Cite as Brenner, 9 J. NAT'L SECURITY L. & POL'Y __ (forthcoming 2018)

A Review of "The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age" by Laura K. Donohue

Joel Brenner*

Professor Donohue has given us a full-throated denunciation of the entire legal framework regulating the government's collection of data about American citizens and permanent residents, whom we call "United States Persons."[1] She contends that in the wake of the digital revolution, current law "is no longer sufficient to guard our rights"[2] – she's right about that – and that we have actually returned to the untrammeled issuance of general warrants that characterized the eighteenth century British practice that our nation's Founders rebelled against. She proposes a thorough revision of the laws governing the collection of foreign electronic intelligence within the United States and abroad, and she advocates severe limitations on the collection and access to digital information of any sort. I will address the merits of her arguments – but first a threshold question: Is this really a book about the future of foreign intelligence?

From the half-century leading to the end of the Cold War, the nearly exclusive control by nation-states over the tools of spy craft seemed like a natural monopoly. The complexity of modern cryptography from the 1930s onward put high-end encryption beyond the capability of all but a few intelligence services.[3] Most forms of electronic intelligence gathering – advanced listening devices, sophisticated radars and antennae, and measurement of weaponry signatures, for example – were also developed by governments and were unavailable to most nations. Free-lance and commercial human spying never went away, but they became the exception after Europe was rigidly divided into East-West blocs, and as border controls, which hardly existed before World War I,[4] became the norm.

Governments' monopoly over most of the tools of spycraft did not disappear overnight. Between the collapse of the Soviet Union in 1991 and the 9/11 attacks a decade later, however, the monopoly largely vanished as these tools became the products and instruments of the marketplace. The encryption now found in an ordinary smart phone can be broken only with extraordinary effort, if at all, and its computing power dwarfs anything available to the presidents

* Joel Brenner is a senior research fellow at the Massachusetts Institute of Technology. He is the former inspector general and senior counsel of the National Security Agency and former head of U.S. counterintelligence under the first three directors of national intelligence. He gratefully acknowledges the assistance of Alexander Loomis of Harvard Law School.

[1] 50 U.S.C. § 1801(i) (2012).

[2] LAURA K. DONOHUE, FUTURE OF FOREIGN INTELLIGENCE 3 (2016).

[3] *See generally* DAVID KAHN, THE CODE BREAKERS: THE STORY OF SECRET WRITING (1967).

[4] *See History of Passports*, GOVERNMENT OF CANADA, http://www.cic.gc.ca/english/games/teachers-corner/history-passports.asp (last visited Nov. 29, 2017). For a colorful evocation of the period, see EVELYN WAUGH, WHEN THE GOING WAS GOOD 7-10 (1946).

and premiers of a previous generation. The monopoly of the two Cold War superpowers over high-thrust rocketry and orbital satellites is ancient history. Countries around the world now compete with, or rely on, private companies to do the heavy lifting. The commercial satellite imagery readily available to the public is also jaw-droppingly good, at resolutions that were state secrets only a few years ago. The advantage of states over private enterprises in surveillance, counter-surveillance, and clandestine operations has not disappeared, but the private sector is catching up fast. At the same time, the digitization of information and the consequent explosion of freely available data have both delighted and disoriented us, turning private lives inside out and making secrets difficult to keep for individuals, businesses, and governments alike – including intelligence services. The ubiquity of data has also made open-source intelligence more valuable than ever and has called into question the scope, though not the necessity, of secret intelligence gathering and analysis. Given advances in the application of artificial intelligence, the pace of change is not slowing down. The challenges this environment presents to intelligence services are severe.[5] In the wake of these developments, the distinction insisted upon by the grand viziers of Langley, South Bank Legoland, and Moscow Center between *i*ntelligence (that's what *you* think, with a small "i") and *I*ntelligence (that's what *we* think, with its reifying initial capital) appears risible.

Profound political, ethical, and legal challenges also confront agencies that make a living stealing secrets. Stealing secrets involves breaking the laws of other nations, including friendly ones. In an increasingly integrated world, we can expect new norms, and perhaps laws, to control that kind of activity. Drones and robots also present still-unresolved questions.[6] Profound issues of mission focus are also up for grabs – whether the CIA will continue to be dominated by its para-military side,[7] and whether the National Security Agency ("NSA") is destined to remain essentially a targeting service for a war machine at the expense of its national intelligence

[5] JOEL BRENNER, AMERICA THE VULNERABLE, INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE at 127-53 (2011). The near-monopoly of nation-states over the means of intelligence gathering was actually an anomaly; we are returning to the historical norm. *Id.* at 190-199.
[6] *E.g.*, George R. Lucas, Jr., *Automated Warfare*, 25 STAN. L. & POL'Y REV. 317, 327 (2014).
[7] *See, e.g.*, Jane Harman, *Disrupting the Intelligence Community: America's Spy Agencies Need an Upgrade*, FOREIGN AFFAIRS, March–April 2015, https://www.foreignaffairs.com/articles/united-states/2015-03-01/disrupting-intelligence-community
[http://web.archive.org/web/20150823124519/https://www.foreignaffairs.com/articles/united-states/2015-03-01/disrupting-intelligence-community].

mission.[8] Distinguishing domestic from foreign communications is increasingly difficult, heightening the need to regulate this aspect of foreign intelligence operations.[9]

Opening a book entitled *The Future of Foreign Intelligence*, this is the platter of issues one would expect on the table. But from this menu, the only dishes Professor Donohue serves up are the government's access to domestic digital data and the legal difficulties that arise from the inevitable mingling of domestic and foreign communications. Her book thus has little to do with the future of foreign intelligence, and rather than evaluate it as such, we will do better to accept it as the book her subtitle accurately describes: *Privacy and Surveillance in the Digital Age*. This is not a mere quibble about a title. Her argument is infected with a fundamental confusion between the scope and purpose of the Foreign Intelligence Surveillance Act ("FISA") and the general regulation of foreign intelligence, and that confusion is reflected in the title. In any case, privacy and surveillance are topic enough for a brief but passionate argument about the constraints (or as she would say, the lack of constraints) on the government's ability to vacuum up everyone's digital exhaust. Professor Donohue shapes this conversation through her teaching and as one of a handful of *amici curiae* appointed to advise the Foreign Intelligence Surveillance Court ("FISC") in cases of broad applicability. On these issues her views demand respectful attention.

I. The Argument

[8] *See* Dana Priest, *NSA Growth Fueled by Need to Target Terrorists*, WASH. POST (July 21, 2013), https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html; MICHAEL V. HAYDEN, PLAYING TO THE EDGE: AMERICAN INTELLIGENCE IN THE AGE OF TERROR 329 (2016) ("Years after I left government, I reviewed my Thursday morning briefing scripts for the President and was struck by how much they focused on terrorism and within terrorism how much they were about South Asia – Pakistan and Afghanistan"); Harman, *supra* note 7 at 105 ("What role does that leave for the NSA? Its top priorities should be code-making, code-breaking, and cyberwarfare. Washington will still need the capacity to penetrate secure state networks and prevent its enemies, state and nonstate, from doing the same. Although the NSA has demonstrated abilities in this sphere, it needs to focus on keeping pace with talented Chinese, North Korean, Russian, and nonstate hackers."). Drawing causal connections between NSA's current priorities and missed opportunities is of course difficult. But in just the last few years, many have criticized America's spies for failing to predict national shifts abroad. *See, e.g.*, Stephen Blank, *Turkey: Another US Intelligence Failure*, ATLANTIC COUNCIL (July 20, 2016), http://www.atlanticcouncil.org/blogs/ukrainealert/turkey-another-us-intelligence-failure; James S. Robbins, *American Intelligence Failure In Syria*, USA TODAY (Oct. 14, 2015), http://www.usatoday.com/story/opinion/2015/10/14/syria-russia-islamic-state-intelligence-column/73861676/; John Crawley, *U.S. Intelligence Under Fire Over Ukraine*, CNN (Mar. 5, 2014), http://www.cnn.com/2014/03/05/politics/ukraine-u-s-intelligence/.

