications for national security.[445] However, the Principles make clear that that the government bears the burden of proving that the restriction is permissible. To do so, it must show that: "(1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest; and (2) the law provides for adequate safeguards against abuse, including prompt, full, accessible, and

---

[440] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information (Johannesburg Principles), November 1996, http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf (accessed July 14, 2014).

[441] Ibid., Principle 1.2.

[442] Ibid., Principle 2(a).

[443] The Tshwane Principles have the same legal standing as the Johannesburg Principles, providing an influential interpretation of the standard, under international law, for balancing access to information with the protection of national security.

[444] The Global Principles on National Security and the Right to Information (Tshwane Principles), June 12, 2013, http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf (accessed July 14, 2014), Principle 1(a).

[445] Ibid., Principle 9(a)(i)-(v).

effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts."[446]

Although the Tshwane Principles, unlike the Johannesburg Principles, do not define "national security," they do recommend it be defined precisely in law in a manner consistent with a democratic society. The principles list a small, illustrative set of types of information that might legitimately be withheld from disclosure on national security grounds provided such nondisclosure is both necessary and proportionate to protect national security.[447] But they specifically list other types of information, which in practice are often withheld, where there is a strong presumption in favor of public disclosure.

Importantly, the Tshwane Principles also make clear that for some categories of information, there is an overriding public interest in disclosure, which means that the information cannot be withheld under any circumstances, because they are "of particularly high public interest given their special significance to the process of democratic oversight and the rule of law,"[448] These categories include information about gross violations of human rights or serious violations of international humanitarian law,[449] as well as state surveillance.[450] Finally, the principles also provide that the disclosure by public personnel of certain categories of wrongdoing (such as human rights violations)—in other words, disclosures by whistleblowers—should be protected.[451]

There is no question that the US government holds some information with grave, direct implications for the safety of the nation. To the extent that it does, the government is entitled—indeed, has a duty—to shield that information from the press and the public in order to protect national security. Yet, if it invokes national security as a basis for

---

[446] Ibid., Principle 3.

[447] Specifically, the Principles list five categories that cover "on-going defense … operations"; "weapon systems"; "specific measures to safeguard the territory of the state" (or other critical strategic assets); "operations, sources, and methods of intelligence services" geared toward protecting national security; and "information concerning national security" that was provided by other states or bodies under a guarantee of confidentiality. Ibid., Principle 9ai-v.

[448] Ibid., Principle 10.

[449] Ibid., Principle 10(a). Such information, which includes "crimes under international law, and systematic or widespread violations of the rights to personal liberty and security," "may not be withheld on national security grounds in any circumstances." Ibid., Principle 10(a)(1). Information related to less serious violations of human rights or humanitarian law remains "subject to a high presumption of disclosure." Ibid., Principle 10(a)(2).

[450] Ibid., Principle 10(e).

[451] Ibid., Principles 37-41.

restricting information, then it needs to make the case that the restriction really is necessary and proportionate, and meets all of the other requirements outlined above.

There is also no question that the US government routinely classifies a broad array of information that, while convenient to keep confidential, is not a serious risk to national security.[452] Even much of the classified information released by Snowden may well fall into this category.

Unclassified information and personal opinions of federal employees are even less likely to be legitimately kept from the public on national security grounds. In fact, certain government agencies implementing their own version of the Insider Threat Program, such as the Peace Corps, may be hard-pressed to show that any information they seek to protect on national security grounds genuinely relates to national security in the precise sense contemplated by international human rights law.

Of course, there is a great deal of information that the US may be legitimately seeking to withhold on grounds that are unrelated to national security—such as international relations, public order, public health and safety, law enforcement, future provision of free and open advice, effective policy formulation, and economic interests of the state. However, the Tshwane Principles make very clear that even when these other justifications for restricting access to information are invoked, "they must at least meet the standards for imposing restrictions on the right of access to information" that apply to information implicating national security.[453] In other words, it is up to the US government to prove that such restrictions are strictly necessary to serve a legitimate interest, and that there are safeguards in place to prevent abuse.

As noted above, it is well established—and the government has often admitted—that over-classification is a problem within the US government.[454] Initiatives—such as the Insider

---

[452] Even the government acknowledges that over-classification occurs. E.g., Ben Rhodes, "The President Signs H.R. 533, The Reducing Over-Classification Act," The White House Blog, October 7, 2010, http://www.whitehouse.gov/blog/2010/10/07/president-signs-hr-553-reducing-over-classification-act (accessed July 14, 2014). The Office of the Director of National Intelligence, "Intelligence Community Classification Guidance Findings and Recommendations Report," January 2008, http://www.fas.org/sgp/othergov/intel/class.pdf (accessed July 14, 2014), p. v. "Pentagon Acknowledges, Combats Overclassification," *Secrecy News*, November 1, 2004, http://fas.org/sgp/news/secrecy/2004/11/110104.html (accessed July 14, 2014).

[453] Tshwane Principles, Principle 2(b).

[454] For more, see Footnote 452.

Threat Program—that seek to prevent or punish disclosure of *all* classified information are by their nature overbroad, even though much classified information might be legitimately withheld. The same is true for directives that seek to restrict *all* unauthorized contact between officials and the media, or that discourage even the sharing of unclassified information. Moreover, contrary to international standards, US law does not adequately protect those who disclose official wrongdoing or information of great public interest. Under the Espionage Act, for example, it is unclear whether the public interest in a disclosure may ever be available as a defense to charges.[455]

The surveillance programs of the US government have dramatically compounded this already serious problem by making it significantly more challenging for third parties—journalists and the public at large—to seek out information that the government withholds but that is of strong public interest and value to a democratic society. In this context, at least three separate rights are thus threatened by the current surveillance regime in the US: the right of government officials to share information through the press with the public; the right of journalists to acquire and share information about the operations of the US government; and the right of the public to access that information through the media. If the government refuses to disclose or declassify this information itself as a matter of official policy, the least it can do is permit its officials, the press, and the public to exercise the right to impart or seek out information that cannot legitimately be withheld.[456] Through its consistent threat to pursue leak investigations, the US continues to impede the free exercise of that human right. And, as this report has shown, journalists and sources are afraid to disclose or discuss matters that should be legitimate topics of public debate because surveillance—combined with the harsh crackdown on leaks—increases the likelihood that the government will know about their conversations and may prosecute or otherwise sanction the participants.

---

[455] For more on this question, see, e.g., Laura Pitter (Human Rights Watch), "Dispatches: Snowden Case Highlights Need for Whistleblower Reform," January 7, 2014, http://www.hrw.org/news/2014/01/07/dispatches-snowden-case-highlights-need-whistleblower-reform; Human Rights Watch, "US: Protect National Security Whistleblowers," June 18, 2013, http://www.hrw.org/news/2013/06/18/us-protect-national-security-whistleblowers.

[456] Other portions of the Johannesburg Principles also support this conclusion. For example, "[p]rotection of national security may not be used as a reason to compel a journalist to reveal a confidential source." Johannesburg Principles, prin. 18. Additionally, expression can be punished, under the principles, only if it is "intended to incite imminent violence," "likely to incite such violence," and tightly connected to the "likelihood or occurrence of such violence." Johannesburg Principles, prin. 6.

Finally, the government has also run afoul of international standards by withholding from public view so many of the details about its surveillance programs. For example, the government has declined to make public many of its minimization procedures and whether they offer any genuine protection to journalists or lawyers in their interaction with sources and clients. Under the standards set forth in the Tshwane Principles and Johannesburg Principles, the US government ought to make public more information about its surveillance practices. Greater transparency would help to eliminate much of the uncertainty surrounding these programs, allowing for a more robust public debate about them, and possibly even helping to allay some of the fears described in this report.

US Constitutional Law

The First Amendment to the US Constitution establishes that "Congress shall make no law … abridging the freedom of speech, or of the press." It also recognizes the freedom of association.[457]

In interpreting the Constitution, the Supreme Court has identified a link between privacy, freedom of association, and freedom of expression. In *NAACP v. Alabama,* the Court held that Alabama could not compel the NAACP to turn over its roster of rank-and-file members because doing so, given past discrimination and hostility toward the NAACP, would likely result in "a substantial restraint upon the exercise by [the NAACP's] members of their right to freedom of association."[458] In reaching that conclusion, the Court underscored its recognition of "the vital relationship between freedom to associate and privacy in one's associations,"[459] and also observed that,

> Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly. [Citations omitted.] It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the "liberty" assured by the

[457] In the First Amendment to the US Constitution, the freedom to associate derives from the language guaranteeing "Congress shall make no law … abridging … the right of the people peaceably to assemble, and to petition the Government for redress of grievances." U.S. CONST. amend I.

[458] *Nat'l Ass'n for Advance. of Colored People v. Alabama*, 357 US 449, 462 (1958).

[459] Ibid. at 462.

> Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech.[460]

As for freedom of the press, the Supreme Court has held it is a "fundamental personal right[]," [461] though it is subject to limitations. For example, journalists may face liability for publishing inaccurate, defamatory items,[462] and may be subpoenaed to appear before grand juries.

Although there are some countries that penalize reporters who publish leaks of government secrets, the United States has not prosecuted reporters who published government secrets provided to them by government sources.[463] Some worry that journalists could be prosecuted under the Espionage Act of 1917, although there is also a strong argument that such prosecutions would require that the journalists act with specific intent to engage in espionage.

Yet the possibility that surveillance feeds the US government's crackdown on leaks still raises constitutional concerns for journalists. As documented above, these forces jointly undermine freedoms of the press by frightening away sources and restricting the ways in which journalists may gather information. Moreover, in leak prosecutions, journalists may be compelled to identify their sources, as evidenced by the current legal battle for *New York Times* reporter James Risen's testimony in the prosecution of Jeffrey Sterling.[464] Journalists may face imprisonment if they decline to testify when ordered to do so.[465]

---

[460] Ibid. at 460.

[461] For example, journalists may face liability for publishing inaccurate, defamatory items. *Lovell v. City of Griffin*, 303 U.S. 444, 450 (1938). They may also be subpoenaed to appear before grand juries.

