2016

Post-911 Government Surveillance, Suppression, and Secrecy

Nadine Strossen

Privacy, Security and Accountability

Ethics, Law and Policy

Edited by Adam D. Moore

ROWMAN & LITTLEFIELD
INTERNATIONAL
London • New York

Published by Rowman & Littlefield International, Ltd.
Unit A, Whitacre Mews, 26-34 Stannary Street, London SE11 4AB
www.rowmaninternational.com

Rowman & Littlefield International, Ltd. is an affiliate of Rowman & Littlefield
4501 Forbes Boulevard, Suite 200, Lanham, Maryland 20706, USA
With additional offices in Boulder, New York, Toronto (Canada), and London (UK)
www.rowman.com

British Library Cataloguing in Publication Information Available
A catalogue record for this book is available from the British Library

ISBN: HB 978-1-78348-475-1
ISBN: PB 978-1-78348-476-8

Library of Congress Cataloging-in-Publication Data

Privacy, security and accountability : ethics, law and policy / edited by Adam D. Moore.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-78348-475-1 (cloth : alk. paper) — ISBN 978-1-78348-476-8 (pbk. : alk. paper) — ISBN 978-1-78348-477-5 (electronic)
1. Privacy, Right of. 2. National security. 3. Liability (Law) I. Moore, Adam D., 1965– editor.
JC596.P759 2016
172'.1—dc23
2015031883

∞™ The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992.

Printed in the United States of America

Chapter Twelve

Post–9/11 Government Surveillance, Suppression and Secrecy

Nadine Strossen

In the wake of the 9/11 terrorist attacks, the U.S. government stepped up its policies of secrecy and surveillance, which had been widely criticized as excessive even before 9/11. The undue secrecy and surveillance propel a vicious spiral. The secrecy shields the surveillance from oversight, and both of them suppress free speech, dissent, and democracy. To quote our Constitution's opening words, "We the People" are the ultimate governors, but we cannot hold those we elect accountable if we do not know what they are doing. Moreover, when we have reason to fear that the government will spy on our communications, we engage in self-censorship.

Thanks to undue secrecy and surveillance, we have exactly the opposite information flow that we should have between We the People and those we elect—they have too much information about us, and we have too little information about them. In 2014, the American Civil Liberties Union (ACLU) and Human Rights Watch issued a joint report that documents how undue surveillance and secrecy are undermining press freedom and the public's right to information.[1] It was based on extensive interviews with dozens of journalists, including many Pulitzer Prize winners. They attest that sources of valuable information have been intimidated by the combination of surveillance, increased leak prosecutions, and new government restrictions on press contacts. As a result, sources hesitate to discuss even unclassified matters of public concern. Describing his ongoing struggle to obtain and publish essential information about the "War on Terror," and to maintain the confidentiality of his sources, *New York Times* reporter James Risen said, "The whole global war on terror has been classified. If we, today, only had that informa-

tion that was officially authorized from the U.S. government, we would know virtually nothing about the war on terror."[2]

The first part of this chapter discusses excessive surveillance, focusing on the dragnet communications surveillance programs that Edward Snowden revealed. It outlines the fundamental Fourth Amendment principles that this sweeping suspicionless surveillance violates, and explains why this constitutional protection is of utmost importance for everyone, including the vast majority of us who "have nothing to hide" in the sense of illicit activities. It also explains why even communications "metadata," or information about our communications, reveals sensitive personal information about people who are not even suspected of any wrongdoing, and hence is none of the government's business. Finally, it rebuts the major defenses that the government has offered for this bulk communications surveillance: that it has played a vital role in countering terrorism; that it is subject to effective oversight by the Foreign Intelligence Surveillance Court; and that it is consistent with the Supreme Court's Fourth Amendment rulings.

The next section of this chapter discusses the unwarranted secrecy that has facilitated the unwarranted communications surveillance, as well as undermining democratic accountability and the rule of law more generally. It focuses on one especially egregious type of undue secrecy: secret laws. Both post–9/11 presidents have relied on secret laws to carry out, free from any meaningful oversight, not only the dragnet communications surveillance programs but also other post–9/11 executive branch programs that likewise pose serious constitutional problems.

Finally, the chapter briefly outlines some pending countermeasures that could rein in unjustified surveillance and secrecy.

SURVEILLANCE

Government agencies at all levels have rapidly been deploying burgeoning surveillance technologies to gain ever more information about us and, hence, power over us. Some such high-tech surveillance programs include cell phone location tracking, drone surveillance, GPS tracking, and license plate readers, which have been increasingly used by multiple local, state, and national law enforcement agencies; the CIA's collection of business records regarding our international money transfers; the National Security Agency's (NSA) collection of online address books and contact lists; the NSA's collection of millions of faces from web images for use in sophisticated facial recognition programs; and the U.S. Postal Service's photographing of all mail.

The surveillance that has understandably provoked the most concern is the NSA's suspicionless spying on the phone and Internet communications of

everyone in this country, as well as people all over the world, even if we are not suspected of any wrongdoing. As the Supreme Court has recognized, surveillance of communications threatens not only privacy rights but also free speech rights, because of the "chilling" or deterrent impact that surveillance has on our communications. This chapter accordingly focuses on these doubly dangerous communications surveillance programs.

Fourth Amendment Principles

These programs violate the fundamental Fourth Amendment limits on any "search and seizure"—that is any government intrusion into our privacy. Although Fourth Amendment privacy rights are no more absolute than any other constitutional rights, the government bears a heavy burden of proof to justify any rights restriction. In general, the Supreme Court has held that any freedom-restricting measure must be necessary to promote a countervailing goal of compelling importance, such that no "less restrictive alternative" would suffice. In other words, the government may not impose a liberty-restricting measure if it could promote its goal through a measure that restricts liberty less. These general constitutional law standards reflect just plain common sense. After all, why should we give up our cherished liberty if we did not gain security in return? Or if we could gain as much security without giving up as much liberty?

Of course, national security is a goal of compelling importance. However, too many of the post–9/11 measures that the government touts as promoting national security are not even effective at doing so, let alone necessary. Therefore, many such measures have been critiqued not only by civil libertarians as unjustifiably undermining our freedom but also by national security experts as ineffective at best, counterproductive at worst. This is true of the dragnet surveillance programs. They sweep in too much information about too many innocent people, thus making it harder to hone in on the dangerous ones. As critics have put it, "The government is trying to find a needle in the haystack by adding more hay to the stack." Some of the harshest critics of dragnet communications surveillance include FBI agents who complain about the huge amount of time they have wasted in tracking down the thousands of completely innocent Americans whose communications have been caught in these fishing expeditions.

