I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

NSA Surveillance: The Implications for Civil Liberties

SHAYANA KADIDAL*

What are the implications for civil liberties of the massive surveillance programs that have come to public attention as a result of Edward Snowden's disclosures? The first challenge for anyone attempting to unravel this issue is the natural tendency of the public to shrug[1] at the volume and complexity of the information flooding out □ from both Snowden and other official sources that have started to speak to the media under the cover of his disclosures. The stories are rapidly evolving, and frankly, complex enough to confuse anyone. But in my view, the greatest contributor to the apparent complexity is the maze of ever-shifting, always highly technical *legal* justifications for the various programs at issue. In what follows, I will argue that the actual surveillance taking place is remarkably consistent from the Bush administration to the present day; although the legal rationales for the surveillance programs are protean, the programs themselves–and therefore their implications for civil liberties–are largely consistent. It is therefore both more enlightening (and simpler) to start a few years in the past, when most of us first heard about the National Security Agency (NSA), in late 2005 when James Risen and Eric Lichtblau of the *New York Times* broke the story[2] that the NSA was collecting large quantities of calls and emails without getting

---

* Senior Managing Attorney, Center for Constitutional Rights, New York City; J.D., Yale, 1994. The views expressed herein are not those of the author's employer, nor, if later proven incorrect, of the author.

[1] In internet terms, "TL;DR.".

[2] James Risen & Eric Lichtblau, *Bush Lets US Spy on Callers without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

approval from a court first, as usually happens with a conventional wiretap warrant.

I. 21ST CENTURY SURVEILLANCE: A BRIEF HISTORY

After holding the story for more than a year–past the 2004 presidential election–the *Times* finally published it in December 2005, shortly before Risen's book *State of War* (which included a chapter on the program) was scheduled for publication. Being the product of such a lengthy period of reporting, the story was rich in detail, but the main revelation was that the NSA, with presidential approval, has since shortly after 9/11 been intercepting calls and emails where one communicant was inside the U.S. and one abroad, where it believed that one of the parties was somehow affiliated with terrorism, all without any warrants or degree of judicial review whatsoever. The story was reported as an example of blatant lawlessness, for this "NSA Program" or "Program" (as I will call it throughout) appeared to circumvent the post-Watergate Foreign Intelligence Surveillance Act (FISA) that was designed to subject most foreign intelligence wiretapping to a system of judicial review similar to that that had applied to domestic wiretaps for criminal investigatory purposes since the 1968 Wiretap Act ("Title III"). Indeed, the Bush Administration, which chose to aggressively defend the Program in the media, admitted as much: surveillance under the Program was of the sort that ordinarily would have been subject to FISA.[3]

That 1978 FISA statute, by appearances, was quite permissive: If the government could provide to the specialized Foreign Intelligence Surveillance Court (FISC) evidence creating probable cause to suspect that a target was working for a foreign power (defined to include terrorist groups), it could get a FISA order–essentially, a wiretap warrant–allowing surveillance of that target's communications. In practice as well as in theory it seemed easy enough for the government to use: There were only five outright rejections among the first 22,987 applications after 1978.[4] Though the administration would argue that

[3] *See* Petition for a Writ of Certiorari at 6, Center for Constitutional Rights v. Obama, No. 13-802 (Jan. 2, 2014), *available at* http://ccrjustice.org/files/Center%20for%20Constitutional%20Rights%20v%20%20Obama_Petition%20for%20Writ.pdf.

[4] *See* Petition for Certiorari, *supra* note 3, at 5; *Foreign Intelligence Surveillance Act Court Orders 1979-2012*, Electronic Privacy Information Center (May 1, 2014), http://epic.org/privacy/wiretap/stats/fisa_stats.html. It does appear that the process before the FISC occasionally results in modifications of the initial applications; this occurred in roughly 2% of the applications submitted in 2012, for instance. *Id.*

judicial approval stood in the way of "speed and agility" in tracking down targets,[5] like Title III the original 1978 FISA provided for retroactive judicial approval in the event of emergencies. And in any event, the administration never asked a rather pliant Congress for approval of changes to the FISA statute, instead proceeding by executive fiat.

The political shockwaves the story generated were largely a consequence of this gross illegality; indeed the administration's spin seemed to project pride in its willingness to break the law, which added to the unease in my own community of civil libertarian litigators. Why not use FISA if the statute was that easy to work with? Our main suspicion at the time was that the administration was trying to eavesdrop on communications that even a very compliant FISC judge would not approve of intercepting: conversations between lawyers and their clients, journalists and their sources. The description of the program–international calls and emails, with one end in the U.S., where one party was suspected (by an NSA staffer, not necessarily based on any tangible evidence) of association with terrorism–fit a vast quantity of our legally-privileged communications. The Center for Constitutional Rights's (CCR) legal staff frequently calls or emails released Guantanamo detainees, their families, or witnesses relevant to their cases, or other overseas lawyers and experts. We also represented torture rendition victim Maher Arar, who lived in Canada at the time of the disclosures, having been released after a year of torture in Syria at the behest of our government, and representatives of a class of immigration detainees unfairly labeled as of interest to the 9/11 investigation, subject to over-long detention under brutal conditions, and subsequently deported overseas. They were all potential targets of the program, and though we need to communicate with them, we felt we had to take costly and burdensome countermeasures (such as traveling overseas to meet in person rather than using the phone) given the existence of this judicially-unsupervised program of surveillance (which by definition did not operate under any judicially-supervised minimization procedures that might otherwise protect plaintiffs' legally privileged communications[6]). We felt the costs created by those counter-measures, the concrete manifestations of the chilling effect cast by the NSA Program, were sufficient to create injury-in-fact for standing

---

[5] Press Release, The White House, Setting the Record Straight: Critics Launch Attacks Against Program to Detect and Prevent Terrorist Attacks (Jan. 4, 2006), *available at* https://www.fas.org/irp/news/2006/01/wh010406.html.