[462] *Branzburg v. Hayes*, 408 U.S. 665, 683 (1972) ("Although it may deter or regulate what is said or published, the press may not circulate knowing or reckless falsehoods damaging to private reputation without subjecting itself to liability for damages, including punitive damages, or even criminal prosecution. See *New York Times Co.* v. *Sullivan*, 376 U.S. 254, 279-280 (1964); *Garrison v. Louisiana*, 379 U.S. 64, 74 (1964); *Curtis Publishing Co.* v. *Butts*, 388 U.S. 130, 147 (1967) (opinion of Harlan, J.,); *Monitor Patriot Co.* v. *Roy*, 401 U.S. 265, 277 (1971).").

[463] The case of Julian Assange could become an exception if the US were to act on threats made by some US officials. For more on Assange's case, see Ed Pilkington, "Julian Assange to file fresh challenge in effort to escape two-year legal limbo," *Guardian*, June 18, 2014, http://www.theguardian.com/media/2014/jun/18/julian-assange-fresh-challenge-legal-limbo-ecuador-embassy (accessed July 14, 2014).

[464] For more on Risen's situation, see Dylan Byers, "Supreme Court rejects James Risen appeal," *Politico*, June 2, 2014, http://www.politico.com/blogs/media/2014/06/supreme-court-rejects-james-risen-appeal-189558.html (accessed July 14, 2014); "US: Don't Press Charges Against New York Times Reporter," Letter from Kenneth Roth to Attorney General Holder, June 4, 2014, http://www.hrw.org/news/2014/06/04/us-don-t-press-charges-against-new-york-times-reporter.

[465] "US: Don't Press Charges Against New York Times Reporter," Letter from Kenneth Roth to Attorney General Holder, http://www.hrw.org/news/2014/06/04/us-don-t-press-charges-against-new-york-times-reporter.

Forcing journalists to choose between imprisonment and revealing their sources clearly (and in one sense, literally) undermines the freedom of the press, at best intimidating sources and journalists, and at worst (when paired with imprisonment of the source) resulting in tangible punishment for both. Surveillance exacerbates journalists' concerns that they will get "caught" doing their jobs and thus face a range of direct or indirect penalties.

The same factors also raise troubling First Amendment questions with respect to journalists' sources themselves, as they are also entitled to freedom of speech. While that freedom faces a range of limits, sources have a right to express their opinions about less sensitive matters,[466] and, in some circumstances, even about matters the government deems to be classified. Even if the government wishes to require its employees to sign non-disclosure agreements,[467] such agreements cannot be too broad. As one district court has put it, "while the scope of government employees' free speech rights may be in some ways narrower than those of private citizens, government employees do not relinquish their First Amendment rights at the door of public employment."[468] More recently, Supreme Court Justice Sonia Sotomayor, writing for a unanimous court, noted that "[s]peech by citizens on matters of public concern lies at the heart of the 1st Amendment. . . . This remains true when speech concerns information related to or learned through public employment."[469]

The DC Circuit Court of Appeals has outlined a balancing test for locating the limit of the government's ability to censor its employees, holding that "restrictions on the speech of government employees must 'protect a substantial government interest unrelated to the suppression of free speech.' … [and] the restriction must be narrowly drawn to 'restrict speech no more than is necessary to protect the substantial government interest.'"[470] In general, the government cannot legitimately prevent employees from disclosing unclassified information.[471]

---

[466] See generally, *Snepp v. US,* 444 U.S. 507 (1980). These restrictions can apply to the sharing of classified information, which federal employees often (if not always) agree to keep secret.

[467] For an example, see Department of Homeland Security, Non-Disclosure Agreement, http://www.fas.org/sgp/othergov/dhs-nda.pdf (accessed July 14, 2014).

[468] *Stillman v. Dep't of Defense*, 209 F. Supp. 2d 185, 217 (D.DC 2002).

[469] *Lane v. Franks*, 573 U. S. ____ (2014). For more on the case, see David G. Savage, "Supreme Court gives public workers 1st Amendment shield," *Los Angeles Times*, June 19, 2014, http://www.latimes.com/nation/la-na-supreme-court-public-employees-20140619-story.html (accessed July 14, 2014).

[470] *McGehee v. Casey*, 718 F.2d 1137, 1142-43 (DC Cir. 1983) (citations omitted).

[471] For example, one district court explicitly has recognized that former government employees have "a First Amendment right to publish unclassified information." *Stillman*, 209 F. Supp. 2d at 217. Indeed, as the DC Circuit has interpreted its own test, "[t]he

Moreover, employees at agencies that disapprove of unauthorized press contact have a particular interest in being able to speak with the press anonymously. According to the Supreme Court, First Amendment protections do indeed extend to some measure of anonymous speech.[472] In particular, the Court has rejected certain ordinances and statutes that require speakers to identify themselves when those identification requirements would "tend to restrict freedom to distribute information and thereby freedom of expression."[473]

Policies that seek to identify (and then punish) government officials for having contact with the press have the same effect. The increased leak prosecutions and the Insider Threat Program sharply curtail the ability of federal officials to express themselves, even with respect to unclassified information or mere opinions. Additionally, in the absence of clear information about how the government deploys surveillance information in its leak investigations, government sources harbor justifiable doubts about their ability to engage in constitutionally protected, anonymous contact with journalists without suffering administrative or legal penalties.

While such policies may be defensible or even desirable to the extent that they protect especially sensitive information, our research indicates that in practice they reach much further. Officials fear punishment for mere association with the press, as well as for sharing unclassified yet valuable information about the operation of the government. As a result, they are less willing to speak to reporters, undercutting the flow of information to the public, and limiting the freedom of expression enshrined in the US Constitution.

Rights Implicated by Surveillance's Impact on Attorneys

Both international human rights law and the US Constitution protect the right to counsel, which is commonly understood in both contexts to include the ability to communicate freely with one's legal counsel—especially in the context of criminal prosecution. That understanding reflects wide recognition that impediments to the exchange of information

---

government may not censor [unclassified materials or information obtained from public sources], 'contractually or otherwise…' [and t]he government has no legitimate interest in censoring unclassified materials." *McGehee*, 718 F.2d at 1141 (citations omitted).

[472] *Talley v. California*, 362 U.S. 60 (1960) (striking down a city ordinance that banned the distribution of any handbills omitting identifying information of the people who produced or distributed them); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) (striking down a similar state statute).

[473] *Talley*, 362 U.S. at 64.

between a defendant and his attorney can render the attorney's legal counsel ineffective, directly undermining the purpose of the right to counsel in the first place.

International Human Rights Law and Standards

The ICCPR provides that a person charged with a criminal offense is entitled "to defend himself in person or through legal assistance."[474] The treaty also defines a right for such a person "to communicate with counsel of his own choosing." It is well established in international human rights law, including in the interpretation of the ICCPR specifically, that full confidentiality of communications is a requirement of the right to counsel.[475]

By engaging in large-scale and sometimes entirely indiscriminate collection of data, the US government falls short of its obligations under the ICCPR to respect the relationship between attorneys and their clients. In gathering so much data, it inevitably picks up confidential legal information as well, including attorneys' domestic call records and the content of various other (typically international) messages and calls. As documented above, the mere fact that the government acquires and retains these materials, even if they are never used adversely, is enough to force lawyers toward more costly and less efficient practices, as they are under an obligation to keep that information confidential. In this way, the government's surveillance programs impede the ability of attorneys to "perform their professional functions without … hindrance … or improper interference."[476]

---

[474] ICCPR., art. 14(3)(d). It also provides for the right "to have legal assistance assigned to him, in any case where the interests of justice so require, and without payment by him in any such case if he does not have sufficient means to pay for it." Ibid.

[475] Human Rights Committee, General Comment 13, Article 14: Administration of justice, U.N. Doc. HRI/GEN/1/Rev.9 (2003) para. 9 (Interpreting the ICCPR as requiring "counsel to communicate with the accused in conditions giving full respect for the confidentiality of their communications," and noting, "[l]awyers should be able to counsel and to represent their clients in accordance with their established professional standards and judgement without any restrictions, influences, pressures or undue interference from any quarter."); see also Human Rights Committee, General Comment 32, Article 14: Right to equality before courts and tribunals and to a fair trial, CCPR/C/GC/32 (2007), para. 34 (noting, "Counsel should be able to meet their clients in private and to communicate with the accused in conditions that fully respect the confidentiality of their communications."). Numerous UN guidelines likewise require "full confidentiality" of communications. E.g., Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, adopted December 9, 1988, UN GAOR Res. 43/173 at 298, 43rd Session, 76th plenary meeting, UN Doc. A/43/49 (1988), principles 18(3)(4), 43 UN GAOR Supp. (Nº 49); Basic Principles on the Role of Lawyers, adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, August 27-September 7, 1990, U.N. Doc. A/CONF.144/28/Rev.1 at 118 (1990), principles 8, 22; Standard Minimum Rules for the Treatment of Prisoners, UN Economic and Social Council resolution 663 C (XXIV), July 31, 1957 and resolution 2076 (LXII), May 13, 1977, para. 93. See also Inter-American Commission on Human Rights, Principles and Best Practices on the Protection of Persons Deprived of Liberty in the Americas, 131st Sess. Mar. 3-14, 2008, principle 5.

[476] Basic Principles on the Role of Lawyers, adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August to 7 September 1990, U.N. Doc. A/CONF.144/28/Rev.1 at 118 (1990), http://www1.umn.edu/humanrts/instree/i3bprl.htm, principle 16. According to their own terms, these principles were "formulated to assist [UN] Member States in their task of promoting and ensuring the proper role of lawyers, should be

Further, a lawyer could well "reveal" confidential information improperly under the rules of professional responsibility if he or she takes inadequate steps to prevent that information from being picked up and stored in a government computer. Even if no unauthorized person actually reviews such information, at that point, the government has gained access to it. Moreover, the government cannot generally know if the information it has collected should be treated as confidential until it reviews it. Even treating information specially at that point, as the government may choose to do under various minimization procedures designed to protect US persons, will not undo the harm.[477] (Failure to treat confidential information specially might exacerbate the harm, however—for example, if the government were to share confidential information with prosecutors in the case against the defendant it concerns.) The salient solution is to engage in more narrow collection on the front end, specifically avoiding the collection of confidential information.