[9] *See also* Michael Morell, *The Importance of Intelligence*, AUSTRALIAN STRATEGIC POLICY INSTITUTE: THE STRATEGIST (Aug. 31, 2016), http://www.aspistrategist.org.au/the-importance-of-intelligence/; HAYDEN, *supra* note 8, at 422 ("Long before Snowden, I was asking CIA's civilian advisory board 'Will America be able to conduct espionage in the future inside a broader political culture that every day demands more transparency and more public accountability from every aspect of national life?' The board studied it for a while and then reported back that they had their doubts.").

Her arrows are aimed chiefly at two specific targets. The first is the Supreme Court's "third-party doctrine," which denies Americans a constitutionally based privacy interest in data they give to third parties, including common carriers and other digital platforms that provide essential services. I enlarge her attack on this doctrine.

Her second major target is the 2008 amendments to the Foreign Intelligence Surveillance Act of 2008[10] (the "FISA Amendments Act" or "FAA"). That law allowed the NSA to collect, without a warrant, communications between targeted foreign citizens and Americans. She and I agree reforms are needed. But she would go further than I would by subjecting foreign intelligence collection to strict warrant requirements. That proposal misunderstands FISA's purpose and constitutional limitations.

Professor Donohue also presents a jaundiced but, as I will explain, undeveloped view of the area of government operations known as intelligence oversight. Finally, she contends that criminal law and the law governing intelligence gathering have little or nothing to do with one another and that the distinction between them is both meaningful and clear. Her most startling and potentially consequential proposal is to resurrect that doctrine by re-erecting "The Wall" that, until 2002, required the complete separation of criminal investigations from all information gathered using foreign intelligence sources and methods. In my view, the destruction of that barrier was one of the most significant and desirable changes to the organization of the federal government following the attacks of 9/11.

I examine her arguments in this order.

II. Third-Party Doctrine and Metadata

In the early 1970s, federal authorities served subpoenas on two banks with which a bootlegger named Miller did business. The banks complied. Miller moved unsuccessfully to suppress the banks' evidence on the grounds that it had been seized without warrants in violation of the Fourth Amendment. He was later convicted of various federal crimes. The Court of Appeals for the Fifth Circuit overturned his conviction, but the Supreme Court reversed. The Court held that:

1. the subpoenaed papers were the bank's business records;
2. the bank was required to maintain them under the Bank Secrecy Act of 1970;[11] and

[10] FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2435, 2436.
[11] 12 U.S.C. § 1829b(d) (2012).

3. Miller had no reasonable expectation of privacy either in the bank's copy of the records or in the original checks, which were negotiable instruments used in commercial transactions.[12]

Miller's holding could easily have been confined to negotiable instruments or to business records maintained under statute. But three years later, in *Smith v. Maryland*[13] the Supreme Court expanded *Miller* to cover any information given to any third party. Petitioner Smith had been convicted of robbery based in part on telephone numbers collected from a pen register placed on his phone without a warrant. Holding that Smith had no Fourth Amendment interest in the phone company's business records, the Court expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial."[14] For good measure the Court added that if Smith did have such an expectation of privacy, it was not one society was prepared to recognize as reasonable. Smith had "voluntarily conveyed" his dialing information to the phone company[15] and had therefore "assumed the risk" that the company would reveal the information to the police. We now had a broad, clearly articulated third-party doctrine: "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[16]

Miller and *Smith* were both based on the "reasonable expectation of privacy" test of *Katz v. United States*.[17] With rare exceptions,[18] lower courts have repeatedly reaffirmed the third-party doctrine. But as Professor Donohue makes clear, that doctrine no longer protects reasonable expectations of privacy. During the 1970s, people only shared information with third parties (other than the bank and the phone company) by handing a box of papers to their lawyers, accountants, or business associates. There were no permanent records of people's messages to their family and friends. Today, by contrast, nearly all information is routinely digitized and shared with cloud service providers. If your smartphone or laptop is backed up by Google, Apple, or anyone else, you have no constitutional privacy interest in its contents. People increasingly keep all manner of personal and business records "on" their smartphones, which combine the features of filing cabinets, photo albums, contact directories, diaries, credit cards, and so forth all in one place. Dating apps record people's sexual preferences and romantic liaisons. And unlike the defendant's phone in *Smith*, which was tethered to a wall, mobile phones

[12] United States v. Miller, 425 U.S. 435, 442 (1976).
[13] Smith v. Maryland, 442 U.S. 735 (1979).
[14] *Id.* at 744.
[15] It would have been more accurate to say that his data had been automatically captured by a common carrier which at that time was still a monopolist of an essential means of communication.
[16] *Smith*, 442 U.S. at 744-45.
[17] 389 U.S. 347 (1967).
[18] *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 44 (D.D.C., 2013), *vacated*, 800 F.3d 559, 562 (D.C. Cir. 2015) (per curiam).

move freely.[19] Mobile phones, especially smartphones, are tracking devices. Uber and Lyft, the weather app, the city transportation app, and many others have little or no value if they do not know exactly where you are. Your mobile phone must also know where you are at all times in order to connect your calls, so it constantly communicates with cell towers even when you're not on the phone. Companies keep this data and often sell it. Our phones thus record not merely where we are now, but where we have been and how long we were there. Soon, thanks to the third-party doctrine, no one will have a reasonable expectation of privacy in almost anything.[20]

Technological developments notwithstanding, the third-part doctrine was also bad law to begin with. It treats a substantive constitutional right as if it were merely an evidentiary privilege that is automatically lost when shared with anyone else. That view does not reflect reasonable expectations of privacy, and it never did. If you disclose to a third party an otherwise privileged conversation with your lawyer, you lose the privilege. But this is merely a rule of evidence. We do not use the subsequent third-party disclosure to declare that the client had no right to share information in confidence with the lawyer in the first place. Rather, we recognize that lawyer and client, like doctor and patient, communicate in a zone of confidence. The third-party doctrine recognizes no such zone for information that ordinary people must, as a necessity of life, share with companies that promise to protect their privacy.[21] In *Miller*, for example, the petitioner's bankers testified that they regarded their customers' records as confidential,[22] and the

---

[19] Americans are fast giving up landlines. *See* Stephen J. Blumberg & Julian V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey*, CTRS. FOR DISEASE CONTROL (December 2014), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201412.pdf ("Preliminary results from the January–June 2014 National Health Interview Survey (NHIS) indicate that the number of American homes with only wireless telephones continues to grow. More than two in every five American homes (44.0%) had only wireless telephones . . . . during the first half of 2014—an increase of 3.0 percentage points since the second half of 2013. More than one-half of all adults aged 18-44 and of children under 18 were living in wireless-only households.").