The same ineffectiveness problem plagues the government's asserted rationale for collecting all data about all of our phone calls. The government says that it uses these massive customer calling records for "data mining," looking for patterns of calls and keywords according to certain mathematical formulas that, it says, might point to suspected terrorists. However, prominent experts have denounced such data mining as "junk science." For example, Jonathan Farley, a math professor at Harvard and a Science fellow at

Stanford's Center for International Security, wrote, "[This] entire spying program [is] based on a false assumption: that you can work out who might be a terrorist based on calling [and keyword] patterns. . . . [B]ut guilt by association is not just bad law, it's [also] bad mathematics."[3]

Beyond the foregoing general constitutional limits on liberty-restricting measures, the Fourth Amendment also lays out two specific limits on government's surveillance power, one substantive and one procedural. It reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Substantively, the Fourth Amendment requires that any search or seizure must be based on "probable cause"—that is, individualized suspicion that the targeted person had engaged in illegal activity or is about to do so. The Fourth Amendment bars suspicionless searches because the government should not engage in fishing expeditions based on mere hunches or, worse yet, discriminatory stereotypes or guilt by association. Procedurally, the Fourth Amendment requires that any search or seizure must be based on a judge-issued warrant, which is a key element in the Constitution's overall scheme of checks and balances. It prevents executive officials from engaging in surveillance on their own initiative, instead requiring an independent judicial assessment that the probable cause standard is indeed satisfied.

Important as the Fourth Amendment requirements are in general, the Supreme Court has stressed that they are especially important when the government's search and seizure power is directed at expressive materials,[4] thus also raising First Amendment free speech concerns. In light of these dual constitutional concerns, the courts and Congress have strictly limited government's electronic surveillance of communications. Until the 9/11 terrorist attacks, even when such surveillance sought foreign intelligence, it still had to comply with the Fourth Amendment's core warrant and individualized suspicion requirements, albeit in somewhat modified forms. Under the 1978 Foreign Intelligence Surveillance Act or "FISA," the government had to seek an order from the special FISA Court, which could issue the order only if it found that there was "probable cause to believe that the target . . . [was] a foreign power or agent of a foreign power," and also that "each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or about to be used, by a foreign power or an agent of a foreign power."[5] In short, there still was individualized targeting of both the surveillance subject and the specific communications devices. Since 9/11, however,

the government has implemented multiple surveillance programs which abandon Fourth Amendment principles, as well as the FISA standards that reflected these principles.

Dragnet Suspicionless Communications Surveillance

Thanks to Edward Snowden, we know much more about these programs than we could have learned in any other way, given the government's excessive secrecy and outright lies. Even members of Congress and FISA Court judges, who were supposedly overseeing and checking surveillance, were in fact kept largely in the dark about these programs. Oregon senator Ron Wyden played a key role in calling attention to this problem. As a member of the Senate Intelligence Committee, he knew that the U.S. government was spying on unsuspected—and unsuspecting—Americans and lying about it to Congress. Wyden honored his duty to preserve the confidentiality of what he had learned through his committee position, but he did everything short of breaching that duty to force the government to come clean. That culminated in his now-infamous exchange with James Clapper, director of national intelligence, during a Senate hearing on March 12, 2013. When Wyden pressed Clapper about whether the NSA was engaging in bulk surveillance of Americans' communications, Clapper said, "No." After the Snowden revelations confirmed that this was a flat-out lie, Clapper dissembled yet again, explaining that this was "the least untruthful" answer he could give.[6] Finally, under pressure of continuing revelations from Snowden, on June 21, 2013, Clapper wrote a letter to the Senate Intelligence Committee apologizing for his "clearly erroneous" testimony.

Snowden's disclosures provided vital information that Clapper and other officials hid, when all other supposed oversight mechanisms had failed. In fact, the dramatic exchange between Ron Wyden and James Clapper was what Snowden called his "breaking point." As he said, "Seeing the Director of National Intelligence . . . lie under oath to Congress . . . meant for me there was no going back. . . . [I]t brought . . . the . . . realization that no one else was going to do this," to honor "[t]he public . . . right to know about these programs."[7]

Through the Snowden revelations and other sources, the American public has been learning about multiple dragnet communications surveillance programs, although we still lack crucial details about them, and there are probably more programs about which we are still completely ignorant. For example, as this chapter was being written, in January 2015, the government acknowledged yet another mass database of U.S. citizens' telephone records that it collected without any individualized suspicion or judicial authorization; the government maintained these records, even if there was no evidence that the callers were involved in illegal activity, until at least September

2013. Maintained by the Drug Enforcement Administration and available to other law enforcement agencies, this database contained information about calls between people in the United States and people in foreign countries "that . . . have a demonstrated nexus to international drug trafficking and related criminal activities." The stored information consisted of the same kind of call data that the NSA has been collecting: phone numbers, time and date, and length. As Vermont senator Patrick Leahy stressed, in a letter to attorney general Eric Holder, "I am deeply concerned about this suspicionless intrusion into Americans' privacy in any context, but it is particularly troubling when done for routine criminal investigations."[8]

PATRIOT Act Section 215

One bulk surveillance program that Snowden disclosed arises under Section 215 of the PATRIOT Act. Section 215 eliminated even the watered-down individualized suspicion requirement that had existed under FISA since 1978, summarized above. It empowers the government to seize anything that it deems "relevant" to a terrorism investigation. This new "relevance" standard is diametrically different from the Fourth Amendment's (and FISA's) strict but sensible "probable cause" standard. In fact, "relevance" is by definition the lowest possible standard; after all, the government indisputably is not entitled to information that is irrelevant to an investigation.

Overreaching as Section 215 was, for several years prior to Snowden's revelations, a couple members of the Senate Intelligence Committee had been warning that the executive branch had been engaging in surveillance that exceeded even these loose standards, through secret interpretations—actually, misinterpretations—of Section 215. Their confidentiality obligations barred them from disclosing any details, even to other members of Congress. For example, in 2011, Senator Wyden declared, "When the American people find out how their government has secretly interpreted the PATRIOT Act, they will be stunned and they will be angry."[9]

Sure enough, beginning in June 2013, the Snowden revelations documented that the government had been relying on Section 215 to gather copious data about literally all telephone users, which was indeed irrelevant to any terrorism investigation—nor did the government dispute this. Rather, the government's rationale is that the information might become relevant in the future. In short, the government's approach is to collect all our data first, and then hope to use it to solve or prevent some crime that might occur sometime in the future. This approach could not be further from the Fourth Amendment's requirements. Moreover, this misreading of Section 215 is completely inconsistent with its language, and has accordingly been denounced by many members of Congress who voted for the PATRIOT Act, including Wisconsin Republican congressman Jim Sensenbrenner, its chief author.