[6] On minimization of legally-privileged communications, *see infra* note 98 and accompanying text.

purposes, so CCR brought suit seeking to enjoin the Program;[7] the ACLU brought a similar suit (on behalf of itself, other lawyers, and journalists) on the same day in January 2006.[8]

However, there were clues even then that this targeted NSA Program was only one aspect of the NSA's expanded post-9/11 surveillance activities. Risen and Lichtblau's initial story–and later others–reported, based on inside NSA sources, that there was a "data mining" component to the program–meaning, essentially, that the NSA was intercepting electronic communications (calls and emails) in a general fashion, not a targeted one, and then either scanning the content of those communications for the presence of certain keywords thought to be themselves suspicious, or applying more complex algorithms to that huge database to flag communications or the parties thereto for further scrutiny. To use a simple example of the latter, suppose a call comes in to a U.S. number from Afghanistan in the middle of the night, and the person called then calls five other people within an hour. A mechanical algorithm can easily identify such situations (even where there was no prior reason to suspect any of the persons on the calls) and flag them for further review. The pattern the algorithm identifies may be characteristic of sleeper cells triggered to action; it may also be characteristic of a family wedding announcement being passed along to close relatives.

Within short order, a case was filed seeking damages against AT&T based on what appeared to be its complicity in just such a massive data-mining operation against its own customers.[9] An AT&T employee whistleblower, Mark Klein, had disclosed to attorneys at the Electronic Frontier Foundation (EFF) the existence of a secret room in AT&T's Folsom St., San Francisco switching station. It appeared that a copy of every electronic communication coming in off the fiber optic undersea cables that entered AT&T's domestic system through the Folsom St. station was being sent off to the NSA through the equipment installed in the secret room; the only people who would enter the room were NSA staffers and one AT&T employee who held the highest security clearance. The complaint in the Electronic Frontier Foundation's case, *Hepting v. AT&T*, also alleged that AT&T had turned over its vast call records database to the government too–

---

[7] *CCR v. Obama*, CENTER FOR CONSTITUTIONAL RIGHTS (2013), http://ccrjustice.org/CCR-v-Obama.

[8] *ACLU v. NSA: The Challenge to Illegal Spying*, AMERICAN CIVIL LIBERTIES (2008), https://www.aclu.org/national-security/aclu-v-nsa-challenge-illegal-spying.

[9] *Hepting v. AT&T*, ELECTRONIC FRONTIER FOUNDATION (2012), https://www.eff.org/cases/hepting.

something which *USA Today* first reported was true of all three U.S.-owned telecom companies in May 2006.[10]

In CCR's case and the ACLU case, the government challenged our standing, essentially asserting that if we had no evidence that we (or our other plaintiffs) were actually surveilled, our claims that we changed the way we use the phone and email because of the NSA Program's chilling effect were legally insufficient to support standing. But one group actually did have proof that they were surveilled. Al Haramain, an Oregon branch of an international Muslim charity, had been placed on the list of "Specially Designated Global Terrorist[s]" "due to the organization's alleged ties to Al Qaeda . . . [D]uring Al-Haramain's civil designation proceeding," Treasury officials inadvertently turned over to the organization's counsel a document labeled "top secret." "[A]fter *The New York Times*' story broke in December 2005, [Al-Haramain] realized that the . . . [d]ocument was proof that it had been subjected to warrantless surveillance in March and April of 2004."[11] Published accounts state that this document provided evidence that the NSA had intercepted communications between an official of Al-Haramain and the charity's American lawyers, Wendell Belew and Asim Ghafoor,[12] whose practices are located in the Washington D.C. area–the sort of surveillance retention of which would surely never be approved by a federal judge supervising a wiretapping order under the original FISA statute or Title III (absent an active role in some criminal conspiracy by the attorneys on the line), exactly the sort of communications we feared the NSA might have been targeting given its circumvention of the permissive FISA statute. This was not the only evidence supporting fears that attorneys' privileged communications were subject to warrantless surveillance: the Bush administration acknowledged in a formal 2007 submission to Congress that, "[a]lthough the [NSA] program does not specifically target the communications of attorneys or physicians, calls involving such persons would not be categorically

---

[10] *See* Complaint at para. 39-40, Hepting v. AT&T, No. C-06-672-JCS (N.D. Cal. Jan. 31, 2006), *available at* https://www.eff.org/files/filenode/att/att-complaint.pdf; Amended Complaint at para. 53-61, Hepting v. AT&T, No. C-06-672-JCS (N.D. Cal. Feb. 22, 2006), *available at* https://www.eff.org/files/filenode/att/att_complaint_amended.pdf.