[20] Cisco forecasts that cloud usage will grow three-fold from 2014-2019, and that by 2019, "more than four-fifths (86 percent) of workloads will be processed by cloud data centers; 14 percent will be processed by traditional data centers." CISCO, *Cisco Global Cloud Index: Forecast and Methodology, 2015–2020* (2016), [http://web.archive.org/web/20160204180157/http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf]. Individuals and businesses are moving to third-party cloud services, particularly in the United States. *See, e.g.*, STATISTA, *United States: Brand preferences for cloud data storage in Q1 2016, by income*, https://www.statista.com/statistics/550987/united-states-brand-preferences-for-cloud-data-storage-by-income/ (last visited June 14, 2016). This trend is bound to grow worldwide. In 2015, 3.37 billion people, or 46.4 percent of the world's population, had Internet access. In North America, the penetration percentage was 87.9 percent. Even in the least connected places, access is growing at a dramatic rate. INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm (last visited June 14, 2016). Facebook alone claimed 2 billion monthly active users as of June 2017. *See* Josh Constine, *Facebook now has 2 Billion Monthly Users… And Responsibility*, TECHCRUNCH.COM (June 27, 2017), https://techcrunch.com/2017/06/27/facebook-2-billion-users/.

[21] As the doctor-patient example illustrates, we know how to create such a zone even when it has no constitutional underpinning. *See also* Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (building on breach of trust cases in developing a proposed right to privacy at common law, breach of trust may be ready for a come-back in the privacy wars).

[22] 425 U.S. at 449.

prosecution admitted as much.[23] But *Miller*'s holding effectively eliminated any such confidence that reasonable customers had.[24] In short, the reasonable expectation test of *Katz* would have fit the facts in *Miller* like a glove, if the Court had only tried it on.[25]

Miller and *Smith* thus represent an attempt to define a substantive right through a mechanical, inapt test borrowed consciously or unconsciously from the law of evidence. The attempt was always flawed in principle. But thanks to technological developments putting virtually all our private information in third parties' hands, it now produces intolerable results. So Professor Donohue is right: Supreme Court precedent does not protect ordinary citizens from government's unreasonable intrusions into private lives. It requires re-thinking.

Several members of the Court appear to agree, as Justice Scalia's opinion for the Court and the concurrences in *Jones v. United States*[26] suggest. *Jones* presented the question whether attaching a GPS tracking device to a man's automobile, and subsequently using that device to monitor the vehicle's movements on public streets, constituted a Fourth Amendment search or seizure. A five-justice majority declined to apply the rule on the narrow ground that, notwithstanding *Katz*'s expectation of privacy test, the government had trespassed in affixing the device to the vehicle.[27] The majority knew that its disposition of the case left the hard question lurking in the wings: "It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[28] Justice Sotomayor concurred but issued a separate opinion to emphasize the larger issue. "I would ask," she wrote, "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." Her implication was clear: "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[29] Justice Alito, joined by Justices Ginsburg, Breyer, and

---

[23] *Id.* at 448-49 (Brennan, J., dissenting).
[24] See *Smith*, 442 U.S. at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").
[25] Nor is it sufficient to say that the bank was obliged to keep the records by the Bank Secrecy Act, because a requirement to preserve records to make them amenable to legal process does not prescribe the process by which the government may obtain them. Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970, 31 U.S.C. § 5311 (2012). If these records are entitled to Fourth Amendment protection, the legislature had no more right to violate that right than did the executive. U.S. Const. amend. IV. The assumption-of-risk rationale is even flimsier, as one could as well say that a party assumes the risk that anyone owing a duty of confidence, including a lawyer or physician or spouse, would breach it.
[26] 565 U.S. 400 (2012).
[27] "[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." *Id.* at 409.
[28] *Id.* at 412.
[29] *Id.* at 416, 417 (Sotomayor, J., concurring).

Kagan, had the same concern. "[I]f long- term monitoring can be accomplished without committing a technical trespass — suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car — the Court's theory would provide no protection."[30] We thus had all nine members of the Court expressing discomfort both with the third-party doctrine and its interplay with *Katz*.[31]

Jones may mark the beginning of the end for an across-the-board third-party doctrine, but the end is unlikely to come at a single stroke. Congress has displayed no enthusiasm for legislating in this area, and courts will be slow to abandon a mechanically applied doctrine that produces clear results.[32] But doctrinal clarity costs too much in today's digital economy. The third-party doctrine destroys information privacy and yields unreasonable results. It is premised on technologically obsolete assumptions about the world – a point that Professor Donohue makes wonderfully clear – and it was unsound from the beginning.

In its time, *Katz* expanded individual rights by holding that citizens enjoy a zone of privacy that moves with them. But its reasonable expectation standard should be re-thought. On the one hand, it is insufficient to deal with technological advances that are rapidly destroying expectations of privacy that still seem reasonable to many people; on the other hand, it could be useful in fashioning protections for information that must, as a practical matter, be shared with third parties. Professor Donohue thinks we may be in "a pre-*Katz* moment," ripe for a doctrinal shift. When a majority of the Court declares that "Fourth Amendment rights do not rise or fall with the *Katz* formulation,"[33] she's probably right.

III. Collection Under FISA

Professor Donohue mounts three principal attacks on the FAA. *First*, it authorizes the collection of bulk electronic metadata without a warrant, by which she apparently means a Title III warrant.[34] She asserts this practice is unconstitutional, by which she presumably means that in

---

[30] *Id.* at 425 (Alito, J., concurring in the judgment). Justice Alito also suggested that the Congress rather than the courts should take the lead in this area. *Id.* at 427-28.

[31] Two years later, a unanimous Court held that digital technology required changes to traditional Fourth Amendment doctrine in *Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. . . . Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives – from the mundane to the intimate.").

[32] Abandoning the third-party doctrine per se could also have implications for the law governing the use of informants by the government. *See* United States v. White, 401 U.S. 745 (1971).

[33] *Jones*, 565 U.S. at 406.

[34] Professor Donohue uses the term "warrant" to refer to both Title III and FISA orders. Under FISA, surveillance orders are formally known simply as orders rather than warrants, apparently because the drafters of that statute wished to make clear that the President's Article II power to collect foreign intelligence was not subject to the Fourth Amendment. I follow the statutory usage. The distinction can be significant. *See In re* Warrant to Search a

her view it should be unconstitutional, because she knows that the third-party doctrine, just discussed, denies citizens a Fourth Amendment right to privacy in communications metadata.[35]

Second, she argues that a FISA order that authorizes the collection of large numbers of international communications that begin or terminate in the United States between foreign persons overseas who are associated with terrorism is unconstitutional. Instead, she believes a FISA order must be restricted to a single, particularized call or message. She provides no constitutional foundation for her position, and there is none.

Third, she argues that the government's unrestrained ability to retain and examine lawfully collected intercepts of conversations involving U.S. Persons under section 702 is unconstitutional and should be regulated. Here again Professor Donohue's arguments about constitutionality are perplexing, at least to this reader, because they are not based on a parsing of constitutional text and Supreme Court decisions as they apply to particular parts of FISA. Instead, she offers a lively disquisition, fully a quarter of the book, on the origins of the Fourth Amendment and the history of general warrants in the run-up to the American Revolution.[36] As a former member of the guild of legal historians, I found this background relevant but, standing alone, unpersuasive. Nevertheless, I agree with her that access to stored 702 data should be regulated, though I doubt we agree on how to do it.