Under the government's unbounded misconstruction of Section 215, it has been collecting "metadata" about all of our phone calls at least since 2006, and perhaps earlier. This metadata includes the phone numbers to and from which we place and receive calls, also revealing the names of the parties to the call; when the calls are made; how long they last; and from what locations they are made. In addition to collecting this information about all of our phone calls, the government swept up this same information about all of our Internet communications from 2001 until 2011. Notably, the government ended this bulk Internet surveillance because it did not produce useful intelligence, as the government was forced to acknowledge under questioning from congressional intelligence committee members.

FISA Section 702

A second communications surveillance program that came to light thanks to the Snowden disclosures, the "PRISM" program, arises under Section 702 of FISA, which codifies the FISA Amendments Act of 2008. Section 702 revolutionized the FISA regime by permitting the mass acquisition of American's international communications—their actual contents—without individualized judicial oversight.

Since Edward Snowden brought PRISM to light, its defenders, including President Obama, have been asserting that it does not apply to any U.S. citizen or resident.

However, that assertion is misleading at best. Section 702 does provide that Americans' domestic calls may not be the direct target of the surveillance, but the government may and does retain Americans' domestic calls that are obtained "incidentally," a potentially boundless group. After all, communication is a two-way street. So if an American is communicating with a foreign "target," no matter how innocently, the government may collect, inspect, and keep the content of that communication. Moreover, the definition of a foreign target is so broad that it inevitably encompasses many innocent Americans as well. First, the government may target anyone it believes to be a foreigner, even if that person is actually an American. Second, the government may target people who are not even suspected of any crime, let alone terrorism. Rather, it may target anyone who is communicating about "foreign affairs," which it defines broadly to include everything from trade to travel, thus putting U.S. businesspeople in the crosshairs, as well as journalists, human rights researchers, academics, and attorneys.

Worse yet, under PRISM, the NSA was automatically searching the phone communications of anyone who was within "three hops" from a targeted person: anyone who had a phone communication with the target during the last five years ("the first hop group"), plus anyone who had a phone communication with anyone in the first hop group during the last five years

("the second hop group"), plus anyone who had a phone conversation with anyone in the second hop group during the last five years. Even if one assumes that, in that time period, each targeted individual had phone communications with just 100 other people, and that each person involved in each "hop" also had phone communications with just 100 other people, that would mean that for each target, the NSA would search the phone communications of 1,000,000 people. In response to the public outcry about this vacuuming up of Americans' communications, President Obama trimmed back the collection to two hops. However, this means that for every target believed to be foreign, the NSA searches the content of the phone communications of ten thousand people.

In 2014, the *Washington Post* ran a chilling expose, analyzing a large cache of phone communications that the NSA had intercepted under Section 702. Edward Snowden said he had provided these communications so the public could assess the actual costs and benefits of Section 702 surveillance. The chief author of the *Washington Post* analysis was the respected national security journalist Barton Gellman. As he observed, "No government oversight body . . . has delved into a comparably large sample of what the NSA actually collects—not only from its targets but also from people who may cross a target's path," even tangentially. The upshot? A full 90 percent of the intercepted communications came from "ordinary Internet users," including Americans, rather than legally targeted foreigners. Describing the highly personal, sensitive nature of the spied-upon communications, the article went on to say:

> Many . . . have a startlingly intimate . . . quality. They tell stories of love and heartbreak, illicit sexual liaisons, mental-health crises, political and religious conversions, financial anxieties and disappointed hopes. . . . [They include] medical records sent from one family member to another . . . pictures [of] infants and toddlers in bathtubs . . . and photos [of] men show[ing] off their physiques, [and of] women model[ing] lingerie.[10]

Executive Order 12333

Another bulk communications surveillance program is based on an executive order that president Ronald Reagan issued in 1981, which authorizes surveillance of the content of communications intercepted on foreign soil, with virtually no limits or oversight. It was designed for communications between non-Americans but it now also sweeps up countless American communications, given technological changes since 1981—specifically, that most purely domestic communications now are located on servers in other countries. In 2014, former State Department official John Tye blew the whistle on this essentially secret surveillance power, in the tradition of Ron Wyden's earlier warnings about NSA surveillance: sounding a general alarm but honoring

confidentiality duties, and hence not revealing details. Ominously, Tye warned, "Based in part on classified facts that I am prohibited by law from publishing, I believe that Americans should be even more concerned about the collection and storage of their communications under [this] Executive Order . . . than under [the PATRIOT Act]."[11]

Why Privacy Matters

Many fellow Americans ask why we should care about these sweeping communications surveillance programs, saying, "I have not done anything wrong, so I have nothing to hide." The fallacious premise is that the only things we would want to hide from government spies would be evidence of wrongdoing. To the contrary, all of us law-abiding folks have compelling reasons to hide completely lawful actions and interactions—indeed, some of our most important, positive, and cherished actions and interactions—simply because they are no one else's business.

George Orwell's prescient dystopian novel, *1984*, powerfully demonstrates the oppression that results from pervasive surveillance; as the novel puts it, Big Brother is always watching us. It shows how such surveillance demeans our dignity and destroys our relationships. This surveillance causes the very same harms that also result from more overtly coercive authoritarian tactics, such as torture and imprisonment. Psychological studies have confirmed that people who are being watched tend to behave differently, and to make different decisions, than when they are not being watched. This effect is so great that a recent study found that "merely hanging up posters of staring human eyes is enough to significantly change people's behavior"[12]—the very type of "Big Brother is Watching" poster that Orwell imagined.