[11] Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1194-95 (9th Cir. 2007).

[12] *See* Patrick Radden Keefe, *State Secrets: A Government Misstep in a Wiretapping Case*, THE NEW YORKER, Apr. 28, 2008, 28-34; Jon B. Eisenberg, *Suing George W. Bush: A bizarre and troubling tale*, SALON.COM (July 9, 2008), http://www.salon.com/2008/07/09/alharamain_lawsuit/.

excluded from interception."[13] And in 2008 the *New York Times* reported "[t]he Justice Department does not deny that the government has monitored phone calls and e-mail exchanges between lawyers and their clients as part of its terrorism investigations in the United States and overseas," and the *Times* further reported that "[t]wo senior Justice Department officials" admitted that "they knew of . . . a handful of terrorism cases . . . in which the government might have monitored lawyer-client conversations.[14] In CCR's own litigation challenging the NSA Program, the government conceded before the district court that it would be a "reasonable inference" to conclude from these statements of government officials "that some attorney-client communications may have been surveilled under" the Program.[15]

Two months after we sued, Al-Haramain and the two U.S. attorneys sued seeking damages. After years of litigation, the Ninth Circuit found the document protected by the state secrets privilege: notwithstanding its accidental and seemingly negligent disclosure, it was still classified top secret–still a state secret–and could not be used in litigation. Put to one side the original copy of the document, now filed with the court–even the attorneys' memories of the document could not be referred to; the proof of surveillance missing from our case was held to be secret and thus entirely unavailable to the Plaintiffs.[16] After further proceedings, the lower court nonetheless found that plaintiffs had established a prima facie case of unlawful surveillance based on circumstantial evidence effectively uncontested by the government, and awarded damages and attorneys' fees, but that ruling was overturned on sovereign immunity grounds by the

---

[13] Responses to Joint Questions from House Judiciary Committee Minority Members, Assistant Attorney General William E. Moschella at 15, ¶45 (Mar. 24, 2006), *available at* http://www.fas.org/irp/ agency/doj/fisa/doj032406.pdf.

[14] Philip Shenon, *Lawyers Fear Monitoring in Cases on Terrorism*, N.Y. TIMES, Apr. 28, 2008, at A14.

[15] *See* Defendant's Reply Brief at 4, Center for Constitutional Rights v. Bush, No. 07-1115 (N.D. Cal.) at 4.

[16] *Al-Haramain*, 507 F.3d at 1193 ("we reverse the [district] court's order allowing Al-Haramain to reconstruct the essence of the document through memory. Such an approach countenances a back door around the privilege and would eviscerate the state secret itself."); *id.* at 1204 ("[The district court's] approach also suffers from a worst of both world's deficiency: either the memory is wholly accurate, in which case the approach is tantamount to release of the document itself, or the memory is inaccurate, in which case the court is not well-served and the disclosure may be even more problematic from a security standpoint.").

Ninth Circuit.[17] The case EFF filed against AT&T sought damages, and it died when Congress passed a retroactive immunity statute, though otherwise they might well have ended up with the same problem as *Al Haramain* given the whistleblower documents' centrality to the claims.

As to our cases, seeking to enjoin the program, the government very aggressively defended the program in public and in court, but then shifted tactics by convincing a FISC judge to approve the whole program by January 2007, just in time to abort the first court of appeals argument challenge in the ACLU case. Different FISC judges reviewed the initial January 2007 order or orders and rejected what the first more pliant judge had approved of;[18] that, in turn, finally provoked the Bush Administration to seek approval from Congress for the NSA's program of surveillance without individualized judicial review of targeting decisions. That approval came first in the form of a temporary statute, allowing the government to seek broad approval for whole programs of surveillance (without individualized review of targets) from the FISC for a six-month period. That authority expired in early 2008, with the presidential campaigns well underway.

By the summer of 2008 the Bush Administration gained lasting Congressional approval to change the post-Watergate-era FISA statute beyond recognition, so that the government would propose a whole program of surveillance to one FISC judge, who would then check off on the whole thing if it seemed designed to sweep in primarily foreign communications. Essentially this was a codification of the existing NSA Program with a veneer of judicial review. Under the 2008 FISA Amendments Act (FAA) the government submits to a FISC judge for approval "targeting procedures" that are "reasonably designed" to ensure that the acquisition is "limited to targeting persons reasonably believed to be located outside the United States" (and correspondingly to exclude communications where all parties are *known* to be inside the U.S.)[19] There need be no specification of individual targets or the facilities, phone lines, or emails to be targeted–essentially dispensing with the traditional particularity requirement entirely. While the government must submit minimization procedures, the statute does not specify what role the FISC has in reviewing them, or whether in

---

[17] Al-Haramain Islamic Found., Inc. v. Obama, 690 F.3d 1089, 1099 (9th Cir. 2012).

[18] *See, e.g.*, Greg Miller, *New Limits Put on Overseas Surveillance*, L.A. TIMES, Aug. 2, 2007, at A16 (reporting that second FISA judge rejected "basket warrants," allowing surveillance without particularized suspicion, that had been previously approved by first judge. Apparently, "[o]ne FISA judge approved this, and then a second one didn't.").