While I find common ground with several of Professor Donohue's specific proposals for further FISA reform, I see two major weaknesses in the foundation of her attacks on FISA collection and thus with her broader argument. The first weakness – in my view, error – is constitutional and legal. It concerns the scope and purpose of the FISA statute, which were limited in their reach by the President's independent constitutional authority to collect foreign intelligence. The second weakness is partly technological and partly a result of failing to acknowledge the altered intelligence challenge in the form of metastasized terrorism that confronts anyone, regardless of political inclination, who wishes to regulate the monitoring of communications. Before addressing these points, however, a brief history of bulk metadata and FISA collection since the attacks is in order.

A. Origins of Bulk Collection and the "702 Program"

Certain E-Mail Account, 829 F.3d 197, 214 (2d Cir. July 14, 2016), *vacated sub nom.*, United States v. Microsoft Corp., 138 S.Ct. 1186 (2018).

[35] *See, e.g.*, United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc); United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016), *cert granted*, 137 S. Ct. 2211 (2017); *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 136 (3d Cir. 2015); United States v. Guerrero, 768 F.3d 351, 358-59 (5th Cir. 2014).

[36] Characterizing arguably overbroad orders as general warrants strikes me as wildly exaggerated, and it would no doubt surprise the judges of the FISC, who spend considerable effort crafting restraints they appear to find meaningful. She concedes, "There are some differences between the general warrants about which the Framers were concerned and those that mark the realm of foreign intelligence today." DONOHUE, *supra* note 2, at 94. Among other things, FISA orders are limited in scope and must have a foreign intelligence nexus.

Shortly after 9/11, the Bush Administration put in place a surveillance program called STELLAR WIND. That program authorized NSA to intercept communications between persons overseas with known terrorist affiliations and persons in the United States. It also authorized the collection of bulk metadata (that is, information about a communication but not its contents)[37] from U.S. telecommunications carriers in order to understand who the persons on the U.S. end of those calls were communicating with. Through link analysis, these metadata connections could be followed for three "hops," thereby gathering call information about a huge number of domestic calls. The program was authorized by Presidential order, outside the FISA structure. FISA at that time did not address metadata collection. Metadata analysis was beginning to play a critical role in wiping out terrorist networks overseas,[38] however, and the Bush Administration believed it would similarly be critical in rolling up any of those networks that extended into the United States.

By late 2003, however, some government officials had become concerned about the legal authority to collect bulk metadata.[39] Consequently, in July 2004 the collection of bulk *Internet* metadata quietly was moved under section 214 of the PATRIOT Act (which amended section 402 of FISA). That statute permits pen registers and trap-and-trace devices, but authorizations for such devices had previously been used only for specific telephone numbers or Internet addresses. However, then-chief judge of the FISC District Judge Colleen Kollar-Kotelly was persuaded that the statute could be used to collect Internet metadata in bulk in real time.[40] Suffice it to say that this was a novel and controversial interpretation of section 214 that vastly expanded the scope of the government's statutory power to collect bulk metadata. And it occurred in secret.

---

[37] Offices of the Inspectors General of the Department of Defense, Departmet of Justice, Central Intelligence Agency, National Security Agency, and Office of the Director of National Intelligence, *Report on the President's Surveillance Program* (the *"Joint IG Report"*) (July 2009) v. 1 at 8, available at https://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html, accessed May 21, 2018. Telecommunications metadata includes such information as the IP address of the other party to the communication, the path taken by the communication, and its duration. Id.

[38] HAYDEN, *supra* note 8, at 76. For a description of how this played out in Iraq, *see*, Shane Harris, *How the NSA Became a Killing Machine*, THE DAILY BEAST (Nov. 9, 2014), http://www.thedailybeast.com/articles/2014/11/09/how-the-nsa-sorta-won-the-last-iraq-war.html. For a discussion of the benefits of NSA programs, *see generally* John McLaughlin, *NSA Intelligence-Gathering Programs Keep Us Safe*, THE WASH. POST (Jan. 2, 2014), https://www.washingtonpost.com/opinions/nsa-intelligence-gathering-programs-keep-us-safe/2014/01/02/0fd51b22-7173-11e3-8b3f-b1666705ca3b_story.html?utm_term=.3ef8662883bd; Philip Mudd, *Mapping Terror Networks: Why Metadata Matters*, THE WALL STREET JOURNAL (Dec. 29, 2013), http://www.wsj.com/articles/SB10001424052702304367204579270472690053740.

[39] *See* BARTON GELLMAN, ANGLER: THE CHENEY VICE PRESIDENCY 151 (2008); JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 181–82 (2007).

[40] *See* Undated Opinion by Judge Colleen Kollar-Kotelly Declassified Without Date or Caption, at 20-21 (FISA Ct.), https://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

The portion of STELLAR WIND relating to the interception of the content of U.S.-foreign calls (but not the portion relating to bulk metadata collection) was exposed by the *New York Times* in December 2005. The disclosure increased the sense of urgency within the Justice Department's Office of Legal Counsel that the telephony portion of metadata collection should also be given a firmer and explicit statutory basis.[41] In May 2006 the collection of bulk *telephony* metadata was moved under section 215 of the PATRIOT Act, which had amended section 501 of FISA. That statute authorized the government to obtain certain business records through legal process.[42] Technically, this meant that NSA stopped "collecting" telephony metadata in real time as part of its intelligence mission and was instead merely obtaining business records through legal process. Practically speaking, however, there was no difference because the business records went to the government more or less as they were generated. Thanks to the third-party doctrine discussed above, this program was entirely constitutional.

The following year, in August 2007, Congress passed the Protect America Act ("PAA") to provide clear statutory authority to collect the *content* of communications between a person overseas and a person in the United States,[43] but that authority expired after only eighteen months. After a hiatus, Congress passed the FAA in July 2008. It remains in effect. Unlike the original FISA, the FAA required a FISA order before a U.S. Person could be targeted, even if that person was overseas, in circumstances where a Title III warrant would be required in a criminal case.[44] This was a significant expansion of FISA's regulatory scope and, to that extent, an expansion of civil liberty.

But the FAA also created what is often called the "702 Program," which is one of Professor Donohue's chief targets. As amended by the FAA,[45] Section 702 permits "the targeting

---

[41] Professor Donohue would deny that the program had *any* statutory basis. She dismisses without discussion the Bush administration's reliance on the Authorization for Use of Military Force ("AUMF") – as if it were frivolous to argue that intelligence collection against persons in communication with the enemy is a normal incident of war-making authority. *See* Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001). For the administration's arguments about its effect, *see* U.S. Dep't of Justice, Att'y Gen., Opinion Letter on Legal Authorities Supporting the Activities of the National Security Agency Described by the President (January 19, 2006), https://www.justice.gov/sites/default/files/olc/opinions/attachments/2015/05/29/op-olc-v030-p0001.pdf. For another view of the limits of the President's Article II power, *see* David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb – A Constitutional History*, 121 HARV. L. REV. 941 (2008).

[42] Internet service providers, unlike phone companies, do not keep business records of communication data. Hence this change was limited to the telephony portion of the metadata program.