Why Government Metadata Collection Violates Privacy

Defenders of the Section 215 bulk metadata collection program contend that this entails an insignificant privacy invasion, in contrast to surveillance of communications' actual content. As one government official correctly concluded, though, government collection of communications metadata under Section 215 is "very, very intrusive."[13] Ironically, the official I have quoted is Vice President Joe Biden, speaking while he was still in the Senate, and critiquing the Bush administration's collection of metadata. Metadata disclosing with whom we communicate, and when, can well be at least as revealing as what we say or write. Consider, for example, calls between a reporter and a government whistleblower, and calls to Alcoholics Anonymous, a gambling bookie, abortion clinic, or hotline for gay teens. An MIT study found that from reviewing people's social networking contacts, which metadata reveal, one can identify their sexual orientation.[14] Likewise, meta-

data from e-mails were sufficient to identify the mistress of the then CIA director David Petraeus, which drove him out of office. The NSA's supercomputers can employ sophisticated data-mining technologies to analyze terabytes of metadata, and thus construct detailed portraits of us and our relationships.

A leading computer expert, Princeton University professor Edward Felten, has explained that the communications metadata that the NSA has been sweeping up conveys highly sensitive information, which traditionally could be obtained only by reviewing communications' content: "The government can learn our religion . . . our work habits . . . our civi[c] and political affiliations . . . the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger . . . and the identities of a prospective government whistleblower and an anonymous litigant."[15]

In fact, as technology advances, the distinction between a communication's content and metadata blurs. For example, the government has argued that a website address is only metadata, and hence should be less protected against surveillance. But the sites we visit online are comparable to the list of books we check out of a library. The very fact that we have visited a certain webpage can be every bit as revealing as the content of an e-mail message. After all, the very reason the government is so eager to sweep up metadata is precisely because it is a treasure trove of information.

Rebutting Government's Defenses of Dragnet Communications Surveillance

The government has offered three major defenses for its sweeping communications surveillance: that it is essential for countering terrorism; that it is subject to oversight by the special FISA Court; and that it comports with Supreme Court decisions construing the Fourth Amendment.

It Is Not Essential for Countering Terrorism

Experts concur that the NSA's indiscriminate communications surveillance has not made any contribution to U.S. counterterrorism efforts. That was the conclusion of both high-level commissions that issued detailed reports on point in 2013 and 2014: the President's Review Group on Intelligence and Communications Technologies[16] and the Privacy and Civil Liberties Oversight Board.[17] For example, in the latter's 2014 report, which reflected an in-depth examination of classified information, it concluded:

> The [NSA's phone records] program has shown minimal value in safeguarding the nation from terrorism. Based on the information [the government] provided . . . including classified briefings and document[s], we have not iden-

> tified a single instance . . . in which the program made a . . . difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.[18]

A federal judge who ruled that this program was unconstitutional reached the same conclusion: "[T]he Government does *not* cite a single instance in which . . . the NSA's bulk . . . collection actually . . . aided in achieving any time-sensitive objective."[19] Likewise, a 2014 report by the New America Foundation, which analyzed all the terrorist plots that the government initially claimed had been thwarted in part due to the NSA's dragnet surveillance—before the evidence forced it to back away from these claims—concluded that such surveillance in fact had had "no discernible impact on preventing acts of terrorism."[20]

FISA Court Supervision Is Insufficient

The government's second major defense of the NSA's massive surveillance is that the FISA Court provides oversight. In fact, though, that court functions more like a rubber stamp for the government than an independent court. Among many other limits, it operates completely in secret, and hears completely one-sided arguments, only from the government.

Thanks to post-Snowden disclosures, we have learned that the FISA Court has repeatedly rebuked the NSA for repeatedly misleading the court about its bulk surveillance, and for repeatedly violating FISA Court orders imposing some modest curbs on that surveillance. In 2009, FISA Court judge Reggie Walton concluded that, since the inception of this surveillance three years earlier, the NSA had engaged in "systematic noncompliance" with court orders designed to minimize the suspicionless collection and review of Americans' communications. Judge Walton also concluded that the NSA had repeatedly made misrepresentations about the program to the FISA Court judges.[21] Stating that he had no confidence that the government was doing its best to comply with the FISA Court's orders, Judge Walton imposed a six-month sanction. Nonetheless, the government persisted in violating FISA Court orders. In 2011, FISA Court presiding judge John Bates said, "The Court is troubled that [this is] the third instance in less than three years in which the government has disclosed substantial misrepresentations regarding the scope of a major collection program."[22] One FISA Court judge actually resigned in protest over the dragnet communications surveillance programs, and testified in Congress about the court's inability to provide any meaningful check.

To put the FISA Court judges' strong reprimands in context, it should be noted that the FISA Court has been critiqued because of its judges' pro-government tilt. Therefore, it is especially troubling that even this court has

repeatedly concluded that the government had not only violated the Constitution and court orders but also lied about its actions.

This repeated government lying about surveillance is an aspect of the government's excessive secrecy. The government has too often been providing either no information or misleading or false information, not only to We the People, but even to the handful of members of Congress on the intelligence committees and to the FISA Court judges, who are supposed to act as watchdogs in our stead. Thanks to some successful Freedom of Information Act lawsuits, we have recently seen some of the FISA Court opinions that authorize this surveillance, which in turn quote the government's arguments. The ACLU's deputy legal director, Jameel Jaffer, compared the government's arguments in the one-sided, secret proceedings before the FISA Court with the government's arguments in the regular federal court system, in which the ACLU and others have been challenging this surveillance post-Snowden.

In the FISA Court, the government made extravagant claims about the supposed necessity and efficacy of such surveillance. For example, it said that this surveillance was "the only effective means" for "keep[ing] track" of suspected terrorists.[23] There is no opponent in the FISA Court, so these bold claims went unchallenged. By contrast, in the open federal court system, the government's claims are subject to rebuttal by opposing parties, and to meaningful scrutiny by independent judges, as well as the public and press. Not surprisingly, in this context, the government's claims about the importance of bulk surveillance are much more modest. Specifically, in open federal court the government has said only that such surveillance is "one method . . . that can "complement . . . other[s]" and "can contribute" to counterterrorism efforts.[24] Surely such a limited security benefit can hardly justify the huge costs to privacy, freedom of speech and press, and democracy.

The Supreme Court's Fourth Amendment Jurisprudence Does Not Authorize This Surveillance

At the time this chapter is being written, there is ongoing litigation in several courts in which the dragnet communications surveillance programs are being challenged, and to date the lower court judges have reached inconsistent results. This chapter will focus on the constitutional principles in general, including as they have been enforced by the Supreme Court rulings that are generally on point, since the high court has not yet ruled on a Fourth Amendment challenge specifically to the communications surveillance.

