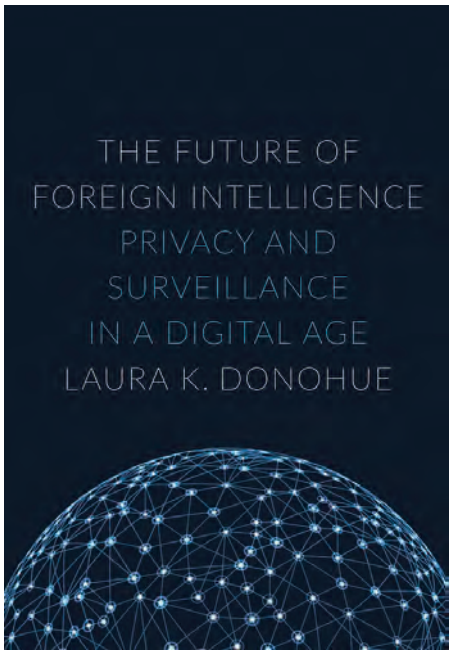
NATIONAL SECURITY. CIVIL LIBERTIES. CAN WE HAVE BOTH?

BY NATHAN SALES

IN THE WAKE OF A CATASTROPHIC TERRORIST ATTACK LIKE 9/11, what balance should the government strike between its weighty national-security responsibilities and its equally solemn duty to preserve Americans' privacy and civil liberties? The question may sound theoretical but it has enormous practical importance. If authorities err on the side of assertiveness, they risk doing violence to our country's most basic values. But if they err on the side of restraint, they risk missing signs of the next plot.

Laura Donohue, a professor at Georgetown University Law Center and one of the country's leading voices in the field of national-security law, is well positioned to tackle the problem. Her important new book, *The Future of Foreign Intelligence,* argues that the government's post-9/11 surveillance programs, begun by the George W. Bush administration and largely continued by President Barack Obama, represent the first kind of error. Faced with an unprecedented threat, she says, authorities responded with equally unprecedented — and unjustified — countermeasures. Agree or not, Donohue's book is a must-read for lawmakers, judges, and citizens who want to understand the difficult policy choices and legal judgments made as the nation confronts the terrorist threat in the digital age.

Donohue begins by describing STELLARWIND, a suite of NSA surveillance programs launched shortly after 9/11. STELLARWIND involved what's known as "bulk" or "programmatic" collection.[1] In addition to targeting individual suspects, as in criminal investigations, the NSA swept up huge troves of data in an effort to identify previously unknown terrorists. In particular, Fort Meade intercepted both metadata and content from phone calls and internet communications. "Metadata" is



THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SECURITY IN A DIGITAL AGE

LAURA K. DONOHUE

OXFORD UNIVERSITY PRESS, 2016

"information that describes who is communicating" — the phone number one dials, the address from which an email is sent, and so on — whereas "content" is the actual substance of the communication.[2] Metadata is the envelope, the letter is content.[3]

At its inception, STELLARWIND wasn't authorized by statute, nor did officials get permission from the Foreign Intelligence Surveillance Court (FISC). Instead, the government grounded the programs on the President's constitutional powers as commander in chief. The administration eventually had second thoughts about this muscular view of presidential power, however, and STELLARWIND was placed on more stable statutory foundations. In 2004, the government transferred the internet metadata program to the part of the Foreign Intelligence Surveillance Act (FISA) that authorizes the FISC to approve pen registers and trap-and-trace devices (which record phone numbers dialed and received); it was discontinued in late 2011. Telephony metadata was shifted in 2006 to FISA's business-records authority — known as "section 215," which is the part of the USA PATRIOT Act that enacted it in its current form. Congress effectively abolished the program in the USA Freedom Act of 2015. Authority to collect internet and telephony content was transferred to section 702 of the 2008 FISA Amendments Act (FAA), in which Congress approved the programs with certain limits.

At its high-water mark, Donohue argues, STELLARWIND represented an enormous and unwarranted intrusion into the private lives of ordinary Americans who had no involvement in terrorism whatsoever. According to Donohue, "thousands of citizens' telephone numbers and e-mail addresses were targeted for content collection"[4] in a dragnet that "swe[pt] in millions of Americans' communications."[5]

Unsupervised bulk surveillance certainly poses serious questions about privacy and civil liberties, but it's important to be precise about the extent to which Americans found themselves in Fort Meade's crosshairs. Take, for instance, the two content programs. The NSA's objective was to intercept the international commu-

nications of suspected al Qaeda operatives located overseas, including their phone calls and emails to and from the United States.[6] So, yes, the NSA did eavesdrop on Americans, but this was a byproduct of targeting terrorists in foreign countries. The collection on Americans was "incidental." (The FAA reflects this distinction as well. It expressly bars the government from targeting Americans anywhere in the world,[7] and authorizes warrantless surveillance only when the government seeks to monitor non-Americans who are "reasonably believed to be located outside the United States."[8]) Incidental collection raises important concerns, to be sure, and strict safeguards are needed to prevent misconduct. But the problem, while serious, differs fundamentally from the deliberate targeting of Americans that produced the notorious abuses of the 1960s and '70s — the monitoring of Rev. King, Operation CHAOS, among others.