US Constitutional Law

The Sixth Amendment to the US Constitution also provides for a right to counsel.[478] A number of circuit courts have emphasized that the heart of this right encompasses the ability of defendants to communicate securely with their attorneys (though some limitations exist, especially for defendants in detention). For example, in *United States v. Rosner*, the Second Circuit held that "the essence of the Sixth Amendment right is, indeed, privacy of communication with counsel."[479] In *Caldwell v. United States*, the DC Circuit Court of Appeals observed that "high motives and zeal for law enforcement cannot justify spying upon and intrusion into the relationship between a person accused of crime and his counsel."[480] The Third Circuit offered a fuller explanation:

> The fundamental justification for the sixth amendment right to counsel is the presumed inability of a defendant to make informed choices about the preparation and conduct of his defense. Free two-way communication

---

respected and taken into account by Governments within the framework of their national legislation and practice." The terms of these principles, while not legally binding, are highly influential in defining the terms of US's human rights obligations under the ICCPR.

[477] For more on the government's treatment of attorney-client communications collected through surveillance, see Section IV, The Government's Rationale for Surveillance.

[478] Specifically, the Sixth Amendment stipulates that "In all criminal prosecutions, the accused shall enjoy the right …. to have the assistance of counsel for his defense." U.S. CONST. amend. VI.

[479] *United States v. Rosner*, 485 F.2d 1213, 1224 (2d Cir. 1973).

[480] *Caldwell v. United States*, 205 F.2d 879, 881 (DC Cir. 1953).

> between client and attorney is essential if the professional assistance guaranteed by the sixth amendment is to be meaningful.[481]

Given current US surveillance practices, countless defendants presently have justifiable reasons for doubting the security of their exchanges with counsel, especially (but by no means exclusively) if they are charged with offenses related to terrorism. Indeed, as this report documents, the situation has become so problematic that attorneys are feeling the need to issue new kinds of warnings to their clients about how they share sensitive information related to their cases. It is beyond the scope of this report for us to determine whether federal prosecutors have ever made use of intercepted confidential communications of defense counsel.[482] But surveillance practices are already interfering with trust and communication between attorneys and defendants, conflicting with the spirit of the right to counsel as articulated by numerous circuit courts and raising serious Sixth Amendment concerns.

---

[481] *United States v. Levy*, 577 F.2d 200, 209 (3d Cir. 1978). This principle, however, has limits. For example, in *Weatherford v. Bursey*, a case involving a confidential government informant who attended early meetings between the defendant and his attorney, the Supreme Court ruled that there was no violation of the defendant's Sixth Amendment rights. Significantly, a dissent by Justices Marshall and Brennan urged the court to adopt a strict *per se* prohibition on interference with the relationship between defendants and their attorneys. *Weatherford v. Bursey*, 429 US 545, 561 (1976) (Marshall, J., dissenting). One factor in the ruling was that the defendant had invited the informant to the meetings; another, more important for present purposes, is that the informant did not pass on relevant information to the prosecution. As the majority opinion phrased it: "As long as the information possessed by [the government's informant] remained uncommunicated [to the prosecution], he posed no substantial threat to [the defendant's] Sixth Amendment rights. Ibid., pp. 556-57. The situation attorneys and their clients face under large-scale electronic surveillance differs materially in several respects, but one difference is particularly relevant: neither the defendant in Weatherford nor his attorney had any reason to suspect government interference in their relationship because they did not know there was a government agent at the meetings; with large-scale electronic surveillance, both defendant and attorney have reason to fear their conversations are being recorded.

[482] Such a practice might very well violate the Constitution. See *Weatherford v. Bursey*, 429 US 545 (1976) (offering the relevant holding).

Recommendations

Everyone has the right to communicate with an expectation of privacy, including privacy from unwarranted or indiscriminate surveillance by governments. This right, which can be restricted only for important reasons such as national security, is essential not just to individual freedom of expression, but to the fair and accountable functioning of a democracy. This report documents the threats that surveillance poses to two professions, vital to a democratic society, that depend on freedom of expression and confidentiality of communications: journalism and law. Those threats are exacerbated by over-classification and excessive government secrecy.

Acknowledging the limits of our knowledge about the details of existing US surveillance programs, we urge the US Congress and the President to adopt the recommendations listed below to limit the government's surveillance activities, strengthen restrictions on the use of information collected through surveillance, increase transparency, and address problems linked to over-classification and leak investigations and prosecutions. The President has the power to make many of these changes unilaterally, and he should use that power without delay. Certain longer-term solutions will require a legislative response, and we urge Congress to act swiftly to provide one.

Narrow the Scope of Surveillance Authorities

International law—including, in particular, the ICCPR—requires that the United States ensure that any interference with the rights to privacy and freedom of expression comply with the principles of legality, proportionality, and necessity for a legitimate aim, such as national security. This is true regardless of the nationality of the individuals affected. Moreover, in circumstances where a state exercises effective control over an individual or that individual's exercise of rights, that state is also obliged to respect such rights even when the individual is located outside its territory.

Many US surveillance practices, as revealed since June 2013, are inconsistent with US obligations under international law and pose a particular threat to the rights to privacy and freedom of expression and access to information guaranteed by Articles 17 and 19 of the ICCPR. To bring its policies in line with the law, and to ensure the measure of privacy

necessary for journalists, lawyers, and others who require confidentiality to perform their responsibilities free from undue interference, the US should take the following steps:

- End mass collection of business records and other information.
    - Among other steps, Congress should pass and the President should sign legislation that would prohibit the mass or large-scale collection of communications metadata or other business records, whether under Section 215 or other authorities, such as pen register and trap and trace statutes. It should also ensure that any new legislation permit the acquisition of communications metadata only upon a showing of individualized suspicion. The President should also cease requesting authorization from the FISC for the large-scale acquisition of telephone metadata, or any other records. Finally, no requirement of compelled data retention for private companies should be imposed to substitute for present government collection and retention practices.
- Narrow the purposes for which all foreign intelligence surveillance may be conducted and limit such surveillance to individuals, groups, or entities who pose a tangible threat to national security or a comparable state interest.
    - Among other steps, Congress should pass legislation amending Section 702 of FISA and related surveillance authorities to narrow the scope of what can be acquired as "foreign intelligence information," which is now defined broadly to encompass, among other things, information related to "the conduct of the foreign affairs of the United States." It should be restricted to what is necessary and proportionate to protect legitimate aims identified in the ICCPR, such as national security. In practice, this should mean that the government may acquire information only from individuals, groups, or entities who pose a tangible threat to national security narrowly defined, or a comparable compelling state interest.
- Establish clear limits on the circumstances under which government agencies may share information collected for intelligence purposes with law enforcement for criminal investigations, and ensure that those limits are made public and are subject to review.

- Law enforcement agencies should not generally have access to databases collected by intelligence agencies, absent some decision by an independent tribunal that, by their terms, permissible law enforcement searches otherwise comply with constitutional and international law standards relating to criminal cases.

Strengthen the Protections Provided by Targeting and Minimization Procedures

Much of the anxiety caused by the government's surveillance programs stems from the permissiveness of the US government's targeting and minimization procedures, which provide weak protections for US persons, and virtually none at all for non-US persons. Those procedures appear to allow easy access to and long-term retention of information of no significant value to a compelling state interest. The US should strengthen the targeting and minimization procedures that protect the privacy of all those whose information is swept into the government's enormous databases. Toward that end, it should take the following steps:

- Require prior review of targeting decisions by a competent, independent, and impartial decisionmaker.
    - Under Section 702 and Executive Order 12,333, executive branch officials hold the power to make unilateral targeting decisions. Targeting decisions made under Executive Order 12,333 are not subject to any independent review. And under Section 702, only the broader procedures for making those decisions—designed to ensure that the government is targeting non-US persons outside the US—are subject to periodic approval of the Foreign Intelligence Surveillance Court. The lack of independent targeting oversight is even more worrisome because the standards for approving targets under Section 702 and Executive Order 12,333 are much lower than in the law enforcement context. Congress should pass (and the President should sign) legislation modifying Section 702 and the executive's authority under Executive Order 12,333 both to narrow the grounds for permissible surveillance (see above) and to require that individual targeting decisions be reviewed by an independent decisionmaker to ensure that any encroachment on any person's rights is fully justified under constitutional

and international law standards. Until such legislation takes effect, the Executive Branch should adopt targeting procedures that require individual targeting decisions to be approved by an independent decisionmaker.

- Prohibit the "backdoor" searches of communications collected, except pursuant to the same standards and procedures that would justify surveillance in the first instance.
    - Presently the government claims the power to search through the information it collects under Section 702 (and perhaps Executive Order 12,333) for the communications of individuals it could not have targeted in the first place. The government should prohibit such backdoor searches to cabin the harm that incidental or excessive collection can inflict.
- Require the prompt destruction of all information collected that is not to or from a target, or that does not contain information necessary to a legitimate aim (such as national security) furthered by surveillance of the target.
    - In particular, such information should be deleted from all government databanks rather than stored for a retention period (regardless of access). That deletion should be audited periodically by an independent authority that reports publicly on the government's retention and deletion practices.
- Prohibit the acquisition, retention, dissemination, or use of protected attorney–client communications or similarly confidential or privileged communications or information.
    - The NSA's current minimization procedures for attorney-client communications acquired under Section 702 are both too narrow and too weak. If the government finds itself reviewing a communication between an individual known to be indicted in the US and an attorney representing that person in connection with the indictment, it must stop reviewing the communication. But the government may retain the communication and preserve any foreign intelligence information it has already discerned. Moreover, there is no protection for the myriad other forms of privileged attorney-client communications—which include communications relating to

criminal proceedings that precede an indictment, criminal matters where the NSA does not yet know of an indictment, and civil matters—aside from the requirement that the NSA's Office of General Counsel review proposed dissemination of such communications. There is also no protection for confidential, as opposed to privileged, information related to ongoing legal representation. The Executive Branch should implement minimization procedures that require the government to delete confidential or privileged attorney communications it gathers through its surveillance programs, without retaining, disseminating, or otherwise using information gleaned from reviewing them.

Disclose Additional Information about Surveillance Programs to the Public

The secrecy surrounding US surveillance authorities has greatly hindered the public debate about the programs, and it has contributed to the uncertainty felt most acutely by those who rely heavily on the confidentiality of their communications, such as journalists and lawyers. To allow for a more meaningful public debate, and to permit the public to understand the true scope of the government's surveillance authorities, the United States should take the following steps:

- Publish detailed, unclassified descriptions of the scale and scope of signals intelligence conducted under all authorities, including Executive Order 12,333.
    - Among other steps, the Executive Branch should report statistics on the number of requests for information the government makes under Section 215, Section 702, and National Security Letters. Such reporting should include the total number of requests under specific legal authorities for specific types of data (content, subscriber information, or metadata), and the number of individuals affected by each as well as their status in the United States (citizens, residents, non-citizens). The President should also disclose detailed, unclassified descriptions of the scale and scope of signals intelligence collection practices pursuant to Executive Order 12,333 that affect both US persons and non-US persons, and clarify the extent to which foreign intelligence surveillance undertaken pursuant to Executive Order 12,333 implicates the private information of persons who are not

suspected of any wrongdoing or of any connection to a national security threat.