[19] 50 U.S.C. § 1881a(g)(2)(A)(i) (2012).

practice the FISC has any role in overseeing their implementation.[20] As the ACLU summarized it:

> The judiciary's traditional function under the Fourth Amendment is to serve as a gatekeeper for particular acts of surveillance, but its function under the FAA is simply to issue advisory opinions blessing in advance the vaguest of parameters under which the government is then free to conduct surveillance for up to one year. The FISA Court does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and ... may not monitor compliance with targeting and minimization procedures.[21]

When Senator (and presidential candidate) Obama switched his position and voted in favor of that statute, the FAA, he effectively removed surveillance from the public political debate for the next five years, because it was no longer a bone of contention between the parties.

The ACLU challenged the FAA in court an hour after it was signed into law, claiming primarily that it violated the Fourth Amendment, and that case, *Clapper v. Amnesty International*, went to the Supreme Court on the same standing issue that the government had made its primary defense to the 2006 cases brought by CCR and the ACLU against the NSA Program. In a 5-4 decision, the ACLU lost: the Court did not hold that chilling-effect surveillance plaintiffs need absolute proof that they were surveilled, but it found that the ACLU's chilling-effect fears were "too speculative" despite the fact that the FAA allowed for very broad surveillance of international communications. A major factor in the majority's reasoning seemed to be that the FISA Court was supposedly[22] reviewing each FAA application for compliance with the Fourth Amendment, as the statute mandated, but

---

[20] On minimization *see infra* notes 98–103 and accompanying text.

[21] *See* Brief for Respondents at 13, Clapper v. Amnesty Int'l USA, No. 11-1025 (Sep. 17, 2012).

[22] Of course, since "[t]he role that the FISA Court plays under the FAA bears no resemblance to the role that it has traditionally played under FISA," *id.*, the FAA having dispensed with the particularity requirement of traditional search warrants and the ongoing judicial supervision of minimization requirements, *see infra* note 98, it is unclear what that Fourth Amendment compliance review would consist of in practice.

the Supreme Court also questioned whether it was realistic to think the ACLU plaintiffs' communications would be targeted and intercepted as a factual matter. (The remnants of our original 2006 case, now in the Ninth Circuit on the issue of records retention by the government, were dismissed as well, relying on *Clapper*.[23])

For future litigants resembling the CCR and ACLU plaintiffs, this first round of NSA litigation set up a framework for any future litigation that is essentially a Catch-22: where plaintiffs lack direct evidence that they were surveillance targets (that is, where reasonable measures taken in response to reasonable fears of very broad surveillance are the only basis for a civil litigant's injury), they are likely to be tossed out of court on standing grounds based on *Clapper*. Where plaintiffs do, somehow, have direct evidence of past or present surveillance, and try to bring a civil suit for damages or try to enjoin interception or retention of records under the surveillance program and have it declared illegal, the evidence of surveillance will be tossed out of court as secret.

Of course–as the majority noted in *Clapper*–this leaves the possibility that the government will seek to introduce evidence from such surveillance in a criminal case, and the defendant will then be able to litigate the validity of the surveillance under the Fourth Amendment regardless of the statutory basis *vel non* of the surveillance. In fact, Solicitor General Verilli specifically argued to the Court that federal courts did not need to reach the merits of the ACLU challenge precisely because the same issue would eventually come up in some criminal case. Of course, that assumes the government wants the issue to be litigated; a typical (strong) criminal case will rely on many veins of evidence, not all of which will be fruits of initial NSA surveillance, and if so, the government may choose its evidence to avoid bringing NSA evidence into court. It is unclear that any previous criminal case has challenged actual surveillance under the NSA Program or any of the other programs reported on since the Risen/Lichtblau story. We now know why: the government's representation in *Clapper* that "it must provide advance notice of its intent" to use "information obtained or derived from"[24] FAA surveillance has not extended to situations where it uses FAA surveillance in applications to acquire traditional FISA surveillance orders. According to the *New York Times*, only some four months

---

[23] *See* Center for Constitutional Rights v. Obama, 522 F. App'x 383 (9th Cir. 2013), *pet'n for reh'g and reh'g* en banc *denied*, Order, Dkt. 50, No. 11-15956 (9th Cir. Oct. 3, 2013), *pet'n for cert. pending*.

[24] Petition for a Writ of Certiorari at 6, *Clapper v. Amnesty Int'l USA*, No. 11-1025 (Feb. 17, 2012).

after this Court decided Amnesty did the Solicitor General learn that his representations to this Court were in error, and only after lengthy debate over the summer did the Justice Department reverse its longstanding position and approve of informing defendants that the fruits of FAA surveillance were used against them.[25] It remains to be seen how frequent such notices will be in criminal cases,[26] and to what extent defendants are able to challenge the surveillance as a practical matter.[27]

In any event, absent the odd criminal case that is entirely reliant on evidence gathered by the NSA, such litigation will proceed only when the government desires it to. The same could be said about other cases involving proof of actual surveillance, such as *Al-Haramain*: if the government wanted to litigate the legality of the NSA Program surveillance of American attorneys, it had the option to not assert the state secrets privilege there. In the current round of Snowden-inspired litigation, the government has acknowledged the authenticity of the Section 215 order allowing for mass gathering of calling records,[28] eliminating the ability of the government to hide behind the catch-22 described above by claiming the material was still secret, and enabling the ACLU's litigation over that program to go forward on the merits. Though this was likely necessary to justify the government's release of a second order apparently limiting use of the records database, it perhaps is a sign that the government (a) believes it will win and (b) feels that it needs the political cover of a favorable ruling on the legality of the call records program from a non-FISC judge.