[43] Protect America Act of 2007, Pub. L. No. 110-55, § 105B, 121 Stat. 552. The PAA also dropped the requirement of a FISA order for foreign-to-foreign communications that happened to "transit" the United States. § 105A. Under the old rule, NSA could freely collect that same communication if it captured it, say, from a satellite signal or a cable overseas, but it needed a FISA order if it captured the communication off a wire in the United States. *Compare* 50 U.S.C. § 1801(f)(2) (2006), *with* § 1801(f)(3) (2006). That requirement protected no one's privacy. It merely regulated the place of interception.

[44] *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703(a)(1), 122 Stat. 2436, 2448.

[45] FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438-48 (codified as amended at 50 U.S.C. § 1881 (2015)).

of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[46] In this context, "foreign intelligence information" means the contents of communications and not merely metadata. A FISA order is not required for this collection. Rather, the Attorney General and the Director of National Intelligence select the information to "target" and then direct electronic communications providers to turn over this information. If the government has "reasonable articulable suspicion" that a foreign person has a terrorist connection, that person may be targeted when the foreign person communicates with someone in the United States. If, for example, a known terrorist overseas is having conversations with a U.S. Person in Minneapolis, our agencies may collect that communication. However, an agency may not do so if the purpose of the collection is really to target the person in Minneapolis. That would be "reverse targeting." Electronic communications service providers may challenge these directives before the FISC and appeal to the FISA Court of Review. By long-standing practice, the database of 702 information may be accessed at any time by intelligence or law enforcement officials without court approval and may be queried with any search term, including U.S. Person identifiers.

Professor Donohue objects vehemently to this program. It appears she would subject 702 collection to the criminal warrant process of Title III. In my view, she reaches this position based on a misunderstanding of FISA's purpose and an unsupportable view of the constitutional requirements governing foreign intelligence collection.

B. FISA's Purpose and Constitutional Requirements

Professor Donohue confuses FISA's purpose with the general regulation of foreign intelligence. This may account for the book's inapt title. She asserts: "FISA represented the culmination of a multibranch, multiyear, cross-party initiative *directed at bringing the collection of foreign intelligence within a circumscribed legal framework*" (emphasis added).[47] This is not true. Foreign intelligence collection is a broad category, occurring in many ways through a variety of human and technological means and gathered against targets that are overwhelmingly outside the United States. FISA brought under law one element of that enterprise, namely, the collection of (i) *electronic* foreign intelligence (ii) taken off a wire or from a radio signal (iii) in the United States. That slice of foreign intelligence, because it was collected domestically, could be (and sometimes had been) used to avoid the search-and-seizure strictures of the Fourth Amendment. In the wake of the Church Committee hearings in 1976, Congress enacted FISA to prohibit such evasions.

[46] § 702(a).
[47] DONOHUE, *supra* note 2, at 10.

The constitutional difficulty with Professor Donohue's argument about collection under FISA is inseparable from this issue of FISA's purpose. Contrary to her assertions, foreign intelligence taken from domestic telecommunication networks involves powers granted to *two* branches of government.[48] Under Article I, Congress has the power to regulate interstate and foreign commerce, including telecommunications (at least when used in commerce).[49] But Congress has long deferred to the view that foreign intelligence collection is an executive function vested in the President under Article II of the Constitution,[50] even though there is no express provision for it in Article II.[51] Indeed, the President's power to monitor communications entering and leaving the country has been recognized since Washington's administration.[52] This is why Congress, in enacting FISA, recognized a reasonableness limitation on its power to control communications entering or leaving the country if they concerned foreign intelligence.[53] It certainly did not contest the principle that the President has the "*exclusive function* to

---

[48] Professor Donohue asserts without citation, "Congress and the courts … had previously considered and declined to recognize claims to Article II authority to conduct foreign intelligence gathering inside the United States absent a warrant." *Id.* at __. If this is a reference to *United States v. United States District Court*, 407 U.S. 297 (1972) ("*Keith*"), it is wrong ("[This case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents"). *Keith*, 407 U.S. at 322–23.

[49] U.S. Const. art. I, § 8, cl. 3; LETTER FROM CONSTITUTIONAL LAW SCHOLARS AND FORMER GOVERNMENT OFFICIALS TO MEMBERS OF CONGRESS 7 (July 14, 2006), https://balkin.blogspot.com/NSA.Hamdan.July14.FINAL.pdf.

[50] See DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF NSA DESCRIBED BY THE PRESIDENT (2006), https://epic.org/privacy/terrorism/fisa/doj11906wp.pdf. The Senate Intelligence Committee also acknowledged that the law was not intended to cover "electronic surveillance abroad." S. REP. NO. 95-701, at 7 (1978). While "protect[ing] the rights of Americans abroad from improper electronic surveillance" might raise constitutional issues, it never even occurred to the Committee that the same could be said of the surveillance of non–U.S. Persons. *Id.* at 7 n.2.

[51] *See* Jack Goldsmith, Zivotofsky II *as Precedent in the Executive Branch*, 129 HARV. L. REV. 112, 114 (2015) ("Until *Zivotofsky II*, [executive branch] lawyers had to rely on shards of judicial dicta, in addition to executive branch precedents and practices, in assessing the validity of foreign relations statutes thought to intrude on executive power."); *see also* JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 72 (2007) ("The president's intelligence authority is derived from his enumerated authorities as commander in chief and chief executive, as well as his collective authority over foreign affairs, and to take care that the laws be faithfully executed. As intelligence is an integral function of military command and the conduct of foreign affairs, as a general matter the president has broad derived authority over the intelligence function. Congress has recognized as much in statute.").

[52] *See* CHRISTOPHER ANDREW, FOR THE PRESIDENT'S EYES ONLY: SECRET INTELLIGENCE AND THE AMERICAN PRESIDENCY FROM WASHINGTON TO BUSH 6-12 (1995); *see also* LOUIS HENKIN, FOREIGN AFFAIRS AND THE UNITED STATES CONSTITUTION 111 (2d ed. 1996) ("From our national beginnings, Congress has recognized the President's exclusive responsibility for gathering intelligence, as an extension of his role as 'sole organ' and his traditional function as 'the eyes and ears' of the United States."); BAKER, *supra* note 51, at 71 ("Presidents have engaged in the practice of domestic and foreign intelligence collection since the advent of the United States. . . . [I]n the landline age, presidents routinely authorized electronic surveillance (wiretapping) to collect foreign intelligence.").

[53] *See* S. REP. NO. 95-604, at 16 (1977) ("The basis for this legislation is the understanding – concurred in by the Attorney General – that even if the President has an 'inherent' constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a *reasonable* warrant procedure governing foreign intelligence surveillance.") (emphasis added); *see id.* at 7 ("The Federal Government has never enacted legislation to regulate the use of electronic surveillance within the United States...").

command the instruments of national force, at least when turned against the outside world for the security of our society."[54] The Bush Administration, by acting as if it had the power to conduct the STELLAR WIND program on a long-term, non-emergency basis outside the FISA framework,[55] failed to recognize that it shared constitutional authority over activities involving the telecommunications of the American people. In a mirror image of that error, former Senator Russ Feingold was also wrong to assert, in a flight of rhetorical excess with which Professor Donohue is much enamored, that electronic foreign intelligence is an area of "absolutely clear, exclusive authority adopted by Congress …."[56] This is wrong. Like Senator Feingold, Professor Donohue ignores FISA's purpose and history, which probably accounts for her failure to explain why the standard for obtaining a FISA order, which she criticizes repeatedly, differs from the Title III warrant standard.[57]