Nor should we overstate the novelty of bulk collection in the post-9/11 era. For Donohue, programmatic surveillance is a radical "depart[ure] from how FISA traditionally worked"; normally authorities must obtain FISC approval to monitor specific individuals who are suspected of being spies or terrorists.[9] Yet certain forms of bulk collection both predate FISA and were preserved by it. When Congress enacted the statute in the late 1970s, the NSA was intercepting huge volumes of telecommunications traffic into and out of the United States — specifically, it was tapping cables in international waters and monitoring satellite-based radio transmissions, all without judicial supervision. Part of the reason for FISA's convoluted definition of "electronic surveillance" is that Congress wanted to maintain these capabilities.[10]

Donohue next provides a lengthy account of the founding generation's hostility to general warrants — "promiscuous" authorizations that don't name "the place to be searched and the individual on whom the warrant would be served"[11] — before turning to the main event: a critique of telephony metadata collection, on both policy and constitutional grounds. The now-defunct 215 program, she argues, was a gross affront to individual privacy. Government access to huge troves of metadata enables it to piece together the most intimate details of our private lives.

GOVERNMENT ACCESS TO HUGE TROVES OF METADATA ENABLES IT TO PIECE TOGETHER THE MOST INTIMATE DETAILS OF OUR PRIVATE LIVES.

The costs, then, are substantial. What about the benefits? Here, Donohue argues, the 215 program was essentially useless. The government could only point to a single case where it helped identify a terrorist, and "[i]t was hardly a smoking gun: for two months, the FBI did nothing with the information."[12] She then develops a more ambitious, and more debatable, claim — that metadata generally "is not a particularly good [tool] for uncovering terrorist plots."[13] In fact, communications and other metadata can be enormously valuable to a technique known as link analysis, in which officials probe hidden ties between known threats and their yet-unknown associates. If authorities had been able to analyze airline reservation data before 9/11, it would have been possible to uncover the links among all 19 hijackers.[14] The story is worth telling at some length:

> Start with two men who helped fly American Airlines flight 77 into the Pentagon: Nawaq Alhamzi and Khalid Al-Midhar. Their names appeared on a U.S. watchlist, because they previously had been spotted at a terrorist meeting in Malaysia. So they would have been flagged when they bought their tickets. Tugging on that thread would have revealed three other hijackers who used the same addresses as the first two: Salem Al-Hamzi, Marwan Al-Shehhi, and Mohamed Atta, the plot's operational ringleader. Officials would have discovered another hijacker (Majed Moqed) who used the same frequent-flyer number as Al-Midhar. Five other hijackers used the same phone numbers as Mohamed Atta: Fayez Ahmed, Mohand Alshehri, Wail Alshehri, Waleed Alshehri, and Abdulaziz Alomari. . . . Officials could have found a twelfth hijacker in an INS watch list for expired visas (Ahmed Alghamdi), and the remaining seven could have been flagged through him by matching other basic information.[15]

What about the Constitution? Donohue argues that the "third-party doctrine" of *Smith v. Maryland*[16] cannot justify bulk metadata collection. In *Smith*, the Supreme Court held that people have no reasonable expectation of privacy in the information they turn over to third parties. Police use of a pen register to record the phone numbers dialed by a suspect therefore isn't a "search" and doesn't require a warrant or probable cause. Donohue counters that section 215 simply collects too much information of the utmost sensitivity to fall within *Smith*. "The information being sought is not different in degree. It is different in kind."[17]

More broadly, the third-party doctrine may have a dim future, as Donohue suggests. Scholars have deplored it for decades — Orin Kerr calls it "the *Lochner* of search and seizure law"[19] — and five members of the Supreme Court questioned its viability in *United States v. Jones*, a case involving GPS tracking.[20] Yet it's not clear that the Court is ready to abandon it in national-security cases. Justice Alito's concurrence, joined by three others, argued that long-term GPS monitoring amounts to a search "in investigations of most offenses."[21] This is so because people reasonably expect that, for garden-variety crimes, police won't devote the substantial resources it would take to track their movements 24 hours a day. But Justice Alito leaves open the possibility that lengthy monitoring might not require a warrant for "extraordinary offenses"; in such cases, society might reasonably expect authorities to undertake "long-term tracking . . . using previously available techniques." Terrorism, espionage, nuclear proliferation, and other national-security crimes certainly sound like the sorts of "extraordinary offenses" Justice Alito and his colleagues had in mind.