---

[25] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 16, 2013, at A3.

[26] For example, despite the fact that NSA intercepts are funneled to DEA agents, with the DEA directed to conceal the origins of the information, *see* John Shiffman and Kristina Cooke, *U.S. Directs Agents to Cover up Program Used to Investigate Americans*, REUTERS, Aug. 5, 2013, *available at* http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 (there is no reported instance of such disclosures occurring to date in drug cases).

[27] The first such acknowledgment occurred on October 25, 2013. Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES (Oct. 26, 2013), http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html?nl=todaysheadlines&emc=edit_th_20131027&_r=0.

[28] *See* Press Release, James R. Clapper, *DNI Statement on Recent Unauthorized Disclosures of Classified Information* (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information.

II. FROM RISEN/LICHTBLAU TO SNOWDEN: CURRENT-DAY PROGRAMS

Even this short history of NSA surveillance from 9/11 to early 2013, told through the litigation narrative, shows a pattern: similar programs run under legal authority that shifts so dramatically that the legal justification for the surveillance eventually comes to seem like an afterthought, rather irrelevant to the (typically unbounded) shape of the surveillance program itself.

So, initially after 9/11, the NSA's various warrantless surveillance programs (some aimed at the content of communications like the NSA program we challenged in our 2006 suit; others aimed at metadata like the phone records program described in *Hepting*) operated under nothing more than the authority of the president's say-so, backed by a single Office of Legal Counsel (OLC) memorandum as cover. That memo was shielded from the OLC's usual oversight processes by a disingenuous use of security clearances to hide it from scrutiny. By 2004, Jack Goldsmith and James Comey forced some aspects of those programs to stop, so the administration turned to National Security Letters to run its metadata programs and changed others.[29] When the Risen/Lichtblau story revealed some of the warrantless electronic content surveillance programs, the administration first defended its executive legal prerogatives shamelessly; then, confronted with a Court of Appeals challenge, went to the FISC court for what turned out to be a few months of reprieve, and when forced by the FISC's change of heart, finally went to Congress to broaden the statute, first in temporary sunsetting fashion, and then more permanently with the FAA. As Marcy Wheeler summarizes it: "As the authorities [for] one program got shut down by exposure or court rulings or internal dissent, [the surveillance] would migrate to another program."[30]

In light of this pattern, it's probably not surprising that today the stories speak not of one "NSA Program" but of a "crazy quilt"[31] of code names: "PRISM," "BLARNEY," "ANGRY NEIGHBOR," "SHENANIGANS," "Transient Thurible," the palindromically-

---

[29] *See* Yochai Benkler, *How the NSA and FBI Foil Weak Oversight*, THE GUARDIAN (Oct. 16, 2013), http://www.theguardian.com/commentisfree/2013/oct/16/nsa-fbi-endrun-weak-oversight.

[30] Marcy Wheeler, *Bush's Illegal Domestic Surveillance Program and Section 215*, EMPTYWHEEL BLOG (Oct. 7, 2009), http://emptywheel.firedoglake.com/2009/10/07/bushs-illlegal-domestic-surveillance-program-and-section-215//.

[31] To paraphrase *Smith v. Maryland*, 442 U.S. 735, 745 (1979) ("We are not inclined to make a crazy quilt of the Fourth Amendment").

menacing "EvilOlive," "Shell Trumpet," "Spinnaret," "WATERWITCH," "HOWLERMONKEY," and so forth. NSA whistleblower Thomas Drake explains the profusion of such names by analogy to the perceived need to come up with catchy company names and job titles within startup/dot-com corporate culture, or "app" names for the iPhone generation. In part because discussions structured around particular programs as marketed within the NSA are meaningless to what's going on, and in part because the confusion engendered by all the flashy code names makes people tune out, I want to simplify by classifying things into two main sets of programs: those that collected the content of communications, and those that collected non-content information about communications, the latter generically referred to as "metadata"–roughly the letter and the envelope, to use the most evocative metaphor.

A. *Metadata Surveillance*

The most publicized of the NSA's metadata programs was one through which the agency, under section 215 of the Patriot Act, got a series of court orders, repeatedly renewed over the years going back to 2006, allowing it to collect all phone records from Verizon (and likely the two other domestically-owned[32] phone providers, Sprint and AT&T, as well).[33] So the NSA requested and received from these telecom companies, lists of all calls their subscribers made and received, including typically-recorded metadata such as the time of day, duration of the call, and the phone numbers on the other end of the line (but not the content, i.e. what was said on the call).