As discussed above, the Fourth Amendment's plain language requires that all searches and seizures must be based on individualized suspicion and a judicially issued warrant, both of which are absent from the dragnet communications surveillance programs. Moreover, the original understanding of

the Fourth Amendment framers reinforces the conclusion that such surveillance is unconstitutional. This is significant, because the Constitution's text and original understanding are the two methods of constitutional interpretation that tend to be favoured by conservatives. Accordingly, the constitutional analysis provides a persuasive reason for conservatives to oppose this surveillance, and in fact many conservative members of Congress have voted to curb it.

By contrast, the government defends such surveillance not by invoking the Fourth Amendment's language or original understanding, but rather by invoking Supreme Court decisions that have cut back on the Fourth Amendment's scope in what the government views as analogous situations. Since these cases involve facts that are materially distinguishable from the bulk surveillance program, they are not controlling. On the contrary, more recent Supreme Court decisions involving other high-tech surveillance indicate that the court will likely enforce the Fourth Amendment robustly in the bulk surveillance context.

In 2013, federal judge Richard Leon, a respected conservative, granted a preliminary injunction against the NSA's dragnet phone records collection, stressing the original understanding of the Fourth Amendment's framers. As he said:

> I cannot imagine a more "indiscriminate" and "arbitrary invasion" than this . . . high-tech collection and retention of personal data on virtually every single citizen . . . without prior judicial approval. Surely such a program infringes on [the] privacy that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison . . . would be aghast.[25]

The Fourth Amendment expressly bars the type of dragnet phone record program that the NSA has been conducting, without any individualized probable cause warrants. On the contrary, this program proceeds under blanket FISA Court warrants, which purport to authorize wholesale, suspicionless collection of all our records. This is the very kind of hated general warrant and general search that fueled both the American Revolution and the Fourth Amendment. Citing this history, the Supreme Court has consistently held that suspicionless, warrantless searches and seizures are almost automatically unconstitutional, and there are powerful originalist arguments that they should always be automatically unconstitutional.

The government argues that bulk phone records collection should instead be judged under the "special needs" exception to the warrant and suspicion requirements, which the Supreme Court created in 1985. It applies only in "exceptional circumstances" where "special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirements impracticable."[26] However, many experts concur that the government could

practicably comply with these requirements in seeking terrorism-related communications. Indeed, even the director of national intelligence has recently "signaled that the information the NSA needs about terrorist connections might be obtainable without first collecting . . . 'the whole haystack' of U.S. phone data."[27]

Even assuming for the sake of argument that the special needs exception did apply to the bulk phone record collection, it would still be unconstitutional. Even under the special needs exception, the court has held that a suspicionless search or seizure is unconstitutional unless "the privacy interests [it] implicate[s] are minimal, "and . . . an important government[] interest . . . would be . . . jeopard[ized] by [an] individualized suspicion requirement."[28] On the contrary, though, the privacy interests that bulk collection implicates are maximal, not minimal: sweeping up countless records about hundreds of millions of innocent Americans, containing the most intimate personal details. Likewise, as also discussed above, dragnet phone records collection also fails the second prong of the "special needs" test, because experts have concluded that the indiscriminate communications surveillance has not advanced our counterterrorism efforts.

In the lawsuits challenging the NSA's bulk phone records program, the government's main defense rests on the "third-party doctrine," which is based on some Supreme Court cases in which the court has held that when we voluntarily disclose data to third parties, we forfeit a "reasonable expectation of privacy" in that data, and hence have no Fourth Amendment claim when the third party gives that data to the government. However, the court has never held that the third-party doctrine always bars Fourth Amendment claims, as the government itself recognizes. For instance, even the government recognizes that we do have a reasonable expectation of privacy in the contents of our calls or e-mails, even though phone companies also have access to them.

The government's third-party argument centers on a 1979 case, *Smith v. Maryland*,[29] which also involved phone records. Beyond that single fact, though, *Smith* is light years apart from the mass surveillance programs now at issue. The court held that Michael Smith, a criminal suspect, had no reasonable expectation of privacy in the list of phone numbers he had called during just two days, which the government did not retain. By contrast, indiscriminate metadata collection presents the following, completely different, question: whether hundreds of millions of Americans who are not criminal suspects have a reasonable expectation of privacy in a complete catalog of the phone numbers, date, time, duration, and location for every call we have made or received since 2006, or even earlier, and continuing on indefinitely, all of which the government will retain for at least five years.

Most Americans probably are not even aware that their phone companies are collecting this detailed information, and we certainly have not consented

to our phone companies systematically turning it all over to the government, in violation of their written privacy policies.

As Professor Felten explained, "The only . . . way to avoid creating such metadata [which is available to the phone companies] is to avoid telephon[e] communication altogether"[30]—in other words, not a real choice, given the vastly increased importance of such communication in our twenty-first-century world. Moreover, as Judge Leon wrote, in support of his holding that the sweeping NSA phone surveillance violates the Fourth Amendment, "It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government."[31]

The key technological changes since 1979, when *Smith* was decided, constitute another reason why that ruling does not apply to bulk phone record collection. As Justice Scalia wrote in a 2001 majority opinion striking down warrantless thermal imaging, our Fourth Amendment privacy should not be left to "the mercy of advancing technology." In the court's 2012 case striking down GPS surveillance under the Fourth Amendment, five justices expressly questioned whether *Smith* applies to new technology, in opinions by Justices Alito and Sotomayor—notably, among the court's most conservative and liberal members, respectively. Likewise, in a 2014 decision concerning cell phones, the justices unanimously recognized that, in effect, "digital is different," so that prior cases allowing searches and seizures incident to arrest do not apply to cell phones, given the vast differences between such digital devices and other items. The same conclusion applies to the *Smith* decision; it simply does not govern dragnet metadata collection. The argument that bulk metadata collection is not materially distinguishable from the *Smith* facts is wrong for the same reason that the Supreme Court in 2014 unanimously rejected the government's argument that cell phone seizures are "materially indistinguishable" from other seizures: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[32]

The government's other major argument in the NSA litigation is that the Fourth Amendment does not apply when it vacuums up this massive, sensitive data, but rather only when it examines the data. This is dead wrong for many reasons starting with, again, the Fourth Amendment's plain language and original meaning. On these points, I will quote two respected conservative scholars, Randy Barnett and Jim Harper: "The Founders thought that the seizure of 'papers' [or data] for later perusal . . . was an abuse distinct from, but equivalent to the use of" the reviled "general warrants."[33] To allow the government to seize first and show probable cause later is exactly the opposite of what the Fourth Amendment explicitly requires, and the opposite of what it meant to our nation's founders.