- Disclose all current and future targeting and minimization procedures for all agencies engaging in surveillance, subject to only those redactions necessary to protect ongoing investigations or sensitive sources and methods.
    - Uncertainty about the government's acquisition of information through its surveillance programs, and its subsequent treatment and use of that information, underlies much of the reluctance of journalists and lawyers to engage in certain types of communication and data storage. Publicizing significantly more information about how the government makes targeting decisions, as well as how it treats information it has gathered, is essential for allaying legitimate concerns about which activities are reasonably secure and which are not. The Executive Branch should promptly release all current targeting and minimization procedures with minimal redactions, and it should continue to release new, unredacted or minimally redacted procedures as they come into effect in the future.
- Declassify or publish detailed descriptions of all opinions of the Foreign Intelligence Surveillance Court, and establish an efficient means for doing so in a timely manner in the future.
- Allow recipients of surveillance orders, who are entrusted with the privacy and security of their users' data, regularly to report statistics concerning government requests for information, including:
    - The number of government requests for information about their users made under specific legal authorities such as Section 215 of the USA PATRIOT Act, Section 702 of FISA, the various National Security Letter statutes, and others;
    - The number of individuals, accounts, or devices for which information was requested under each authority;
    - The number of individuals, accounts, or devices affected by those requests under each authority; and

- The number of requests under each authority that sought communications content, basic subscriber information, and/or other information.

Reduce Government Secrecy and Restrictions on Official Contact with the Media

The government's tendency to over-classify information relating to its surveillance activities contributes significantly to the lack of transparency about those activities. Its efforts to protect all of that information, including by imposing strict restrictions on contact between federal officials and the press, are contributing to journalists' and sources' fear of surveillance and harming the ability of the press to report on matters of public concern. Accordingly, the US should take the following steps:

- Reform the classification system to prevent over-classification and to facilitate prompt declassification of information of public interest.
    - The Executive Branch should enact meaningful measures to combat over-classification. It should impose new limits on the types of information that may be classified, significantly shorten the period for which information may be classified,[483] and implement a process to identify and expedite the declassification review of information of significant public interest. It should also impose penalties on agencies or officials that engage in over-classification.
- Narrow administrative restrictions on the ability of government officials to talk with others about matters of public concern.
    - Among other steps, the President should order a review of the Insider Threat Program to ensure that it is not leading to harmful outcomes, including by allowing agencies to create policies that interfere with the ability of federal officials to interact with the press on matters that are unclassified or that do not pose any significant, tangible risk to national security or to other critical state interests recognized in international human rights law. The President should also direct the revocation of

[483] Mike German and Jay Stanley, ACLU, "Drastic Measures Required: Congress Needs to Overhaul U.S. Secrecy Laws and Increase Oversight of the Security Establishment," July 2011, https://www.aclu.org/files/assets/secrecyreport_20110727.pdf (accessed July 17, 2014), p. 48.

Intelligence Community Directive 119 to permit non-designated intelligence community employees contact with the press (subject to typical restrictions on sharing classified information), and to remove the requirement to report contact with the press. Congress should conduct oversight hearings on the implementation of the Insider Threat Program and other government policies and programs that may be improperly inhibiting government officials' communication with the media and restricting the public's access to information.

Enhance Protections for National-Security Whistleblowers

Those who disclose official wrongdoing or information of great public interest to the media perform an important service in a democratic society and should be protected. Similarly, journalists who report their disclosures should not be forced to divulge their sources. Even if a revelation does not point to a clear violation of the law, the public disclosure of that information should not be prosecuted—and a leaker should have a defense against prosecution for divulging classified or confidential information—where the public interest in that information outweighs the harm to a state interest such as national security. Accordingly, the US should take the following steps:

- Prohibit the prosecution of those who are not government employees or contractors for the receipt, possession, or public disclosure of classified information.
    - Journalism is not a crime, and treating it potentially as such discourages everyday reporting essential to understanding the operation of our government. The onus should be on the government to protect any legitimate secrets, not on journalists under the threat of serious criminal penalties. This would not insulate journalists from prosecution for other sorts of crimes, such as theft, hacking, or bribery.
- The public disclosure of information should not be prosecuted where the public interest in disclosure outweighs any specific harm to national security or a comparable state interest caused by disclosure.
    - The public disclosure of information is not espionage and should not be prosecuted as such. Moreover, to the extent criminal penalties are sought

for public disclosures, they should be available only for the disclosure of narrow categories of information defined by law, where disclosure would pose a real and identifiable risk of causing significant harm to national security or a comparable state interest. The law should also provide for a public interest defense in such cases. Under that defense, the public interest in disclosures relating to US government waste, fraud, corruption, or illegal activities should presumptively outweigh any legitimate interest in secrecy.

- Strengthen legal protections for national security whistleblowers, including contractors.
    - Strengthen federal law to provide intelligence and national security sector employees and contractors a) an enforceable right to report abuse internally and b) legal protection from retaliation if they do so, in addition to the public interest defense recommended above. Pending the enactment of legislative guarantees, the President should forbid retaliation and prosecution against such employees and contractors and provide an independent channel for challenging such actions should they occur.

Acknowledgments

This report was researched and written by G. Alex Sinha, Aryeh Neier fellow with the US Program at Human Rights Watch and the Human Rights Program at the American Civil Liberties Union. Maria McFarland Sanchez-Moreno, US Program deputy director at Human Rights Watch, participated in some of the research interviews. Andrea Prasow, deputy Washington Director at Human Rights Watch, also participated in one of the research interviews and provided key contacts. Significant research, proofreading, and formatting assistance were provided by Samantha Reiser, Paul Smith, and Jeanne Jeong, associates in the US Program at Human Rights Watch; as well as Alex Simon-Fox, Erin Weber, Cassandra Kildow, and Phoebe Young, interns in the US Program at Human Rights Watch. Other US Program staff—including Clara Long, Grace Meng, Alba Morales, and Brian Root—graciously offered contacts and insight.

This report was reviewed at Human Rights Watch by Maria McFarland Sanchez-Moreno, US Program deputy director; Alison Parker, US Program director; Cynthia M. Wong, senior researcher on the Internet and human rights; Laura Pitter, senior national security researcher; Dinah PoKempner, general counsel; and Joe Saunders, deputy program director. At the American Civil Liberties Union, it was reviewed by Steven Watt, Human Rights Program senior staff attorney; Jameel Jaffer, deputy legal director and Center for Democracy director; Alex Abdo, Speech, Privacy and Technology staff attorney; Naureen Shah, legislative counsel; Gabe Rottman, legislative counsel and policy advisor; Neema Singh Guliani, legislative counsel; Michael W. Macleod-Ball, Washington Legislative Office chief of staff. Layout, graphics, and production were coordinated by Grace Choi, publications director; Kathy Mills, publication specialist; and Fitzroy Hepkins, mail manager for Human Rights Watch.

Human Rights Watch and the American Civil Liberties Union wish to thank the journalists, attorneys, and others who generously shared their time—and in some cases, sensitive information about their experiences and practices—to ensure that this report properly captured their perspectives. We are especially grateful because many interviewees kindly fielded uncomfortable questions, which required them to lay bare their uncertainties about the adequacy of their professional practices for operating under the cloud of large-scale, electronic surveillance. Human Rights Watch and the American Civil Liberties Union would

also like to thank those government officials who spoke to us about delicate matters related to ongoing surveillance programs, as well as the public affairs officers and others who facilitated those conversations.

Appendix

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: 212-290-4700
Fax: 212-736-1300; 917-591-3452

April 17, 2014

Information and Privacy Coordinator
Central Intelligence Agency
Washington, D.C. 20505

Office of Freedom of Information
1155 Defense Pentagon
Washington, DC 20301-1155

Defense Intelligence Agency
ATTN: DAN-1A Rm E4-234
Washington, DC 20340-5100

Inspector General of the Department of Defense Chief, FOIA/PA Office
400 Army Navy Drive, Rm 201
Arlington, VA 22202-4704

National Geospatial-Intelligence Agency
General Counsel's Office, GCP Mail Stop D-10
4600 Sangamore Road
Bethesda, MD 20816-5003

National Reconnaissance Office
Information Access & Release Center
ATTN: FOIA Officer
14675 Lee Road
Chantilly, VA 20151-1715

National Security Agency
ATTN: FOIA Office (DJ4)
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

Carmen L. Mallon (as custodian of records for the Office of the Attorney General)
Chief of Staff
Office of Information Policy
Department of Justice
Suite 11050
1425 New York Avenue, N.W.
Washington, D.C. 20530-0001

Chief, FOIA/PA Unit
Criminal Division
Department of Justice
Suite 1127, Keeney Building
Washington, D.C. 20530-0001

Freedom of Information & Privacy Act Unit (SARF)
Drug Enforcement Administration
8701 Morrissette Drive
Springfield, VA 22152

FOIA Coordinator
Law and Policy Section
Environment and Natural Resources Division
Department of Justice
P.O. Box 7415, Ben Franklin Station
Washington, DC 20044-7415

Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843

FOIA Contact
Justice Management Division
Department of Justice
Room 1111, 950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001

FOIA/PA Coordinator
National Drug Intelligence Center
319 Washington Street, Fifth Floor
Johnstown, PA 15901-1622

Arnetta James
FOIA Initiatives Coordinator
National Security Division
Department of Justice
950 Pennsylvania Avenue, N.W., Room 6150
Washington, D.C. 20530-0001

Supervisory Paralegal
Office of Legal Counsel
Department of Justice
Room 5515, 950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001

Carmen L. Mallon (as custodian of records for the Office of Legal Policy)
Chief of Staff
Office of Information Policy
Department of Justice
Suite 11050
1425 New York Avenue, N.W.
Washington, D.C. 20530-0001

Office of Information Programs and Services
A/GIS/IPS/RL
U. S. Department of State
Washington, D. C. 20522-8100

Jennifer L. Hudson
Director, Information Management Division
Office of the Director of National Intelligence
Washington, D.C. 20511

Sent via FedEx

Re: Freedom of Information Act Request/Expedited Processing Request

To Whom It May Concern:

This letter constitutes a joint request ("Request") by Human Rights Watch ("HRW"), and the American Civil Liberties Union and the American Civil Liberties Foundation (collectively "ACLU"), under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and the applicable implementing regulations for documents concerning the

policies and procedures governing the acquisition, retention, dissemination, and use of information gathered as part of various government surveillance programs.