Donohue has a somewhat more sympathetic view of the content collection authorized by section 702. A legislative fix to FISA was necessary, she explains, because of the email problem. Thanks to the internet's architecture, foreign-to-foreign messages — emails sent from, say, London to Paris — sometimes pass through servers located in the United States. As a result, "communications previously exempted from FISA had begun to fall within the statute, triggering the FISC approval process."[22] Section 702 restored the default rule: The feds needn't obtain a court order to intercept foreign-to-foreign communications, even if they happen to pass through this country on their way to their final destinations. The NSA has implemented section 702 expansively, using it not just to target particular suspects but for bulk collection. Two programs are of particular interest: PRISM, in which the NSA receives bulk data from communications providers, and "upstream" collection, in which the NSA taps into the internet backbone.

Constitutionally speaking, this surveillance depends on a foreign-intelligence exception to the Fourth Amendment's warrant requirement, and Donohue faults a 2002 decision of the Foreign Intelligence Surveillance Court of Review (FISCR) that she says announced such a rule "*for the first time*."[23] "The U.S. Supreme Court," she points out, "has *never* recognized" a foreign-intelligence exception.[24] That's true, but plenty of other courts have, including the Third, Fourth, Fifth, and Ninth Circuits.[25] Indeed, the FISCR emphasized that "all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."[26]

While section 702 doesn't require judges to approve particular targets before the government monitors them, it does direct the FISC to review the government's "targeting" and "minimization" procedures at regular intervals to ensure that they are "consistent with the requirements of [the FAA] and with the fourth amendment."[27] The point of these procedures is to keep the NSA from deliberately collecting Americans' communications and, if it inadvertently does, to limit what can be done with them. Donohue cautions that the FISC's review is fairly perfunctory. Even when a violation occurs the court is reluctant to give more than "a slap on the wrist."[28] Yet an incident from late 2011 gives reason to hope that FISC oversight is more robust than that.

IT IS, IN OTHER WORDS, A TALE OF EXECUTIVE ACTION FOLLOWED BY LEGISLATIVE AND JUDICIAL REACTION.

The government alerted the FISC that the NSA's upstream collection was sweeping up telecommunications bundles that included both foreign-to-foreign messages (which may be intercepted under section 702) as well as domestic ones (which may not). Observing that the NSA's procedures "tend[] to maximize retention of [domestic] information," the court held that they violated both section 702 and the Fourth Amendment, and it ordered the government to adopt stricter minimization procedures within 30 days or end the program.[29] The following month officials came back with more restrictive rules — among other changes, the NSA would segregate the bundles in restricted databases, stamp them with special markings, and keep them for just three years (down from five).[30] The court thus performed pretty much how we would expect a neutral and detached magistrate to perform. It identified constitutional and statutory violations, struck down the offending procedures, and allowed the program to continue only after the government cured the violations.

Donohue is also skeptical of the FISC's role in traditional FISA cases, describing the court as more or less a rubber stamp for the government's surveillance requests. "Between 1979 and 2003," she observes, the "FISC denied only 3 out of 16,450 applications." And of the 18,473 applications decided in the past decade, it "only denied 8 in whole and 3 in part."[31] Yet there are other signs that the FISC is more active in policing the government than this lopsided batting average would suggest. The FISC's presiding judge recently reported that, over a three-month period in 2013, he and his colleagues declined to approve nearly 25 percent of the government's applications, requiring "substantive changes" before allowing the requested surveillance.[31] The FISC doesn't say "no" very much, put it says "not yet" pretty often.

Donohue concludes by proposing reforms that she says would strike a more equitable balance between privacy values and national-security needs. Her first is to rebuild the pre-9/11 "wall" that prevented cops and spies from sharing information with one another. Doing so is necessary, she argues, to prevent pretextual surveillance; the government might "use FISA in place of [criminal laws] . . . to avoid restrictions that protect individual rights."[32]

At the risk of overstatement, this would be a catastrophic mistake. The information-sharing wall was as responsible as any other factor for the government's failure to stop the 9/11 attacks. The 9/11 Commission reported that, in August 2001, a group of intelligence analysts was trying desperately to find Khalid al-Midhar, an al Qaeda operative who had entered the country a few months earlier. An FBI agent saw a message describing the manhunt and immediately contacted the intelligence team, demanding to know more and offering to help. He was told to stand down. Because he "was designated a 'criminal' FBI agent, not an intelligence FBI agent, the wall kept him from participating in any search for Midhar." And, for good measure, he should "destroy his copy" of the message "because it contained NSA information." The agent responded with an angry email: "Whatever has happened to this — someday somebody will die — and wall or not — the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.'"[33] Tragically, he was right. Days later Khalid al-Midhar would help crash American Airlines flight 77 into the Pentagon.