If the government's contrary position prevailed, it could collect any of our data, including the contents of our communications, on the pledge that we should trust government employees not to actually look at it without first getting a warrant. This "trust us" argument is risible given government's track record of negligently and intentionally failing to protect the confidentiality of our data. As discussed above, the FISA Court has harshly chided the NSA for repeatedly violating even the modest limits that the FISA Court had imposed on the bulk phone record program. The government is not even able to protect its own data against leakers and hackers. To cite one recent example, we learned in late 2014 of a massive online data breach of the U.S. Postal Service, disclosing sensitive information about more than 800,000 USPS employees, including their Social Security numbers. Moreover, government employees have consistently snooped on and used data that is supposed to be maintained as confidential for a host of personal and political reasons. Therefore, the government's "trust us" argument flies in the face of the facts, as well as Fourth Amendment principles.

SECRECY

Overview

As discussed above, the argument that dragnet communications surveillance is no problem for anyone who has "nothing to hide" is deeply flawed. Moreover, the nothing-to-hide argument is a double-edged sword. If it were true that you have nothing to hide unless you are doing something wrong, then the *government* should declassify everything and end all of its secrecy policies! Of course, though, even the most ardent transparency advocate recognizes that government has legitimate secrets, such as the names of undercover agents and battle plans. On the other hand, even the most ardent security hawk recognizes that the United States now is enforcing egregiously excessive secrecy policies, covering material that posed no real security risk. For example, in 1970, a Defense Department report concluded that the amount of classified information "could profitably be decreased perhaps as much as 90 percent,"[34] but instead, the trajectory since then has been towards even more overclassification. It is also widely acknowledged that too often, officials hide information from the public only to protect themselves from political embarrassment.

Many studies have documented how the already excessive secrecy policies pre–9/11 became enormously more so after 9/11. For example, in 2010, the *Washington Post* published an article entitled "Top Secret America," which summarized the findings of its two-year investigation as follows:

> The top-secret world the government created in response to the [911] attacks . . . has become so large . . . and so secretive that no one knows how much money it costs, how many people it employs, [and] how many programs exist within it. . . . [It] amounts to an alternative geography . . . a Top Secret America hidden from public view and lacking in thorough oversight.[35]

Some examples of the Obama administration's unwarranted secrecy include:

- rampant overclassification;
- a crackdown on whistle-blowers;
- imposing severe restrictions on officials' press contacts;
- in overly aggressive leak investigations, subpoenaing reporters, wiretapping media outlets, spying on journalists' private e-mail accounts, and even threatening reporters with potential prosecution;
- resisting the Freedom of Information Act (FOIA);
- refusing to disclose basic information to Congress;
- secret lawmaking; and
- aggressive assertion of the "state secrets privilege" to dismiss lawsuits that challenge unconstitutional and illegal actions in the "War on Terror."

This chapter will now expand on a couple of these unjustified secrecy policies, by way of example.

The War on Whistleblowers and Investigative Journalists

The Obama administration has prosecuted more whistleblowers under the infamous 1917 Espionage Act than all prior administrations added together. In its first ninety-two years, the act was used only three times to prosecute government officials for press leaks. By contrast, the Obama administration has pursued eight such prosecutions. Moreover, a less well-known statistic underscores an even more dramatic disparity between the Obama administration and all others in its persecution of leakers; as summarized by ACLU legislative counsel Gabe Rottman, "the Obama administration has secured 526 months of prison time for national security leakers, versus only twenty-four months total jail time for [all such leakers] since the American Revolution."[36] As Rottman explains, the historically light sentencing in media leak cases reflected at least in part press freedom concerns.

Not surprisingly, the administration's aggressive stance towards whistleblowers has chilled government sources, hence freezing access to vital information for journalists and the public, as documented in the 2014 ACLU/Human Rights Watch report noted in the introduction. For example, *New York Times* journalist Scott Shane, who covers national security, said that "government officials who might otherwise discuss sensitive topics . . . refer to these [Espionage Act] cases in rebuffing a request for background infor-

mation."[37] The administration's overbearing policies in this area have been criticized by even such a strong proponent of strong executive power and national security policies as the *Wall Street Journal*. It said that the administration is engaging in "a pattern of anti-media behavior," and that its leak investigations "are less about deterring leakers and more about intimidating the press."[38]

Especially troubling is the Administration's prosecution of Pfc. Chelsea (formerly Bradley) Manning for the potential capital offense of "aiding the enemy," when he leaked documents to WikiLeaks.

Under the prosecution's theory, because Manning knew the materials would be published and that al-Qaeda could then read them, she indirectly communicated with the enemy. In response to the judge's inquiry, the prosecutors said that they would have brought the same charges if Manning had leaked the materials to the *New York Times* rather than WikiLeaks. Even the noted First Amendment attorney Floyd Abrams, who has criticized both Chelsea Manning and WikiLeaks, nonetheless condemned this prosecution, stating, "Anyone who holds freedom of the press dear should shudder at the threat that the prosecution's theory presents to journalists, their sources and the public that relies on them."[39]

By contrast to the administration's prosecution and punishment of those who have leaked information about illegal government conduct, it has done nothing at all to punish those who committed the illegal conduct. For example, the only person to do time for the CIA's torture policies is the whistleblower who brought them to light. Likewise for the illegal NSA surveillance program in the Bush administration—the only person to be penalized was the whistleblower who told the *New York Times* about it, then had his life ruined with vindictive investigations. Moreover, the telecoms that illegally cooperated were retroactively immunized from all legal accountability.

In addition to the Obama administration's double standard towards whistleblowers and the wrongdoers on whom they blow the whistle, it also has a double standard about leaks. As is consistently the case in any presidential administration, top officials selectively leak information about sensitive matters that reflect positively on it or serve other strategic purposes, while decrying and punishing leaks that reflect negatively on it or otherwise undermine its goals. As one commentator summed it up, the Obama administration is "trumpeting information that makes [it] look good while suppressing with the force of the criminal law anything that does the opposite."[40]

The adverse impact of the Obama administration's "War on Whistleblowers" was well summarized by the following statement: "Often the best source of information about waste, fraud, and abuse in government is an existing government employee committed to public integrity and willing to speak out. Such acts of courage and patriotism, which can sometimes save lives and often save taxpayer dollars, should be encouraged rather than stifled."[41]

Sadly, this statement came in 2009 from president-elect Obama.