The order published by the *Guardian* newspaper[34] could be read standing alone to simply demand that these records be turned over to the NSA for whatever use they deem necessary. The administration subsequently released other orders that indicated that the FISC orders only permitted it to query the database of calling records so assembled

---

[32] Danny Yadron and Evan Perez, *T-Mobile, Verizon Wireless Shielded from NSA Sweep*, WALL ST. J. (June 14, 2013), *available at* http://online.wsj.com/news/articles/SB10001424127887324049504578543800240266368. (Subsequent to the Snowden revelations, a majority stake in Sprint was purchased by SoftBank, a Japanese telecom company.).

[33] Indeed, the story was reported on as far back as 2006. *See* Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY (May 11, 2006), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[34] *Verizon forced to hand over telephone data—full court ruling*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

to investigate records of someone's calling patterns when "a small circle of designated NSA officers" felt they had "reasonable articulable suspicion" that that person had some connection to terrorism,[35] but it also admitted that it then scrutinized the calling records of everyone that first person called, and everyone those people called. On Frigyes Karinthy[36]/Six-Degrees-of-Kevin-Bacon principles, that surely includes a huge swath of humanity for each of the 300 individuals[37] the NSA allegedly limited its phone database investigations to in 2012; depending on input variables about the size of the typical acquaintance pool, estimates have varied between 3 million and tens of millions of people per target.[38] Other metadata collection programs have been disclosed since then, including a series of programs to collect all web surfing data (that is, all internet addresses a consumer visits), under the not-at-all sinister name EvilOlive. A firm picture of how many steps out from an initial suspect the NSA will reach is not clear for other metadata programs.[39]

The administration's defenses of the call records program as policy have focused on both the limitations on querying the database referred to above, and the idea that this information is the same data

---

[35] Steven G. Bradbury, *Understanding the NSA Programs*, LAWFARE RESEARCH PAPER SERIES (Sep. 1, 2013) *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf.

[36] *Frigyes Karinthy*, WIKIPEDIA, http://en.wikipedia.org/wiki/Frigyes_Karinthy (last visited Apr. 9, 2014).

[37] *See Klayman v. Obama*, 2013 WL 6571596 at *7, 2013 U.S. Dist. LEXIS 176925, *31–*32 (D.D.C. Dec. 16, 2013) ("In 2012, for example, fewer than 300 unique identifiers met this RAS standard and were used as "seeds" to query the metadata, but "the number of unique identifiers has varied over the years." Shea Decl. ¶ 24.").

[38] *See Three Degrees of Separation: Breaking Down the NSA's 'hops' Surveillance Method*, THE GUARDIAN (Oct. 28, 2013), http://www.theguardian.com/world/interactive/2013/oct/28/nsa-files-decoded-hops (at typical 190-friend connection level of the average Facebook user, 3rd degree of separation results in 5 million non-redundant "friends of friends of friends"; at 1000 friends, nearly 27 million people are three hops from the initial seed); see also Patrick C. Toomey, *The NSA's Shadow Database*, ACLU BLOG (Jan. 28, 2014), https://www.aclu.org/blog/national-security/nsas-shadow-database (suggesting that a duplicate database, consisting of *all* records of users three hops removed from all seeds for whom reasonable articulable suspicion existed, may then be searched by NSA without restriction).

[39] *See, e.g.*, Shane Harris, *Three Degrees of Separation is Enough to Have You Watched by the NSA*, FOREIGN POLICY (July 17, 2013), http://killerapps.foreignpolicy.com/posts/2013/07/17/3_degrees_of_separations_enough_to_have_you_watched_by_the_nsa (three steps, citing testimony of NSA Deputy Director Chris Inglis).

that the private telecom companies already keep on their subscribers, as they routinely track usage for billing purposes, the main differences being duration of retention (the FCC requires no more than 18 months; the NSA claims it keeps these records no longer than five years) and the fact that many companies' data are now accumulated into one NSA database, allowing for a more complete picture of the interrelationships between callers who subscribe to different providers.

In some ways this defense points us towards the root of the real problem for civil liberties. Private companies routinely accumulate huge volumes of data about their consumers in order to sell them more product: not just the usual corporate suspects like Google (who can discern which banner ads are likely to get your attention for an advertiser□and be useful to you–by scanning through your email to tell what things are occupying your thoughts), but also your supermarket or drug store. Those free loyalty cards that Duane Reade urges consumers to sign up for are used to track a consumer's identity and create a purchase history tied to that identity. The frequent sizeable discounts given to cardholders on many goods are worth the bargain for the merchant, who can then start targeting those consumers with customized ads and discount offers to draw them back into the store.[40]

Interestingly, the NSA, with access to many more streams of data, may have been doing this on its own by pulling together many consumer-purchase databases[41] with credit card records. The most prominent example of a case NSA claims its newly-revealed operations helped uncover, would-be New York City subway bomber Najibullah Zazi, was said to be making TATP (acetone peroxide) bombs with cosmetic peroxide. Early in the investigation the FBI cited to three other individuals near Zazi's Colorado town who also bought small quantities of acetone or peroxide; they were never mentioned by

---

[40] *See, e.g.*, Alice E. Marwick, *How Your Data Are Being Deeply Mined*, N.Y. REVIEW OF BOOKS (Jan. 9, 2014), http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined/?insrc=wci; Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