Title III was passed in 1968 in response to the Supreme Court's *Katz* decision one year earlier.[58] Congress reacted by crafting standards for issuing surveillance warrants sufficient to meet Fourth Amendment standards in criminal cases. Under Title III, a magistrate may issue a warrant authorizing the executive to acquire the contents of a wire, oral, or electronic communication if:

(1) "there is probable cause for belief that an individual is committing, has committed, or is about to commit" certain crimes; and
(2) if "there is probable cause for belief that particular communications concerning that offense will be obtained through such interception"; and

---

[54] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 645 (1952) (Jackson, J., concurring) (emphasis added); *cf.* Zivotofsky *ex rel.* Zivotofsky v. Kerry, 135 S. Ct. 2076, 2094 ("Throughout the legislative process, however, no one raised a serious question regarding the President's exclusive authority to recognize the PRC – or to decline to grant formal recognition to Taiwan. Rather, Congress accepted the President's recognition determination as a completed, lawful act; and it proceeded to outline the trade and policy provisions that, in its judgment, were appropriate in light of that decision. This history confirms the Court's conclusion in the instant case that the power to recognize or decline to recognize a foreign state and its territorial bounds resides in the President alone.") (internal citations omitted).

[55] The first STELLAR WIND order was signed on October 4, 2001. Thirty-three months later, on July 14, 2004, a FISA order was entered under which the program began to be transitioned to FISA. *Joint IG Report*, v. 1 at 7, 52.

[56] DONOHUE, *supra* note 2, at 36 (citing 154 CONG. REC. S6382 (daily ed. July 8, 2008) (statement of Sen. Feingold)); *cf. Youngstown,* 343 U.S. at 635-38 (1952) (Jackson, J., concurring). *Youngstown* involved competing Congressional and Executive authority where President Truman had ordered the seizure of steel mills on national security grounds during the Korean War. Justice Jackson proposed three categories of presidential acts corresponding to three levels of authority: Category One involved acts taken "pursuant to an express or implied authorization of Congress," Category Two involved acts taken in the "absence of a congressional grant or denial of authority," and Category Three involved acts taken in defiance of the express or implied will of Congress. *Id.*

[57] 18 U.S.C. § 2518 (2012).

[58] Katz v. United States, 389 U.S. 347 (1967), holding that a government interception of a telephone call required a warrant. At the time of the decision, there were no statutory standards for issuing warrants in such cases; hence the need for Title III.

(3) if "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous"; and
(4) if (in most cases) "there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person."[59]

Would the imposition of these requirements on foreign intelligence collection be unreasonable? Surely it would be, because it would irrationally assume that foreign intelligence may not be collected in the United States unless there were probable cause to believe a crime were involved, and because it would be an unreasonable constraint on Executive power. A great deal of foreign intelligence does not involve the commission of crimes cognizable in U.S. courts. The Supreme Court has recognized that there is no constitutional obligation to apply these statutory requirements to "domestic security surveillance [, which] may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"[60] The Court also doubted that such requirements applied to collection "with respect to activities of foreign powers or their agents."[61] If they did apply, we would arguably be in Justice Jackson's third category, in which the President's power is at its lowest ebb. "Courts can sustain exclusive presidential control in such a case only by disabling the Congress from acting upon the subject."[62] Justice Jackson was an eminently practical man. As he said, "any actual test of power is likely to depend on the imperatives of events and contemporary imponderables, rather than on abstract theories of law."[63] He might therefore simply say that where two lawful but different powers both impinge on a single area of governmental activity, Congress must exercise its power – and Congress' power must be construed – in a manner that does not unreasonably impinge on the President's authority and, in this case, on his duty to protect the nation. There are limits on what Congress can do.

In contrast to Title III, the FISA standard to which Professor Donohue objects was created to deal with an entirely different problem than the investigation of crime, namely, the potential misuse of the President's power to collect foreign intelligence in the United States. The President has the power to collect foreign intelligence *even in the United States* without a search warrant.[64] A surveillance operation against a foreign embassy in Washington, for example, has

---

[59] 18 U.S.C. § 2518(3) (2012).
[60] 407 U.S. at 322.
[61] *Id.*
[62] *Youngstown*, 343 U.S. at 637-38.
[63] *Id.* at 637.
[64] *See Katz*, 389 U.S. at 363 (1967) (White, J., concurring) ("Wiretapping to protect the security of the Nation has been authorized by successive Presidents"); *United States v. United States Dist. Ct. for E.D. of Mich.*, 444 F.2d 651, 669–71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson); *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002) ("[A]ll the other courts to have decided the issue [have]

never required a Title III warrant; nor does it now require a FISA order.[65] However, if that power is abused to collect against citizens on the pretext, for example, that the citizen was or might be a member of a foreign-controlled entity, the Fourth Amendment's warrant requirement would be effectively evaded. The purpose of the FISA standard was to police such evasion, not to impose a criminal-law standard on foreign intelligence collection.[66] This is why, under FISA, an interception order may issue if the court finds there is probable cause to believe only that "(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power …; (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power"; and certain procedures are followed to minimize inadvertent collection.[67] Professor Donohue gets this history and purpose all wrong. She writes, "The point of having lowered [FISA] standards [compared to Title III] was to facilitate the collection of information about significant threats to national security."[68] No, it wasn't. Congress was not facilitating executive power; it was regulating a portion of that power severely and for the first time.

Professor Donohue is on stronger ground in her criticism of the lowered standard for the production of business records under FISA. The statute was amended in 2015 so that the government was required merely to certify, not to demonstrate, to the FISC that the records sought were merely relevant to an authorized investigation "to protect against international terrorism or clandestine intelligence activities."[69] In such a case, the magistrate may not inquire further and *must* enter the order. Professor Donohue asserts that the statute as it now stands is unconstitutional on its face, but that would be true only if persons had a constitutionally recognized privacy interest in data given to third parties. At present they do not. I would agree, however, that the relaxed standard has produced a British-style regime of seizure orders independent of the judiciary, and I would strengthen the standard to require the FISC judge to determine that the government has a factual basis for its assertion.[70]

---

held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.")

[65] 50 U.S.C. § 1822(a) (2012).

[66] *Compare* S. REP. NO. 95-604, at 7 (1977) ("This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."), *with id.* at 18 ("[T]he Supreme Court noted that the reasons for domestic surveillance may differ from those justifying surveillance for domestic crimes and that, accordingly, 'different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate needs of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.'") (quoting *Keith*, 407 U.S. at 322).

[67] 50 U.S.C. § 1805(a)(2) (2012).

[68] DONOHUE, *supra* note 2, at 28.

[69] 50 U.S.C. § 1861 (2012).

[70] Professor Donohue also notes that the number of FISA orders now exceeds the number of Title III warrants per year. She asserts there is now a direct relationship between the decline in Title III warrants and the increase in FISA orders. DONOHUE, *supra* note 2, at 30. Her data suggest she may be correct, but a deeper inquiry (and better data) would be required to prove the point. One would think that the changed nature of the threat to the nation had something to do with it.

The statute also creates too much room for evasion of the Title III warrant standard and may thus be unconstitutional *as applied*, even under *Smith*. Suppose the FBI wanted to compel the production of the business records of an American citizen who was not an agent of a foreign power but may have been colluding with a foreign agent in a *different* criminal scheme. The government could get a production order without having to obtain a Title III warrant. It would simply have to assert that evidence in the second scheme would somehow be useful in investigating the first one. That would be a dangerous infringement of constitutional protection against arbitrary executive power, and I hope it could not be defended merely by reference to the President's Article II powers.