Excessive Secrecy Undermines National Security

All of this unwarranted secrecy obviously is antithetical to First Amendment values, democratic accountability, and the rule of law. Worse yet, it also has an adverse impact on national security. Of course, the asserted justification for such secrecy is to advance national security. In fact, though, experts concur that excessive secrecy actually undermines security by preventing effective information sharing among government officials, as well as between the public and private sectors, thus leading to flawed intelligence. This point was underscored, for example, by none other than a former head of the whole classification system, J. William Leonard, who served as director of the Information Security Oversight Office from 2002 until 2011. As he said, "Government secrecy just about guarantees the absence of an optimal decision on the part of our nation's leaders, often with tragic consequences for our nation."[42] In the same vein, the staff director of the bipartisan 9/11 Commission, Eleanor Hill, declared that the intelligence community's "most potent weapon" is "an alert and informed American public."[43] Conversely, the commission concluded that excessive secrecy was one of the factors that could well have contributed to the 9/11 attacks, which it indicated could have been foiled with more information sharing. Indeed, the commission expressly asserted, "Had KSM known that Moussaoui had been arrested, he would have cancelled the attacks."[44]

Secret Laws

Of all the forms of unjustified secrecy, none is more inconsistent with democratic self-government than secret laws. When Senator Wyden first warned Americans about the government's secret interpretation of the PATRIOT Act in 2011, the whole concept of a secret law was shocking, inherently antithetical to our form of government by the people. Indeed, a prominent conservative federal judge, Richard Posner, wrote, "The idea of secret laws is repugnant."[45] Sadly, as with so many post–9/11 abuses that at first seemed like something out of a dystopian novel, secret laws have come to seem almost routine, even though still repugnant.

Post–9/11, both the Bush and the Obama administrations have been relying on two major sources of secret law, which are secret not only from the American people but also from members of Congress, including even members of the intelligence committees, who are supposed to be overseeing intelligence operations, and who are given top-secret security clearances for that purpose. Nonetheless, as Senator Wyden told the *New Yorker*, when people

ask him about sensitive national security issues, he answers, "What do I know? I'm only on the [Senate] Intelligence Committee."[46]

The first major source of secret law comes from the Department of Justice's Office of Legal Counsel, which writes memos that guide the executive branch. These memos have purported to authorize multiple measures that are widely considered illegal and unconstitutional, including torture and targeted killing of U.S. citizens away from any battlefield, as well as dragnet NSA surveillance. To its credit, the Obama administration did disclose the torture memos that were written during the Bush administration, but it has fought against release of other memos, which have authorized its own controversial policies.

The second major source of secret law about dragnet communications surveillance consists of the FISA Court opinions that have interpreted federal statutes and the Constitution as allegedly authorizing dragnet surveillance. Again, public interest organizations and journalists have been fighting for disclosure of these opinions. While some have been released, others have not. To be sure, these opinions should be redacted to the extent that they reveal security-sensitive facts. By contrast, what should not be kept secret is the legal reasoning that allegedly justifies the NSA's sweeping surveillance. This is especially critical because the Supreme Court has not reviewed any of these FISA Court opinions. Therefore, as the *New York Times* observed, "[The FISA Court] has . . . become . . . a parallel Supreme Court, serving as the ultimate arbiter on surveillance issues."[47] In short, these secret FISA Court opinions are tantamount to secret Supreme Court rulings, underscoring why such secrecy is anathema.

POTENTIAL REFORMS

In the wake of the Snowden revelations, there has been more positive momentum to rein in excessive surveillance and secrecy than there has been since 9/11. There have been meaningful steps in the right direction on two major fronts: litigation and legislation.

On the litigation front, there have been some significant pro-privacy victories in lower courts. Furthermore, while the Supreme Court has not directly ruled on communications surveillance in particular, it has issued a couple recent rulings about other high-tech forms of surveillance that strongly protect privacy rights, and could certainly be the basis for positive rulings on communications surveillance too.

On the legislative front, bipartisan bills have been introduced in both houses of Congress that would rein in NSA surveillance as well as excessive secrecy. Since the Snowden disclosures, a couple bills constraining NSA surveillance have received majority votes in the House of Representatives;

this is the first time since 9/11 that either house of Congress has voted to curb government surveillance at all. Even the Obama administration has expressed support for some of these reforms. Important support is also coming from U.S. tech companies, whose business has been greatly harmed by NSA surveillance and the worldwide mistrust it is creating about the security of U.S. products and services. A recent report projected that, in 2015–2016 alone, U.S. tech companies could lose up to $35 billion in canceled contracts and missed opportunities.[48]

CONCLUSION

As the Supreme Court has repeatedly reminded us, we must never let our concern for security blind us to what exactly we are striving to secure. For example, during the Cold War, the court declared, "It would indeed be ironic if, in the name of national defense, we would sanction the subversion of . . . those liberties . . . which make the defense of the Nation worthwhile."[49] In the case of excessive surveillance and secrecy, the irony is compounded because, in national security terms, these policies are at best ineffective and at worst counterproductive.

NOTES

1. G. Alex Sinha, Human Rights Watch, and American Civil Liberties Union, *With Liberty to Monitor All: How Large Scale US Surveillance is Harming Journalism, Law, and American Democracy* (New York: Human Rights Watch, 2014).
2. James Risen, interview by Lesley Stahl, *CBS 60 Minutes*, October 12, 2014, http://www.cbsnews.com/news/war-on-leaks-national-security-press-freedom/.
3. Jonathan David Farley, "The N.S.A.'s Math Problem," *New York Times*, May 16, 2006, http://www.nytimes.com/2006/05/16/opinion/16farley.html?_r=0.
4. See, e.g., *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978).
5. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801 et seq. (2008).
6. James Clapper, interview by Andrea Mitchell, *NBC Nightly News*, June 8, 2013, http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/874-director-james-r-clapper-interview-with-andrea-mitchell.
7. "Snowden Exklusiv: Das Interview," video, 30:28, interview of Edward Snowden by Hubert Siebel from Norddeutscher Rundfunk, broadcast by ARD TV on January 26, 2014, posted by "ARD_Stinkt," January 27, 2014, http://liveleak.com/view?i=f93_1390833151.
8. Michael S. Schmidt and Matt Apuzzo, "U.S. Discloses New Trove of Phone Call Records," *New York Times*, January 16, 2015, http://www.nytimes.com/2015/01/17/us/dea-kept-telephone-records-on-americans-justice-department-says.html.
9. Senator Wyden of Oregon, speaking during a debate about the official interpretation of the Patriot Act on May 26, 2011 (157 Cong. Rec. 8179 [2011]).
10. 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.