[41] It has frequently been noted that many consumer profiles available from companies that specialize in assembling them are underwhelming in how accurate a picture of an individual's preferences they assemble, *see, e.g.*, Paul Rosenzweig, *How to Find Out What Big Data Knows About You*, NEW REPUBLIC (Oct. 7, 2013), http://www.newrepublic.com/article/115041/what-big-data-does-and-doesnt-know-about-me; Again, along the lines of any network effect, the combination of several sources should be expected to exponentially increase the usefulness/intrusiveness of a profile.

officials again,[42] but the fact the FBI could identify presumably innocent individuals as suspects so quickly is a clue that perhaps the government has assembled a massive database of consumer purchasing records by agglomerating a large number of similar databases collected by companies. As with the phone records database, expanding the databases expands the number of hits one may generate for a narrow query (e.g. people who purchased peroxide in X quantity within Y miles of Aurora, Colorado; people who are two call steps removed from a terrorist's cell phone).

But the fact that three innocent Coloradans may have been briefly flagged as of interest to a real terrorism investigation by dint of benign consumer purchases is not the problem here–alarming as it may be to average Americans who felt they had "nothing to fear" from NSA activities. Nor are the potential flaws with the government's (or the court's) interpretation of the scope of which records may be the subject of a Section 215 order. While the government's reading of Section 215 of the Patriot Act–one that the largely conservative judges of the FISC have agreed with–is a broad one, and perhaps had a distorting effect on annual reporting to Congress of the number of times Section 215 had been used, the question of Congressional intent is one on which reasonable people can disagree.[43]

The true legal problem underlying broad metadata collection programs is that the government has long believed it doesn't need a court order of any kind to grab information like these phone records,

---

[42] Marcy Wheeler, *Meet 3 PATRIOT Act False Positives Investigated for Buying Beauty Supplies*, EMPTYWHEEL BLOG (June 7, 2013), http://www.emptywheel.net/2013/06/07/meet-3-patriot-act-false-positives-investigated-for-buying-beauty-supplies/#sthash.77GHoOHW.dpuf.

[43] *See, e.g.*, Greg Nojeim, *NSA Spying Under Section 215 of the PATRIOT Act: Illegal, Overbroad, and Unnecessary*, CENTER FOR DEMOCRACY AND TECHNOLOGY (June 19, 2013), https://www.cdt.org/files/pdfs/Analysis-Section-215-Patriot-Act.pdf; Orin Kerr, *My (Mostly Critical) Thoughts on the August 2013 FISC Opinion on Section 215*, THE VOLOKH CONSPIRACY (Sep. 17, 2013), http://www.volokh.com/2013/09/17/thoughts-august-2013-fisc-opinion-section-215/; *contra* Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata under Section 215 and Foreign-Targeted Collection under Section 702*, LAWFARE RESEARCH PAPER SERIES (Sep. 1, 2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf. In addition to the relatively detailed post-Snowden analysis offered by Judge Eagan of the FISC in defense of the program, *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], No. BR 13-109 FISA Ct. (Aug. 29, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf, two district courts have now reached opposing conclusions on the legality of the phone records program in cases seeking injunctive relief brought by third-party litigants: *see* Klayman v. Obama, 2013 WL 6571596 (D.D.C. Dec. 16, 2013) (unconstitutional), ACLU v. Clapper, No. 13-CV-3994 (S.D.N.Y. Dec. 27, 2013) (lawful).

because the Fourth Amendment does not even apply to them under what is known as the "third party doctrine." In *Smith v. Maryland*, 442 U.S. 735 (1979),[44] the Supreme Court held that government does not need a warrant to track the phone numbers you call because you are handing those numbers over to the phone company to route your call (and bill you for the service) every time you dial a number, and once you *voluntarily* give any information to a third party, the government is entitled to simply demand it from the third party as readily as if it were a confession you had given to your neighbor.

So the Fourth Amendment and its warrant protections do not apply to information like dialed phone numbers–that you turn over to a third party for their use. The most frequent analogy used to justify the distinction between the private contents of the phone conversation (protected by the Fourth Amendment) and the numbers (not protected) is the difference between the address written on the outside of a letter and the contents of the envelope: the contents are protected, the address is not. [45]

Smith is widely criticized;[46] one reason most people have not heard about it is that Congress re-regulated much of this area by statute shortly afterwards, in response to the decision.[47] The Court said it was "doubt[ful] that people in general entertain any actual expectation of privacy in the numbers they dial,"[48] perhaps because that was an era of being billed per call, but at the time local numbers didn't show up on most bills, a fact to which the Court has no answer beyond saying it was "not inclined to make a crazy quilt of the fourth amendment"[49] by making its rule turn on the distinction between local and long-

---

[44] The origins of the doctrine are usually traced to both *Smith* and *United States v. Miller*, 425 U.S. 435 (1976) (banking records).

[45] We now know, coincidentally, that the Post Office is scanning the outside of all mail envelopes in its system for the government. *See* Ron Nixon, *U.S. Postal Service Logging All Mail for Law Enforcement*, N.Y. TIMES (July 3, 2013), http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html?_r=0 (describing the "Mail Isolation Control and Tracking" program, instituted after post-9/11 anthrax mail attacks).