I. Background

Over the last several months, media reports have confirmed for the American people that much of their private information is susceptible to collection and use as part of surveillance programs operated by a variety of U.S. government agencies. On June 5, 2013, for example, The Guardian reported that the National Security Agency ("NSA") has been collecting all of the phone records of customers of a major telecommunications provider, Verizon Business Network Services ("Verizon").[1] Those records contain the "metadata"—which numbers are calling which, when, and for how long—of all Verizon calls that originate or terminate (or both) within United States.[2] The collection is authorized by the Foreign Intelligence Surveillance Court ("FISC") under Section 215 of the USA PATRIOT Act.[3] That program, often referred to as the "bulk telephony metadata program,"[4] was renewed as recently as January 2014.[5] We now know that the program has been authorized by the FISC since 2006, that it operated without FISC approval prior to 2006, and that it sweeps up the call records of customers of providers other than Verizon.[6]

On June 6, 2013, The Guardian disclosed the existence of another NSA program—called "PRISM"—which allows the NSA to obtain "'emails, chat conversations, voice calls, documents and more" from a variety of electronic communication service providers, such as Microsoft, Yahoo, and Google.[7] PRISM

---

[1] *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, GUARDIAN, Jun. 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-recordsverizon-court-order.

[2] *Id.*

[3] *Id.* A link to the FISC order is also available from the Guardian article. *See also* Emma Roller, *This Is What Section 215 of the Patriot Act Does*, SLATE (Jun. 7, 2013, 1:17 PM), http://www.slate.com/blogs/weigel/2013/06/07/nsa_prism_scandal_what_patriot_act_section_215_does.html. Note that Section 215 of the PATRIOT Act is also known as Section 501 of the Foreign Intelligence Surveillance Act ("FISA"). *DNI Clapper Declassifies Additional Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act*, IC ON THE RECORD (Jan. 17, 2014), http://icontherecord.tumblr.com/post/73652799309/dni-clapper-declassifies-additional-documents.

[4] Geoffrey Stone, *Is the NSA's Bulk Telephony Metadata Program Constitutional?*, THE HUFFINGTON POST (JAN. 3, 2014, 3:17 PM), http://www.huffingtonpost.com/geoffrey-r-stone/is-the-nsas-bulk-telephon_b_4538173.html.

[5] Press Release, Office of the Director of National Intelligence, Foreign Intelligence Surveillance Court Approves Government's Application to Renew Telephony Metadata Program (Jan. 3, 2014), http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/994-foreign-intelligence-surveillance-court-approves-government%E2%80%99s-application-to-renew-telephony-metadata-program.

[6] *See, e.g.,* RICHARD CLARK ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 17 (2013) [*hereinafter* PRESIDENT'S REVIEW GROUP], *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (referring to the government's storage of bulk telephony metadata but omitting reference to any specific service provider).

[7] Dominic Rush & James Ball, *PRISM Scandal: tech giants flatly deny allowing NSA direct access to*

operates under Section 702 of the FISA Amendments Act ("FAA"),[8] a law that gives the Director of National Intelligence and the Attorney General joint power to seek yearlong surveillance orders from the FISC that allow the government to target foreigners abroad without warrants, individualized suspicion, or judicial review.[9] While the FAA had already raised concerns that Americans' communications would be swept up "incidentally,"[10] the breadth of PRISM apparently surprised even the companies directly implicated in the program.[11]

On June 27, The Guardian reported that for much of the period between 2001 and 2011, the NSA gathered metadata on Americans' internet usage and email communications.[12] At least one aim of the program was to perform "contact-chaining"—discerning the identities of people who were linked to foreign intelligence targets by mutual contacts.[13] On November 18, the Director of National Intelligence declassified an opinion from the Foreign Intelligence Surveillance Court authorizing the program under the provisions of the Foreign Intelligence Surveillance Act governing the use of pen registers and trap-and-trace devices.[14]

On August 5, 2013, Reuters reported that the Drug Enforcement Administration ("DEA") has supported its work on routine drug investigations by drawing on a massive database comprising, in part, information gathered via NSA surveillance.[15] According to Reuters, the DEA alerts other law enforcement officials as to the need (for example) to stop and search particular vehicles.[16] Defendants who are arrested pursuant to such searches have been kept in the dark about the role that NSA surveillance played in their cases; indeed, sometimes even the prosecutors and judges do not know what triggered

---

servers, GUARDIAN (Jun. 6, 2013, 7:48 PM), http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining.

[8] Ewen MacAskill, *NSA paid millions to cover Prism compliance costs for tech companies*, GUARDIAN (Aug. 22, 2013, 10:34 AM), http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

[9] HUMAN RIGHTS WATCH, COMMENTS OF HUMAN RIGHTS WATCH TO THE PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, 5 (2013) [hereinafter COMMENTS OF HUMAN RIGHTS WATCH], *available at* http://www.hrw.org/news/2013/08/01/comments-human-rights-watch-privacy-and-civil-liberties-oversight-board-pclob.

[10] *See, e.g.*, Letter from ACLU to the U.S. Senators 2 (June 25, 2008), *available at* https://www.aclu.org/sites/default/files/images/general/asset_upload_file902_35782.pdf (expressing concern where the real target is abroad but an American is "on the other end of those communications").

[11] Rush & Ball, *supra* note 7.

[12] Glenn Greenwald & Spencer Ackerman, *NSA Collected US Email Records In Bulk For More Than Two Years Under Obama*, THE GUARDIAN (Jun. 27, 2013, 11:20 AM), http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

[13] *Id.*

[14] Orin Kerr, *Problems with the FISC's Newly-Declassified Opinion on Bulk Collection of Internet Metadata*, LAWFARE (Nov. 19, 2013, 2:35 AM), http://www.lawfareblog.com/2013/11/problems-with-the-fiscs-newly-declassified-opinion-on-bulk-collection-of-internet-metadata/. The opinion is available online as well. *See* No. PR/TT (FISA Ct.), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

[15] John Shiffman & Kristina Cooke, *Exclusive: U.S. directs agents to cover up program used to investigate Americans*, REUTERS, Aug. 5, 2013, *available at* http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

[16] *Id.*

these investigations.[17] The DEA has used this practice (known as "parallel construction") to prevent the fact of NSA involvement in routine drug cases from becoming known.[18]

On August 8, 2013, the New York Times reported that the NSA searches through the content of most emails as they enter or leave the United States.[19] According to the report, the NSA temporarily copies a substantial portion of all text-based communications entering or leaving the country, scans them for designated "selectors," saves the messages that contain those selectors, and deletes the rest.[20] The program—called UPSTREAM—operates under the FAA.[21]

On November 14, 2013, the New York Times reported that the CIA has also been using Section 215 of the PATRIOT Act, collecting business records pertaining to worldwide money transfers.[22] While details about the program remain scarce, the Times reported that purely domestic money transfers are exempt, while foreign transfers (as well as those originating or terminating within the U.S.) are not.[23]

On December 4, 2013, the Washington Post reported that the NSA "is gathering nearly 5 billion records a day on the whereabouts of cellphones around the world."[24] The records concern "hundreds of millions of devices," including location data on Americans' devices that are gathered "incidentally."[25] The article noted that "[a]nalysts can find cellphones anywhere in the world, retrace their movements and expose hidden relationships among the people using them."[26] The public does not know how the government handles domestic phone location data collected incidentally.

On March 11, 2014, the New York Times reported on a secret order by the FISC from 2002, known as the "Raw Take" order, which "weakened restrictions on sharing private information about Americans."[27] Before the order came down, only "narrow exceptions" permitted the agencies to share information without first "deleting irrelevant private details and masking the names of innocent Americans who came into contact with

---

[17] *Id.*
[18] *Id.*
[19] Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. TIMES, Aug. 8, 2013, http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all.
[20] *Id.*
[21] *Id.*
[22] Charlie Savage & Mark Mazzetti, *C.I.A. Collects Global Data on Transfers of Money*, N.Y. TIMES, Nov. 14, 2013, http://www.nytimes.com/2013/11/15/us/cia-collecting-data-on-international-money-transfers-officials-say.html?_r=0.
[23] *Id.*
[24] Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST, Dec. 4, 2013, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.
[25] *Id.*
[26] *Id.*
[27] Charlie Savage & Laura Poitras, *How a Court Secretly Evolved, Extending U.S. Spies' Reach*, N.Y. TIMES, (Mar. 11, 2014), http://www.nytimes.com/2014/03/12/us/how-a-courts-secret-evolution-extended-spies-reach.html?_r=0.

a terrorism suspect."[28] But the Raw Take order made it possible for "counterterrorism analysts at the NSA, the FBI and the CIA to share unfiltered personal information"—"unevaluated, unminimized information."[29] Further, "[t]he Raw Take order . . . also relaxed limits on sharing private information about Americans with foreign governments."[30] Indeed, citing the Raw Take order, the government in 2006 empowered specialists in designated NSA facilities to share information about Americans with foreign governments without first consulting the Attorney General, as formerly required.[31]

On March 18, 2014, the Washington Post reported that the NSA "has built a [voice interception] surveillance system capable of recording '100 percent' of a foreign country's telephone calls."[32] While the Post did not identify the country in question, it noted that the program—called "MYSTIC"—"enable[s] the agency to rewind and review conversations as long as a month after they take place" (using a search tool called "RETRO").[33] According to the article, the program may soon be extended to other countries.[34] Significantly, "large numbers of conversations involving Americans would be gathered from the country where RETRO operates."[35] Additionally, "[t]he NSA does not attempt to filter out . . . calls [involving Americans], defining them as communications 'acquired incidentally as a result of collection directed against appropriate foreign intelligence targets.'"[36]