Fortunately there are a number of promising reforms that stop short of rebuilding

the wall. An important one is already in place. FISC proceedings are normally ex parte, but Congress recently authorized the court to appoint outside counsel to provide an adversarial perspective in a case that "presents a novel or significant interpretation of the law";[35] the court has named Donohue herself as one of the people who are eligible for appointment. In addition, to reduce the risk that rogue officers might rummage around in sensitive data, policymakers might require judicial approval for "[a]ny query of foreign intelligence databases . . . where citizens' information is involved."[36] (The Obama administration required something similar for the 215 program before it was abolished; analysts could query the database only if the FISC found a "reasonable, articulable suspicion.") And to prevent mission creep — the risk that information collected for national-security purposes will be used in routine matters like criminal law, public health, and for "myriad other purposes"[37] — policymakers could insist on stronger minimization rules with stricter limits on the types of investigations in which the information may be used.

In the end, the story Donohue tells may be a familiar one after all. Facing an unparalleled terrorist threat and immense challenges posed by technological change, the executive branch responded aggressively with novel initiatives that disrupted established ways of doing business. Then, as the immediate crisis receded, Congress and the courts began to reassert themselves and police the executive's use of power more rigorously. The result was that some of the new programs were discontinued while others were domesticated — allowed to persist, now on more durable statutory foundations and with additional safeguards in place. It is, in other words, a tale of executive action followed by legislative and judicial reaction. That story points to the strains our tripartite system of government experiences when Hamilton's "vigorous Executive"[38] takes decisive steps in times of national emergency. But it also has a more comforting lesson about the system's durability, and its tendency to roll back initial excesses and restore something like the prior equilibrium.

NATHAN A. SALES is Associate Professor of Law at Syracuse University College of Law. He teaches and writes in the fields of national security law, counterterrorism law, administrative law, and constitutional law.

[1] *See, e.g.*, William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 Tex. L. Rev. 1633, 1635 (2010).

[2] Laura Donohue, The Future of Foreign Intelligence: Privacy and Surveillance in the Digital Age 18 (2016).

[3] Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that Isn't,* 97 NW. U. L. REV. 607, 611 (2003).

[4] Donohue, *supra* note 2, at 19.

[5] *Id*. at 38.

[6] *See* Letter from William E. Moschella, Ass't U.S. Att'y Gen., to Pat Roberts, Chairman, Senate Select Comm. On Intelligence, at 1 (Dec. 22, 2005), *available at* http://nsarchive.gwu.edu/NSAEBB/NSAEBB178/surv34.pdf.

[7] 50 U.S.C. §§ 1881b, 1881c.

[8] *Id.* § 1881a(a).

[9] Donohue, *supra* note 2, at 59.

[10] David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act*, *in* Legislating the War on Terror: An Agenda for Reform 217, 224–25 (Benjamin Wittes ed., 2009).

[11] Donohue, *supra* note 2, at 76.

[12] *Id*. at 43.

[13] *Id*.

[14] Markle Foundation, Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force 28 (2002).

[15] Stewart A. Baker & Nathan Alexander Sales, *Homeland Security, Information Policy, and the Transatlantic Alliance*, *in* Legal Issues in the Struggle Against Terror 277, (John Norton Moore & Robert F. Turner eds., 2010).

[16] 442 U.S. 735 (1979).

[17] Donohue, *supra* note 2, at 118.

[18] *Smith*, 442 U.S. at 748 (Stewart, J., dissenting).

[19] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich L. Rev. 561, 563 (2009).

[20] 132 S. Ct. 945 (2012).

[21] *Id.* at 964 (Alito, J., concurring in the judgment).

[22] Donohue, *supra* note 2, at 34.

[23] *Id*. at 146 (emphasis in original).

[24] *Id*. at 145 (emphasis in original).

[25] *See United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973); *United States v. Buck*, 548 F.2d 871 (9th Cir. 1977). *But see Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc).

[26] *In re Sealed Case No. 02-001*, 02-002, 310 F.3d 717, 742 (FISCR 2002).

[27] 50 U.S.C. § 1881a(i)(3)(A).

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

[29] [Case Title Redacted], 2011 WL 10945618, at *27 (FISC Oct. 3, 2011).

[30] [Case Title Redacted], 2011 WL 10947772 (FISC Nov. 20, 2011).

[31] Donohue, *supra* note 2, at 139.

[32] Letter from Reggie B. Walton, Presiding Judge, FISA Ct., to Charles E. Grassley, Ranking Member, Sen. Comm. on the Judiciary, at 1 (Oct. 11, 2013).

[33] Donohue, *supra* note 2, at 31.

[34] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, at 270–71 (2001).

[35] 50 U.S.C. § 1803(i)(2)(A).

[36] Donohue, *supra* note 2, at 151.

[37] *Id*. at 109.

[38] The Federalist No. 70 (Alexander Hamilton).