11. John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans," *Washington Post*, July 18, 2014, http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

12. Sander van der Linden, "How the Illusion of Being Observed Can Make You a Better Person," *Scientific American*, May 3, 2011, http://www.scientificamerican.com/article/how-the-illusion-of-being-observed-can-make-you-better-person/.

13. "Sen. Biden on NSA Database," CBS News video, 3:38, May 12, 2006, https://www.youtube.com/watch?v=8T4EPYSt5Dk.

14. Carter Jernigan and Behram F. T. Mistree, "Gaydar: Facebook Friendships Expose Sexual Orientation," *First Monday* 14, no. 10 (October 2009), doi: 10.5210/fm.v14i10.2611.

15. Declaration of Professor Edward W. Felten, ¶ 56–58, *ACLU v. Clapper*, 959 F Supp. 2d 724 (S.D.N.Y. 2013).

16. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (2013), 33.

17. 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 Court* (2014), 146, 169n.

18. Ibid., 11.

19. *Klayman v. Obama*, 957 F. Supp. 2d 1, 40 (D.D.C. 2013).

20. Peter Bergen et al., *Do NSA's Bulk Surveillance Programs Stop Terrorists?* New America Foundation, January 2014, https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf.

21. In re Production of Tangible Things From [redacted], Order, No. BR 08-13, 2009 WL 9150913, at *5 (FISA Ct. Mar. 2, 2009).

22. [Redacted], 2011 WL 10945618, at *5, n14 (FISA Ct. Oct. 3, 2011).

23. Judge Reggie Walton cited in Jameel Jaffer, "The Basis for the NSA's Call-Tracking Program Has Disappeared, If It Ever Existed," https://www.aclu.org/blog/basis-nsas-call-tracking-program-has-disappeared-if-it-ever-existed.

24. Declaration of Acting Assistant Director of FBI Robert J. Holley, 2, 4, *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

25. *Klayman*, 957 F. Supp. 2d at 42.

26. *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985). (Blackmun, J., concurring).

27. Siobhan Gorman, "NSA Chief Opens Door to Narrower Data Collection," *Wall Street Journal*, February 27, 2014, http://www.wsj.com/news/articles/SB10001424052702304071004579409582715306814?mod=rss_Technology&mg=reno64-wsj. ("But Gen. Alexander . . . signaled that the information the NSA needs about terrorist connections might be obtainable without first collecting what officials have termed 'the whole haystack' of U.S. phone data.")

28. *Skinner v. Ry. Labor Execs' Ass'n*, 489 U.S. 602, 624 (1989).

29. *Smith v. Maryland*, 442 U.S. 735 (1979).

30. Declaration of Professor Edward W. Felten, 13, *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

31. *Klayman v. Obama*, 957 F. Supp. 2d 1, 33 (D.D.C. 2013).

32. *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

33. Randy E. Barnett and Jim Harper, "Why NSA's Bulk Data Seizures are Illegal and Unconstitutional," *Federalist Society for Law and Public Policy Studies*, October 21, 2013, http://www.fed-soc.org/publications/detail/why-nsas-bulk-data-seizures-are-illegal-and-unconstitutional.

34. Memorandum from the Office of the Director of Defense Research and Engineering to the Chairman of the Defense Science Board on the Report of the Defense Science Board Task Force on Secrecy, July 1, 1970, http://www.fas.org/sgp/othergov/dsbrep.html.

35. Dana Priest and William M. Arkin, "A Hidden World, Growing Beyond Control," *Washington Post*, July 19, 2010, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/.

36. Gabe Rottman, "On Leak Prosecutions, Obama Takes it to 11. (Or Should We Say 526?)," *Washington Markup* (blog), ACLU, October 14, 2014, https://www.aclu.org/blog/free-speech/leak-prosecutions-obama-takes-it-11-or-should-we-say-526.

37. Margaret Sullivan, "The Danger of Suppressing the Leaks," *New York Times*, March 9, 2013, http://www.nytimes.com/2013/03/10/public-editor/the-danger-of-suppressing-the-leaks.html.

38. "A Journalist 'Co-Conspirator,'" *Wall Street Journal*, May 20, 2013, http://www.wsj.com/articles/SB10001424127887324102604578495253824175498.

39. Floyd Abrams and Yochai Benkler, "Death to Whistle-Blowers?," *New York Times*, March 13, 2013, http://www.nytimes.com/2013/03/14/opinion/the-impact-of-the-bradley-manning-case.html.

40. Jennifer Lynch and Trevor Timm, "The Dangers in Classifying the News," *Deeplinks* (blog), Electronic Frontier Foundation, October 18, 2011, https://www.eff.org/deeplinks/2011/10/dangers-classifying-news.

41. "The Obama-Biden Plan," Change.gov, http://change.gov/agenda/ethics_agenda/.

42. See William Leonard, "Classification: Radical, Let Alone Incremental, Reform Is Not Enough!," *Informed Consent*, August 9, 2009 (on file with author).

43. "Joint Inquiry into the Terrorist Attacks of September 11, 2001: Hearing Before the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence," 107th Cong. 683 (2002) (statement of Eleanor Hill, Staff Dir. of Joint Inquiry Comm.), http://www.intelligence.senate.gov/pdfs/1071086v2.pdf.

44. 9/11 Commission Report, at 276. See also id. n.107. http://www.9-11commission.gov/report/911Report.pdf.

45. *United States v. Farinella*, 558 F.3d 695, 700 (7th Cir. 2009).

46. Ryan Lizza, "State of Deception: Why won't the President rein in the intelligence community?," *New Yorker*, December 16, 2013, http://www.newyorker.com/magazine/2013/12/16/state-of-deception.

47. Eric Lichtblau, "In Secret, Court Vastly Broadens Powers of N.S.A.," *New York Times*, July 6, 2013, http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all&_r=0.

48. James Staten, "The Cost of PRISM Will Be Larger Than ITIF Projects," *Forrester* (blog), August 14, 2013, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects. Staten wrote, "Earlier this month The Information Technology & Innovation Foundation (ITIF) published a prediction that the U.S. cloud computing industry stands to lose up to $35 billion by 2016 thanks to the National Security Agency (NSA) PRISM project, leaked to the media in June. We think this estimate is too low and could be as high as $180 billion or a 25% hit to overall IT service provider revenues in that same timeframe."

49. *United States v. Robel*, 389 U.S. 258, 264 (1967).