On March 28, 2014, the Director of National Intelligence, James Clapper, confirmed that the NSA has executed warrantless searches of Americans' communications collected under Section 702 of FISA.[37] Clapper claimed that the "queries were performed pursuant to minimization procedures approved by the Fisa court and consistent with the statute and the fourth amendment."[38] In an article about Clapper's letter that appeared in The Guardian, Senator Ron Wyden characterized the legal authority for such searches as a "backdoor search loophole."[39] As that article noted, the

---

[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] Barton Gellman & Ashkan Soltani, *NSA surveillance program reaches 'into the past' to retrieve, replay phone calls*, WASH. POST (Mar. 18, 2014), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.
[33] *Id.* Both MYSTIC and RETRO are authorized under Executive Order 12,333. *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] Letter from James R. Clapper, Dir. Nat'l Intelligence, to Ron Wyden, Member, Senate Select Comm. on Intelligence (March 28, 2014), *available at* http://www.wyden.senate.gov/download/?id=130BFF88-A3C0-4315-A23B-C4F96C499D9D&download=1.
[38] *Id.*
[39] Spencer Ackerman & James Ball, *NSA performed warrantless searches on Americans' calls and emails – Clapper*, GUARDIAN (Apr. 1, 2014), http://www.theguardian.com/world/2014/apr/01/nsa-surveillance-loophole-americans-data.

media have already reported on this "back door," but Clapper's confirmation "drew greater attention to the issue."[40]

* * *

Collectively, these revelations reveal a growing surveillance state, implicating the privacy of countless American citizens and residents. The government has frequently defended the programs by claiming that secret procedures protect the rights of innocent individuals whose data or communications are swept up by the government's surveillance. But little information regarding those limitations is public, and what information is public gives cause only for greater concern.

For example, the so-called "minimization procedures" relied upon by the NSA in conducting surveillance under Section 702 of the FISA Amendments Act contain broad exceptions permitting the NSA to store the communications of innocent American citizens and residents.[41] The procedures even permit the NSA to collect and store communications protected by the attorney-client privilege and to search its vast databases for communications of or about specific U.S. persons.[42]

The public has access to a handful of other procedures governing the acquisition, retention, dissemination, and use of information gathered under the government's various surveillance programs.[43] But the information released to date provides, at best, an

---

[40] *Id.*

[41] Glenn Greenwald & James Ball, *The Top Secret Rules that Allow NSA to Use US Data Without a Warrant*, THE GUARDIAN (Jun. 20, 2013 6:39 PM), http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.

[42] *See generally 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*, DIRECTOR OF NATIONAL INTELLIGENCE, http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf; *Procedure used by NSA to target non-US persons: Exhibit A – full document*, GUARDIAN (Jun. 20, 2013, 2:35 PM), http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document; *Procedure used by NSA to target non-US persons: Exhibit B – full document*, GUARDIAN (Jun. 20, 2013, 2:35 PM), http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document.

[43] The government has partially declassified several versions of United States Signals Intelligence Directive 18. NATIONAL SECURITY AGENCY, PROCEDURES FOR MONITORING RADIO COMMUNICATIONS OF SUSPECTED INTERNATIONAL NARCOTICS TRAFFICKERS (1986), *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018%20Annex%20J.pdf; Ex. C: Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism, Docket No. BR 06-05 28 (FISA Ct. 1993), *available at* http://www.dni.gov/files/documents/1118/CLEANED016.%20REDACTED%20BR%2006-05%20Exhibits%20C%20%28Memo%20of%20Law%29%20and%20D-Sealed.pdf (attached to the pleading); NATIONAL SECURITY AGENCY, LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES (2011), *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf. It has also released the 2003 minimization procedures for FBI collection under Section 215. *In re* the Matter of the Application of the U.S. for an Order Authorizing the Production of Any Tangible Things (U), Docket No. BR 06-09 (FISA Ct. Sept. 5, 2006), *available at* http://www.dni.gov/files/documents/1118/CLEANED95.pdf. Additionally, it has released NSA training materials that mention minimization procedures—none of which are more recent than 2009. *See* Jan. 8, 2007 PowerPoint on Metadata Obtained Pursuant to FISA,

incomplete account of the procedures in place that purportedly safeguard the right to privacy of innocent individuals ensnared by the government's surveillance practices.

Moreover, the sheer breadth of the government's surveillance authority and the correspondingly weak protection in place for innocent individuals (based on what is publicly known thus far) undermine the freedoms of expression and association guaranteed by the First Amendment. Nonetheless, the government has yet to provide meaningful explanation as to what constraints—if any—it believes the First Amendment imposes on its surveillance practices.

Accordingly, this Request seeks records pertaining to the policies and procedures governing the acquisition, retention, dissemination, and use of information gathered by the government through ongoing surveillance programs. Relatedly, it also seeks records concerning the limitations that the government believes the First Amendment imposes on its surveillance practices.

II. Records Requested

1. Minimization policies and procedures addressing the acquisition, retention, dissemination, or use of information gathered pursuant to:
    a. any provision of the Foreign Intelligence Surveillance Act, as amended;
    b. Executive Order 12,333;
    c. the cell phone location program disclosed by the Washington Post;[44]
    d. the various statutes authorizing the issuance of "national security letters";[45] and
    e. any authority relied upon by the government to conduct "bulk collection" of information (as the government or the Foreign Intelligence Surveillance

---

NATIONAL SECURITY AGENCY, http://www.odni.gov/files/documents/1118/CLEANED049.%20%20OVSC1204%20v1OGCAprl15.pdf (last visited Feb. 5, 2014) (designed for use by NSA personnel with access to the bulk telephony metadata acquired by NSA pursuant to Section 501 of FISA, for purposes of performing analytical functions); Aug. 2009 PowerPoint for NSA Cryptological School Course on Legal, Compliance, and Minimization Procedures, NATIONAL SECURITY AGENCY, http://www.dni.gov/files/documents/1118/CLEANED021.extracts.%20Minimization%20Pr...cted%20from%20file%20021-Sealed.pdf (last visited Feb. 5, 2014) (designed for NSA personnel, these materials provided access to bulk telephony and electronic communications metadata acquired pursuant to Section 501 of FISA and Section 402 of FISA respectively); Jan. 8, 2007 Web-based Training Slides on Bulk Telephony Metadata Program pursuant to Section 501 of FISA, http://www.dni.gov/files/documents/1118/CLEANED032.%20Basket%202%20-%20NSA%20training.log.pdf (last visited Feb. 5, 2014).

[44] *See* Barton Gellman & Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show*, WASH. POST, Dec. 4, 2013, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

[45] 12 U.S.C. § 3414 (2006); 15 U.S.C. § 1681u (2006); 15 U.S.C. § 1681v (2006); 18 U.S.C. § 2709 (2006); 50 U.S.C. § 3162 (2014).

Court has used that term[46]).

2. All records addressing or discussing which limitations (if any) are or should be imposed by the First Amendment to the U.S. Constitution on the acquisition, retention, dissemination, or use of information under the authorities listed in 1(a)-(e) above.

3. Training or briefing materials referring to any records captured by (1) and/or (2) above.

4. Manuals, memoranda, correspondence, or other records defining or elaborating on terminology from, standards in, or exceptions to any minimization policies or procedures captured by (1) or (2) above.

We request that responsive electronic records be provided electronically in their native file format, if possible. *See* 5 U.S.C. § 552(a)(3)(B). Alternatively, we request that the records be provided electronically in a text-searchable, static-image format (PDF), in the best image quality in the agencies' possession, and that the records be provided in separate, Bates-stamped files.

We also request that you provide an estimated date on which you will complete the processing of this request. *See* 5 U.S.C. § 552(a)(7)(B).

III. Request for Expedited Processing

We request expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E) and 22 C.F.R. § 171.12(b), 28 C.F.R. § 16.5(d), 32 C.F.R. § 299.5(f), and 32 C.F.R. § 286.4(d)(3). There is a "compelling need" for these records because the information requested is urgently needed by two organizations primarily engaged in disseminating information in order to inform the public about actual or alleged Federal government activity. 5 U.S.C. § 552(a)(6)(E)(v); *see also* 22 C.F.R. § 171.12(b); 28 C.F.R. § 16.5(d); 32 C.F.R. § 299.5(f); 32 C.F.R. § 286.4(d).

A. Both HRW and the ACLU are organizations primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.

Both HRW and the ACLU are "primarily engaged in disseminating information" within the meaning of the statute and regulations. 5 U.S.C. § 552(a)(6)(E)(v)(II); 22

[46] *See, e.g.*, *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013); *In re* Production of Tangible Things from [Redacted], No. BR 0813, 2009 WL 9150913 (FISA Ct. Mar. 2, 2009).

C.F.R. § 171.12(b)(2); 28 C.F.R. § 16.5(d)(1)(ii); 32 C.F.R. § 299.5(f)(2); 32 C.F.R. 286.4(d)(3)(ii). Obtaining information about government activity, analyzing that information, and widely publishing and disseminating that information to the press and public is a critical and substantial component of the work of both organizations, and one of their primary activities. See ACLU v. Dep't of Justice, 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding non-profit public interest group that "gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience" to be "primarily engaged in disseminating information" (internal citation omitted)).[47] Both organizations disseminate this information to educate the public and promote the protection of civil liberties and human rights.

HRW's primary method of advocacy is conducting investigations and publishing its findings in reports in order to generate publicity and influence policy. HRW publishes in depth reports and up-to-the-minute information concerning human rights issues around the world, including inside the United States,[48] and its findings are often discussed in newspapers and other news media in addition to in its own publications.[49] Additionally, HRW issues press releases[50] and publishes several op-eds on a weekly basis drawing public attention to human rights issues inside the United States.[51] The reports, articles and public comments that HRW publishes on these matters are available on the HRW website, which had 10.2 million visitors in 2013.[52] HRW also provides multimedia features presenting our findings on our YouTube channel, which had over 5 million views in 2013. In that year, HRW produced 62 such multimedia features, including one feature that was viewed more than 3 million times in the single month of February 2014.[53]

---

[47] *See also Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005) (finding Leadership Conference—whose mission is "to serve as the site of record for relevant and up-to-the-minute civil rights news and information" and to "disseminate[] information regarding civil rights and voting rights to educate the public [and] promote effective civil rights laws"—to be "primarily engaged in the dissemination of information").

[48] *U.S. Domestic Policy*, HUMAN RIGHTS WATCH, http://www.hrw.org/en/united-states/us-program (last visited Mar. 10, 2014).