C. Technology Effects

The advent of fiber-optic technology long before the passage of the FAA had the unintended effect of expanding the FISA's reach in irrational ways that are not widely understood. When FISA was enacted in 1978, telecommunications meant telephone and telegraph; there was no commercial Internet. Most long distance telecommunications employed a satellite link at some point in the transmission. That is, the electronic impulses representing a caller's voice on a call between, say, New York and Hamburg, or between Hamburg and Tokyo, were sent via radio frequency up to a satellite and then down from a satellite before finishing their journey by copper wire. If NSA wanted to target that communication, it could and usually did collect it though the air, probably from an overseas location, so it was not regulated by FISA. Even if it was collected from a location inside the country, FISA did not regulate the collection as long as no U.S. Person was the target.[71] With the advent of commercial fiber-optic cable on international lines beginning in 1988,[72] international call quality and reliability improved dramatically. But it also meant that the call between Hamburg and Tokyo was probably transmitted through a wire in the United States and thus became subject to FISA if collected in the United States, which was the easier and less risky way to do it. And given the U.S.-centric quality of the worldwide fiber-optic cable networks,[73] many other foreign-to-foreign communications also became subject to FISA. An unintended and perverse result was that a large volume of communications having nothing to do with FISA's purpose was brought under the act. This was a major nuisance, and it meant that in a significant class of cases, FISA was not

[71] As originally passed in 1978, FISA defined "electronic surveillance" as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(f), 92 Stat. 1783, 1785.

[72] Jeremiah Hayes, *A History of Transatlantic Cables*, IEEE COMM. MAG., Sept. 2008, at 42, 47.

[73] *See Submarine Cable Map*, TELEGEOGRAPHY, http://www.submarinecablemap.com [http://web.archive.org/web/20160618040914/https://www.submarinecablemap.com] (last accessed June 18, 2016).

protecting the privacy of U.S. Persons. It was merely regulating the place of collection. The PAA and then the FAA fixed that anomaly.

A typical fiber-optic trunk cable carries a petabit of data per second.[74] The government does not "tap" these cables using alligator clips in the basement wire closet of an apartment building like in a 1940s movie. Interception occurs at a carrier's switching station. If done by the police or FBI under a Title III warrant, the targeting must be precise because the government is forbidden from collecting anything outside the terms of the warrant. In the case of foreign intelligence, however, the situation is largely reversed. The President has the power to collect any communication likely to have foreign intelligence value, except that he must take care not to collect U.S. Persons' communications except as authorized by FISA. This reversal is based on constitutional requirements, but it offends Professor Donohue. She asserts that FISA orders should be limited to "*seizing or monitoring the content carried by a single telephone line, or to and from a particular computer address.*"[75] The Constitution does not require the President to take such a dainty approach to foreign intelligence collection, and Congress appears to believe, correctly in my view, that it has no power to impose such a requirement.

IV. Access to Stored U.S. Person Data

So much for electronic collection under section 702. Let us now turn to the analysis of 702 data and the access to data that intelligence analysis and law enforcement both require. As Professor Donohue correctly notes, the database of information collected under this section has become enormous. It contains the records of a publicly unknown but undoubtedly very large number of communications involving U.S. Persons in the United States communicating with intelligence targets overseas. Our intelligence agencies and the FBI may search that database using U.S. Person selectors for any purpose, without restraint, whenever they feel like it, even years after the collection occurred, even if they have lost interest in the overseas target. This state of affairs is merely the application of the long-standing rule that once a communication of a U.S. Person or anyone else has been lawfully collected, an agency may access that communication for any reason.

I share Professor Donohue's objection to this legal state of affairs under section 702, and the objection will be more powerful if placed in a broader context. We have entered an era when the terms on which the government may search lawfully gathered information are becoming as important as the terms on which the information may be lawfully collected. The government's access to vast quantities of information about U.S. Persons is growing dramatically. U.S. intelligence agencies already hold massive databases of information about Americans. They also

---

[74] Matthew Peach, *NEC and Corning Achieve Petabit Optical Transmission*, OPTICS.ORG (Jan 22. 2013), http://optics.org/news/4/1/29.
[75] DONOHUE, *supra* note 2, at 32 (emphasis added).

have access to readily available commercial databases through a few keystrokes or through the purchase of proprietary databases. The data ocean is expanding as if propelled by a Digital Big Bang, and dealing with it requires automated analytic capabilities at a previously unimaginable scale. Most of this data ocean is held by private companies, whose ability to gather it and whose skill in analyzing it exceed the government's. The vast expansion of the private data market means that the government itself will gather *relatively* less data and purchase *relatively* more of it in open markets. Indeed, in some cases the ability to purchase commercial data in the open market will make restrictions on collection irrelevant.

Historically our laws and regulations have controlled who may *collect* intelligence, whose communications may be collected, how they may be collected, and what may be collected.[76] Once information about U.S. Persons has been lawfully collected, we also regulate how and to whom it may disseminated, but we have not regulated the conditions or frequency under which the collecting agency may access or analyze it. Section 702 is merely an example of this historical way of doing business. The protections afforded to U.S. Persons through collection rules always seemed sufficient to protect our liberty. I predict this is going to change. We are probably at the threshold of a new era. In the future, we are likely to be at least as concerned with the state's ability to access information already collected, or available in the marketplace, as we have been with the conditions under which the state may collect it using its own resources.

Greater attention to data access as opposed to data collection will also be impelled by a change in intelligence agencies' mission. Their task is no longer simply to acquire the communications of known foreign agents or to hunt moles in their own organizations, as was the case throughout the Cold War. Knowing who the foreign targets were was relatively easy. Stealing their communications was hard.[77] That mission is now accompanied by a new one that has deep legal and public support, namely, to discover terrorist networks before they can wreak havoc. In the foreseeable future, this challenge will probably condition the intersection between government's intelligence gathering and citizens' rights more than any other factor, yet it strangely finds no place in this book. In pursuit of terrorists, stealing the secrets is usually the less difficult task. The harder and more important part is knowing who they are, and that involves access, under controlled conditions, to communications data in bulk – to both metadata and to lawfully collected intercepts – and sifting them for information with intelligence value. To a significant degree, therefore, the challenge in intelligence collection has been turned on its head. Whether we like it or not, from now on more and more information will be in government

---

[76] *See, e.g.*, Exec. Order No. 12,333, United States Intelligence Activities, 3 C.F.R. 200 (1981), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), and Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008); 50 U.S.C. § 1801.

[77] *See also* HAYDEN, *supra* note, 8 at 32 ("Intelligence [during the Cold War] was hard work, but it was difficult for our adversary to hide tank armies of Group Soviet Forces Germany or the vast Soviet ICBM fields in Siberia. That enemy was pretty easy to find. Just hard to kill. This was different. This enemy was relatively easy to kill. He was just very, very hard to find.").

hands or easily available to government. Increasingly the questions will be: When can government look at it? And how can we police abuses?