[49] From January 1, 2011, to January 1, 2012, Human Rights Watch appeared in Agence France Press 1,800 times, Reuters News 681 times, Associated Press Newswires 565 times, All Africa 1,152 times, CNN Newswire 712 times, BBC News 410 times, *The Guardian* (UK) 310 times, and *The New York Times* 255 times. Additionally, Human Rights Watch often appears in major US papers such as *The Washington Post, The Wall Street Journal, USA Today, The Pittsburgh Post-Gazette, The Los Angeles Times, The Chicago Tribune, The Houston Chronicle*, and others. Internationally, Human Rights Watch has been cited by *The International Herald Tribune, Der Spiegel* (Germany), *The Toronto Star* (Canada), *The Jakarta Post* (Indonesia), *El Pais* (Spain), *Le Monde* (France), *The Sydney Morning Herald*(Australia), *The Times* (London), *Le Progres Egyptien* (Egypt), *Mail and Guardian* (South Africa), *The Ottowa Citizen* (Canada), as well as hundreds of other print news sources around the world.

[50] *U.S. Domestic Policy: News Releases*, HUMAN RIGHTS WATCH, http://www.hrw.org/by-issue/news-filter/579?date_filter%5Bvalue%5D%5Byear%5D=2013 (last visited Mar. 10, 2014).

[51] *U.S. Domestic Policy: Commentaries*, HUMAN RIGHTS WATCH, http://www.hrw.org/by-issue/commentaries/ (last visited Mar. 10, 2014).

[52] HUMAN RIGHTS WATCH, http://www.hrw.org (last visited Mar. 10, 2014).

[53] *Russia: Gay Men Beaten on Camera*, HUMAN RIGHTS WATCH (Feb. 3, 2014), https://www.youtube.com/watch?v=zMTbFSJ_Tr4.

HRW's regular means of disseminating and editorializing information obtained through FOIA requests include our investigatory reports published on our website, as well as updates posted to the organization's 2 million followers in social media, including 950,000 Twitter followers and 758,000 Facebook fans. HRW has published numerous analyses of data obtained from the US government under FOIA, including investigations of US Immigration and Customs Enforcement deportation and detention practices and investigations of police department practices.[54] Moreover, HRW has published analysis of data obtained under state public records requests examining a variety of policy issues, including the practices of police departments and courts, and the implementation of state sentencing laws.[55] HRW also uses visualization tools to highlight the findings of our analysis of data obtained under FOIA.[56]

This Request is made for the purpose of obtaining information that will be used to supplement an HRW report regarding surveillance in the United States. The release of the report will be timed to inform ongoing Congressional debate on surveillance practices. HRW will work with other organizations to disseminate the information, to generate publicity in tandem with others, and to generate a maximum amount of public awareness using the many tools described above. In order to do this, it is essential that we be able to begin to work with the disclosed information as soon as possible. If we are unable to do this within this time frame, our ability to inform the public about this aspect of government activities will be seriously and irreparably harmed.

The ACLU's regular means of disseminating and editorializing information obtained through FOIA requests include: a paper newsletter distributed to approximately 450,000 people; a bi-weekly electronic newsletter distributed to approximately 300,000 subscribers; published reports, books, pamphlets, and fact sheets; a widely read blog; heavily visited websites, including an accountability microsite, http://www.aclu.org/accountability; and a video series.

The ACLU also regularly issues press releases to call attention to documents obtained through FOIA requests, as well as other breaking news.[57] ACLU attorneys are

---

[54] *Forced Apart (By the Numbers),* HUMAN RIGHTS WATCH (Apr. 15, 2009), http://www.hrw.org/reports/2009/04/15/forced-apart-numbers-0; *A Costly Move,* HUMAN RIGHTS WATCH (Jun. 14, 2011), http://www.hrw.org/reports/2011/06/14/costly-move-0; *Capitol Offense,* HUMAN RIGHTS WATCH (Jan. 24, 2013), http://www.hrw.org/reports/2013/01/24/capitol-offense-0.

[55] *The Price of Freedom*, HUMAN RIGHTS WATCH (Dec. 3, 2010), http://www.hrw.org/node/91360; http://www.hrw.org/reports/2010/12/02/price-freedom-0; *When I Die, They'll Send Me Home*, HUMAN RIGHTS WATCH (Oct. 17, 2008), http://www.hrw.org/reports/2008/10/17/when-i-die-they-ll-send-me-home.

[56] *A Costly Move*, HUMAN RIGHTS WATCH, http://www.hrw.org/features/a-costly-move/main-dashboard (last accessed Mar. 10, 2014).

[57] *See, e.g.*, Press Release, American Civil Liberties Union, Documents Show FBI Monitored Bay Area Occupy Movement (Sep. 14, 2012), http://www.aclu.org/node/36742; Press Release, American Civil Liberties Union, FOIA Documents Show FBI Using "Mosque Outreach" for Intelligence Gathering (Mar. 27, 2012), http://www.aclu.org/national-security/foia-documents-show-fbi-using-mosque-outreach-intelligence-gathering; Press Release, American Civil Liberties Union, FOIA Documents Show FBI Illegally Collecting Intelligence Under Guise of "Community Outreach" (Dec. 1, 2011), http://www.aclu.org/national-security/foia-documents-show-fbi-illegally-collecting-intelligence-under-guise-community; Press Release, American Civil Liberties Union, FOIA Documents from FBI Show

interviewed frequently for news stories about documents released through ACLU FOIA requests.[58]

The ACLU website specifically includes features on information about actual or alleged government activity obtained through FOIA.[59] For example, the ACLU maintains an online "Torture Database," a compilation of over 100,000 pages of FOIA documents that allows researchers and the public to conduct sophisticated searches of FOIA documents relating to government policies on rendition, detention, and interrogation.[60] In addition to websites, the ACLU has produced an in-depth television series on civil liberties, which has included analysis and explanation of information the ACLU has obtained through FOIA.

The ACLU has also published a number of charts that collect, summarize, and analyze information it has obtained through FOIA. For example, through compilation and analysis of information gathered from various sources—including information obtained from the government through FOIA—the ACLU has created an original chart that provides the public and news media with a comprehensive index of Bush-era Office of

---

Unconstitutional Racial Profiling (Oct. 20, 2011), http://www.aclu.org/national-security/foia-documents-fbi-show-unconstitutional-racial-profiling; Press Release, American Civil Liberties Union, Documents Obtained by ACLU Show Sexual Abuse of Immigration Detainees is Widespread National Problem, (Oct. 19, 2011), http://www.aclu.org/immigrants-rights-prisoners-rights-prisoners-rights/documents-obtained-aclu-show-sexual-abuse; Press Release, American Civil Liberties Union, New Evidence of Abuse at Bagram Underscores Need for Full Disclosure About Prison, Says ACLU (Jun. 24, 2009), http://www.aclu.org/national-security/new-evidence-abuse-bagram-underscores-need-full-disclosure-about-prison-says-aclu.

[58] *See, e.g.*, Carrie Johnson, *Delay in Releasing CIA Report Is Sought; Justice Dep't Wants More Time to Review IG's Findings on Detainee Treatment*, WASH. POST, June 20, 2009 (quoting ACLU staff attorney Amrit Singh); Peter Finn & Julie Tate, *CIA Mistaken on 'High-Value' Detainee, Document Shows*, WASH. POST, June 16, 2009 (quoting ACLU staff attorney Ben Wizner); Scott Shane, *Lawsuits Force Disclosures by C.I.A.*, N.Y. TIMES, June 10, 2009 (quoting ACLU National Security Project director Jameel Jaffer); Joby Warrick, *Like FBI, CIA Has Used Secret 'Letters,'* WASH. POST, Jan. 25, 2008 (quoting ACLU staff attorney Melissa Goodman).

[59] *See, e.g.*, *Predator Drones FOIA*, AMERICAN CIVIL LIBERTIES UNION, http://www.aclu.org/national-security/predator-drone-foia; http://www.aclu.org/national-security/anwar-al-awlaki-foia-request (last visited Mar. 10, 2014); *Accountability for Torture*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/accountability-torture (last visited Apr. 7, 2014); *Index of Bush-Era OLC Memoranda Relating to Interrogation, Detention, Rendition and/or Surveillance*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/sites/default/files/pdfs/safefree/olcmemos_2009_0305.pdf (last visited Apr. 7, 2014); *Mapping the FBI: Uncovering Abusive Surveillance and Racial Profiling*, AMERICAN CIVIL LIBERTIES UNION, http://www.aclu.org/mappingthefbi (last visited Mar. 10, 2014); *Bagram FOIA*, AMERICAN CIVIL LIBERTIES UNION, http://www.aclu.org/national-security/bagram-foia (last visited Mar. 10, 2014); *CSRT FOIA*, AMERICAN CIVIL LIBERTIES UNION (Mar. 13, 2008) https://www.aclu.org/national-security/csrt-foia; *ACLU v. DOJ – Lawsuit to Enforce NSA Warrantless Surveillance FOIA Request*, AMERICAN CIVIL LIBERTIES UNION (Mar. 13, 2013), http://www.aclu.org/safefree/nsaspying/30022res20060207.html; *Patriot FOIA*, AMERICAN CIVIL LIBERTIES UNION (Aug. 10, 2004), http://www.aclu.org/patriotfoia; *Spy Files*, AMERICAN CIVIL LIBERTIES UNION, http://www.aclu.org/spyfiles (last visited Mar. 10, 2014); *National Security Letters FOIA*, AMERICAN CIVIL LIBERTIES UNION (Oct. 11, 2007), http://www.aclu.org/safefree/nationalsecurityletters/32140res20071011.html; and *Ideological Exclusion*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/national-security/ideological-exclusion (last visited Apr. 7, 2014).

[60] *The Torture Database*, AMERICAN CIVIL LIBERTIES UNION, http://www.torturedatabase.org (last visited Apr. 7, 2014).

Legal Counsel memos relating to interrogation, detention, rendition and surveillance.[61] That chart describes what is publicly known about the memos and their conclusions, who authored them and for whom, and whether the memos remain secret or have been released to the public in whole or in part.[62] Similarly, the ACLU produced a chart of original statistics about the Defense Department's use of National Security Letters based on its own analysis of records obtained through FOIA.[63]

HRW and the ACLU plan to analyze and disseminate to the public the information gathered through this Request. The records requested are not sought for commercial use, and the Requesters plan to disseminate the information disclosed as a result of this Request to the public at no cost.[64]

B. The records sought are urgently needed to inform the public about actual or alleged government activity.

The records sought are urgently needed to inform the public about actual or alleged federal government activity. *See supra* Part I. The requested records relate to a "breaking news story of general public interest," 22 C.F.R.§ 171.12(b)(2)(i), 32 C.F.R. 286.4(d)(3)(ii)(A), are "a matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence,"28 C.F.R. § 16.5(d)(1)(iv), and are also "urgently needed" to inform the public about an "actual or alleged federal government activity." 22 C.F.R. § 171.12(b)(2)(i)–(ii); 28 C.F.R. § 16.5(d)(1)(ii); 32 C.F.R. § 299.5(f)(2); 32 C.F.R. § 286.4(d)(3)(ii).

As discussed above, the breadth of the government's surveillance activities has been a significant matter of public concern since at least June of 2013. The records sought would illuminate the government's measures for minimizing the acquisition, dissemination, retention, and use of Americans' personal data. That information is essential to allay the justifiable concerns of the public in its exercise of the core constitutional rights protected by the First Amendment.

* * *

---

[61] *Index of Bush-Era OLC Memoranda Relating to Interrogation, Detention, Rendition and/or Surveillance*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/sites/default/files/pdfs/safefree/olcmemos_2009_0305.pdf (last visited Apr. 7, 2014).

[62] *Id.*

[63] *Statistics on NSLs Produced by Department of Defense*, AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/files/assets/nsl_stats.pdf (last visited Apr. 7, 2014).

[64] In addition to the national ACLU offices, there are 53 ACLU affiliate and national chapter offices located throughout the United States and Puerto Rico. These offices further disseminate ACLU material to local residents, schools, and organizations through a variety of means, including their own websites, publications, and newsletters. Further, the ACLU makes archived materials available at the American Civil Liberties Union Archives at Princeton University Library.

Accordingly, expedited processing should be granted.

IV. Application for Waiver or Limitation of Fees and Costs

A. Release of the records is in the public interest.

We request a waiver of document search, review, and duplication fees on the grounds that disclosure of the requested records is in the public interest and because disclosure is "likely to contribute significantly to public understanding of the operations or activities of the [Government] and is not primarily in the commercial interest of the requester." *See* 5 U.S.C. § 552(a)(4)(A)(iii); 22 C.F.R. § 171.17(a); 28 C.F.R. § 16.11(k); 32 C.F.R. § 286.28(d).

As discussed above, numerous news accounts reflect the considerable public interest in the records we seek. Given the ongoing and widespread media attention to this issue, the records sought in the instant Request will significantly contribute to public understanding of the degree to which First Amendment rights are secure under the current surveillance regime.

In addition, disclosure is not in the commercial interest of HRW or the ACLU. As described above, any information disclosed by either organization as a result of this FOIA request will be available to the public at no cost. Thus, a fee waiver would fulfill Congress' legislative intent in amending FOIA. *See Judicial Watch Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) ("Congress amended FOIA to ensure that it be 'liberally construed in favor of waivers for noncommercial requesters.'") (citation omitted).

B. HRW and the ACLU qualify as representatives of the news media.

We also request a waiver of all fees other than document reproduction fees, excluding the first 100 pages, on the grounds that HRW and the ACLU both qualify as "representative[s] of the news media" and the records are not sought for commercial use. 22 C.F.R. § 171.15(c); 28 C.F.R. § 16.11(d); 32 C.F.R. 286.28(e)(7). Accordingly, fees associated with the processing of this request should be "limited to reasonable standard charges for document duplication." 5 U.S.C. § 552(a)(4)(A).

HRW and the ACLU each meet the statutory and regulatory definitions of a "representative of the news media" because each is an "entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience." 5 U.S.C. § 552(a)(4)(A)(ii)(II); *see also Nat'l Sec. Archive v. Dep't of Def.*, 880 F.2d 1381, 1387 (D.C. Cir. 1989); *cf. Am. Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding non-profit public interest group to be "primarily engaged in

disseminating information"). HRW and the ACLU are both "representative[s] of the news media" for the same reasons that they are "primarily engaged in the dissemination of information." *See Elec. Privacy Info. Ctr. v. Dep't of Def.*, 241 F. Supp. 2d 5, 10–15 (D.D.C. 2003) (finding non-profit public interest group that disseminated an electronic newsletter and published books was a "representative of the news media" for FOIA purposes).[65] Indeed, the ACLU recently was held to be a "representative of the news media." *Serv. Women's Action Network v. Dep't of Defense*, No. 3:11CV1534 (MRK), 2012 WL 3683399, at *3 (D. Conn. May 14, 2012). *See also Am. Civil Liberties Union of Wash. v. Dep't of Justice*, No. C09–0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding ACLU of Washington to be a "representative of the news media"), *reconsidered in part on other grounds*, 2011 WL 1900140 (W.D. Wash. May 19, 2011).

Notably, courts have found other organizations whose mission, function, publishing, and public education activities are similar in kind to HRW's and the ACLU's to be "representatives of the news media." *See, e.g.*, *Elec. Privacy Info. Ctr. v. Dep't of Defense*, 241 F. Supp. 2d 5, 10-15 (D.D.C. 2003) (finding non-profit public interest group that disseminated an electronic newsletter and published books was a "representative of the media" for purposes of FOIA); *Nat'l Security Archive*, 880 F.2d at 1387; Judicial Watch, Inc. v. Dep't of Justice, 133 F. Supp. 2d 52, 53-54 (D.D.C. 2000) (finding Judicial Watch, self-described as a "public interest law firm," a news media requester).[66]

---

[65] On account of these factors, fees associated with responding to FOIA requests are regularly waived for the ACLU. In June 2011, the National Security Division of the Department of Justice granted a fee waiver to the ACLU with respect to a request for documents relating to the interpretation and implementation of a section of the PATRIOT Act. In October 2010, the Department of the Navy granted a fee waiver to the ACLU with respect to a request for documents regarding the deaths of detainees in U.S. custody. In January 2009, the CIA granted a fee waiver with respect to the same request. In March 2009, the State Department granted a fee waiver to the ACLU with regard to a FOIA request submitted in December 2008. The Department of Justice granted a fee waiver to the ACLU with regard to the same FOIA request. In November 2006, the Department of Health and Human Services granted a fee waiver to the ACLU with regard to a FOIA request submitted in November of 2006. In May 2005, the U.S. Department of Commerce granted a fee waiver to the ACLU with respect to its request for information regarding the radio-frequency identification chips in United States passports. In March 2005, the Department of State granted a fee waiver to the ACLU with regard to a request regarding the use of immigration laws to exclude prominent non-citizen scholars and intellectuals from the country because of their political views, statements, or associations. In addition, the Department of Defense did not charge the ACLU fees associated with FOIA requests submitted by the ACLU in April 2007, June 2006, February 2006, and October 2003. The Department of Justice did not charge the ACLU fees associated with FOIA requests submitted by the ACLU in November 2007, December 2005, and December 2004. Finally, three separate agencies—the Federal Bureau of Investigation, the Office of Intelligence Policy and Review, and the Office of Information and Privacy in the Department of Justice—did not charge the ACLU fees associated with a FOIA request submitted by the ACLU in August 2002.

[66] Courts have found these organizations to be "representatives of the news media" even though they engage in litigation and lobbying activities beyond their dissemination of information/public education activities. *See, e.g.*, *Elec. Privacy Info. Ctr. v. U.S. Dept. of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003); *Nat'l Sec. Archive v. U.S. Dept. of Defense*, 880 F.2d 1381, 1387 (D.C. Cir. 1989); *see also Judicial Watch, Inc v. U.S. Dept. of Justice*, 133 F. Supp. 2d 52, 53-54 (D.D.C. 2000). *See also*, *Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005) (finding Leadership Conference to be primarily engaged in disseminating information even though it engages in substantial amounts of legislative advocacy beyond its publication and public education functions).

* * *

Pursuant to the applicable regulations and statute, we expect the determination regarding expedited processing within 10 calendar days. *See* 5 U.S.C. § 552(a)(6)(E)(ii)(I).

If the Request is denied in whole or in part, we ask that you justify all withholdings by reference to specific exemptions to FOIA. We expect the release of all segregable portions of otherwise exempt material. We reserve the right to appeal a decision to withhold any information or to deny a waiver of fees.

Thank you for your prompt attention to this matter. Please furnish all applicable records to:

G. Alex Sinha
Human Rights Watch
350 Fifth Avenue – 34th Floor
New York, NY 10118

I affirm that the information provided supporting the request for expedited processing is true and correct to the best of my knowledge and belief.

Sincerely,

_____

G. Alex Sinha
Human Rights Watch
350 Fifth Avenue – 34th Floor
New York, NY 10118
212.377.9427
sinhaa@hrw.org

WITH LIBERTY TO MONITOR ALL

How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy

With *Liberty to Monitor All,* a joint report by Human Rights Watch and the ACLU, documents the insidious effects of large-scale US surveillance on the practice of journalism and law in the United States, and the threat it poses to basic freedoms and democratic values. The report is based on extensive interviews with journalists, lawyers, and senior US government officials.

Journalists covering intelligence, national security, and law enforcement find that surveillance—combined with increased leak prosecutions and restrictions on contact between officials and the press—intimidates sources, making them more hesitant to discuss even unclassified issues of public concern. Journalists describe adopting elaborate, burdensome security techniques, and publishing less information of public interest.

Lawyers must uphold a professional responsibility to maintain the confidentiality of information related to their clients. They also rely on the free exchange of information with their clients to build trust and develop legal strategy. Increased surveillance creates uncertainty as to whether lawyers can ever provide true confidentiality, and undermines the right to counsel.

The US has an obligation to protect national security, and may engage in surveillance to the extent it is lawful, necessary, and proportionate to a legitimate state interest. But many existing surveillance programs are indiscriminate or overbroad, and threaten freedom of expression, the right to counsel, and the public's ability to hold its government to account. The US should reform these programs to ensure they are targeted and legitimate, increase transparency around national security and surveillance matters, and take steps better to protect whistleblowers and the media.

Headquarters of the US National Security Agency in Fort Meade, Maryland.
Photo by Trevor Paglen, 2014.

aclu.org | hrw.org