V. Oversight

The subject of potential abuse – by which I mean intentionally or systematically unlawful intelligence collection[78] – brings us to the question of oversight, but this is a subject on which Professor Donohue, after raising it, has little to say. She treats us to a tantalizing observation by Stanford's Professor Scott Sagan, whose work on nuclear weapons policy led him to conclude, in her words, that "the *more* protection one builds into a system, somewhat counterintuitively, the *less* secure it may become." This is a brilliant insight of remarkably limited value here, since hardly anyone (including Professor Sagan[79]) would argue the converse: That the less protection one builds into the system of intelligence oversight, the more secure it is likely to become. Indeed Professor Donohue wants "more robust oversight."[80] But she is vague on what that means. Her only concrete suggestion is to say it would be a good idea to have more people like her – amici curiae appointed by FISC – but this is what the USA Freedom Act actually did in 2015.

What Professor Sagan describes is a version of the shared responsibility trap, in which an actor with partial or redundant responsibility becomes lazy and inattentive in the belief that others have their eyes on the ball ("social shirking," he calls it).[81] As the former inspector general of the National Security Agency during the STELLAR WIND period, that's not how I saw intelligence oversight. My office had its hands full and was deeply involved not only in uncovering abuse after the fact (not usually involving intelligence collection, I might add) but also in preventing it. Different oversight mechanisms in different organizations are designed to accomplish different objectives – they are not redundant – and their critics usually pay insufficient attention to what the different parts are meant to do. It is unreasonable, say, to expect the House and Senate select committees on intelligence to monitor collection activities. Their responsibilities are strategic and general, not tactical and granular. In contrast, it would be reasonable for these budget authorizing committees to require that new collection capabilities be auditable to a standard agreeable to agency inspectors general, who are (or should be) able to

---

[78] Inadvertent collection (e.g., of U.S. Persons' communications in the course of lawful foreign intelligence collection) is anticipated by statute and is not abusive unless it is not mitigated as provided by statute. *See* 50 U.S.C. §1881(h) (2012).

[79] Scott Sagan, *The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security*, 24 RISK ANALYSIS 935, 935-46 (2004) ("The implication of the argument, however, is not that redundancy never works in efforts to improve reliability and security. Moreover, the central policy lesson is not that the U.S. government should reject all proposals to place more security forces at nuclear facilities, given the heightened terrorist threat after the September 11, 2001 attacks. Instead, the lesson is that we need to be smarter in the way we think about redundancy.") (emphasis omitted).

[80] DONOHUE, *supra* note 2, at 136-38.

[81] Sagan, *supra* note 78, at 939. Sagan discussed three factors that vitiate the value of redundancy: common-mode errors, insider threats, and social shirking. *Id.*

monitor collection. But no oversight system will be perfect, and expecting perfection (usually with a handwringing reference to the unanswerable question, Who will watch the watchers?) leads only to the continual imposition of additional oversight mechanisms on top of one another, a tendency that expands the pool of unproductive employment opportunities at the expense of efficiency.

Expecting perfection also leads to what I call the Oversight Paradox: The closer one is to the activity being overseen, the more one will know about how it works, but the less one will be trusted; and the farther one is from the activity, the less one will know but the more one will be trusted. Since the Snowden disclosures, this paradox has been compounded by a different misunderstanding. Agency oversight officials are charged with preventing waste, fraud, and abuse, which includes illegality. But the bulk metadata collection program ordered by the President, personally approved by the attorney general under guidelines approved by the Justice Department, disclosed to the leaders of both houses of Congress and the chairmen and ranking members of both intelligence committees, and sanctioned in particular cases by more than a dozen federal judges *was not unlawful*. The problem was that the law was arguably secret — not to the Congress but to the public. No oversight system is built to deal with the failure of political judgment that led to that circumstance.[82]

VI. Remedies

Professor Donohue and I agree on a number of specific proposals and disagree profoundly on FISA's rationale and constitutional limitations. First, we agree that the 702 database of lawfully collected U.S. Person information should be regulated, though not on how to do it. She asserts that the Constitution requires a Title III warrant before the government can search *its own* database using U.S. Person selectors.[83] This is a novel view, and she provides no support for it. As will be clear in a moment, her proposal is part of an ill-conceived program to re-create the pre-9/11 condition of voluntary ignorance in which the government had to pretend that it did not know things that it did in fact know. If access conditions are going to be imposed, a determination by the Deputy Attorney General that an inquiry was reasonably related to an open federal investigation would suffice to avoid aimless searches of U.S. Person data for an investigatory predicate. In my view, that is the potential evil to be prevented.

Second, we agree that retention limits should apply to known U.S. Person information in the 702 database. I propose a period not to exceed five years.

---

[82] *See* Joel Brenner, Forty Years After Church-Pike: What's Different Now?, Henry F. Schorreck Memorial Lecture at NSA, (May 15, 2015) (available at http://joelbrenner.com/forty-years-after-church-pike-whats-different-now-2/).
[83] Under the USA Freedom Act of 2015, we require a FISA order before the government can access metadata records held by telecommunications providers, but these are third-party records. USA Freedom Act, Pub. L. No. 114-23, § 103, 129 Stat. 268, 272 (2015).

Third, we both favor relieving FISA judges of some of their other workload as Article III federal district judges during their tenure on the FISC.[84]

Fourth, we agree that the standard for the production of tangible things under FISA should be strengthened. Congress should make it the same as the standard for the obtaining a surveillance order under the act. Both orders involve the same infringement on personal liberty, and it is irrational to think that one kind of infringement (acquisition of records of past communications) is less serious than the other (acquisition of current communications).

But then Professor Donohue and I part company because, if her basic diagnosis is constitutionally unsound, her favorite remedy could kill the patient. In her judgment, the fundamental problem with the FAA is that it muddled a supposedly clear distinction between foreign intelligence and criminal law. Consequently, she proposes that we build this dichotomy back into law and government operations. This is an appalling proposition, because if we have learned anything since 9/11, it is that the distinction was illusory. The barrier between criminality and foreign intelligence gathering was not done in by a nefarious ideological attack; it collapsed under the weight of the Twin Towers and our inability to track terrorists effectively.[85] Foreign intelligence investigations often, even usually, involve criminal acts,[86] and they often touch our own citizens and territory. Wishful thinking embellished with a different verbal formula will not make these facts go away. Professor Donohue's refusal to acknowledge them then leads her to propose the re-erection of "The Wall"[87]—that is, the hermetical separation of criminal and intelligence investigators that had created a state of self-imposed blind man's bluff between law enforcement and intelligence officials before 9/11, and the abolition of which was essential to our ability to maintain our security. Re-erecting that Wall would mean abolishing or neutering the Justice Department's recently created National Security Division and re-imposing the voluntary ignorance and dysfunctionality by which the government's left hand had no idea what its right was doing. Fortunately, the extreme undesirability of this proposal is matched by the extreme unlikelihood of its being adopted. Neither the country nor the courts are likely ever again to endorse self-imposed ignorance as a national policy.

---

[84] Professor Donohue criticizes the political composition of the FISC as heavily Republican and therefore, in her view, anti-civil liberties. Apart from the dubious connection with political affiliation and libertarian views, she assumes that the number of Democrats on the court reflects the number of Democrats who have been offered the job. One Democratically appointed district judge of my acquaintance turned down the job—too much extra work, he said.

[85] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 270–71 (W.W. Norton & Co. 2004) (2004).

[86] *In re* Sealed Case, 310 F.3d 717, 744 (FISA Ct. Rev. 2002) ("[T]he criminal process is often used as part of an integrated effort to counter the malign efforts of a foreign power.").

[87] DONOHUE, *supra* note 2, at 27, 150.