[46] Orin Kerr, *The Case for the Third Party Doctrine*, 107 Mich. L. Rev. 561, 563 n.5 (2009) ("A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote." (then citing ten academic works criticizing the doctrine)).

[47] *See* Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986), codified at 18 U.S.C. §§ 2510–2522.

[48] *Smith*, 442 U.S. at 742.

[49] *Id.* at 745.

distance numbers. Commentators have also suggested the case should simply be confined to its facts and understood as an implicit consent case (something Marshall's dissent refutes by pointing out the illusory nature of consent in the context of monopoly providers of telecom services). In the modern era of unlimited (or volume) calling plans one might readily questions whether the crazy-quilt is simply the content/routing information distinction: why shouldn't the content of the phone call also be considered something "voluntarily turned over to the phone company[?]" And it is hard to square the notion that people lack an expectation of privacy in their electronic communications records nowadays, where the degree to which we live our lives online would have been unimaginable in 1979.

The government, however, believes the upshot of *Smith* is that vast categories of information we digital moderns usually assume will be kept private can in fact be obtained by the government without asking a court for approval. Instead, the government need only issue a subpoena to your corporate provider. So not just phone records[50] (who you called and who called you), but records of internet web sites you visited,[51] all your banking records[52] and credit information,[53] records held by your travel agents,[54] older emails stored by your email provider, and older stored texts,[55] and drafts of emails, and files you

---

[50] *See, e.g.*, 18 U.S.C. § 2709 (NSL statute regarding telecom subscriber and billing records).

[51] As to (numerical) IP addresses, *see United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008) ("Neither this nor any other circuit has spoken to the constitutionality of computer surveillance techniques that reveal...the IP addresses of websites visited....We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the [Supreme] Court approved in *Smith*."); Orin Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U.L. Rev. 607, 644-648 (2003) (noting ambiguities in statutory controls on URLs (non-numerical web addresses) and web search queries).

[52] *See, e.g.*, 12 U.S.C. § 3414 (2012) (NSL statute regarding records from financial institutions).

[53] *See, e.g.*, 15 U.S.C. §§ 1681(u), 1681(v) (2012) (authorizing NSLs directed to consumer credit reporting agencies).

[54] *See, e.g.*, 50 U.S.C. § 436 (2012) (NSL statute regarding travel agencies, financial institutions, and credit agencies).

[55] *See, e.g.*, Letter from AT&T Executive Vice President Timothy P. McKone to Sen. Edward J. Markey at 5 (Oct. 3, 2013), *available at* http://www.markey.senate.gov/documents/2013-10-03_ATT_re_Carrier.pdf (noting texts will be turned over on mere subpoena).

store on the cloud,[56] all can be obtained without court order through issuance of a subpoena to the corporate third party holding the records or other material on behalf of you, the consumer. That is shockingly broad list, including essentially all of your commercial interactions with the outside world.

There are very limited restrictions in the case law on what the government can subpoena,[57] and Congress has passed statutes authorizing broader subpoenas–National Security Letters are the variant most widely known to the public–allowing various sorts of business records to be demanded *en masse* without judicial involvement, nor, typically, notice to the business' client whose customer records are being sought.[58]

The lack of notice means the end user will typically not have an opportunity to challenge the surveillance. What if the provider resists the subpoena?[59] In practice, we should expect that to nearly never happen. The providers of most concern here are telecom companies. And the telecom industry is so heavily regulated □ and so beholden to government on rate regulation, taxes, antitrust issues, wireless bandwidth access □ that it has every reason to cooperate with any demand, no matter how legally outrageous. Its track record over the last decade is proof in point: only Qwest offered any resistance to the

---

[56] *See* Theodoric Meyer and Peter Maass, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA (July 31, 2013) (summarizing provisions of ECPA), http://www.propublica.org/special/no-warrant-no-problem-how-the-government-can-still-get-your-digital-data; Julian Sanchez, *Can §215 Be Used for Content Collection?*, JUST SECURITY (Dec. 13, 2013), http://justsecurity.org/2013/12/13/can-215-be-used-for-content/.

[57] *See, e.g.*, Bradbury, *supra* note 35, at 5; Orin Kerr, *Metadata, the NSA, and the Fourth Amendment: A Constitutional Analysis of Collecting and Querying Call Records Databases*, THE VOLOKH CONSPIRACY (July 17, 2013), http://www.volokh.com/2013/07/17/metadata-the-nsa-and-the-fourth-amendment-a-constitutional-analysis-of-collecting-and-querying-call-records-databases/ (subpoena must be "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unnecessarily burdensome") (quoting *See v. City of Seattle*, 387 U.S. 541, 544 (1967)).

[58] *See supra* notes 50, 52-54.

[59] Kerr, *Metadata*, *supra* note 57 (characterizing Barnett's argument elsewhere), *e.g.*, Brief of Amicus Curiae Cato Institute in Support of Petitioner at 17-18, 25, *In re* Elec. Privacy Info. Ctr., No. 13-58, (U.S. Aug. 12, 2013), *available at* http://object.cato.org/sites/cato.org/files/pubs/pdf/tsac_cato_institute_13-58.pdf (arguing that both "Verizon and EPIC are being deprived of their property in secret proceedings").

NSA Program,[60] there appears to have been no provider resistance to the Section 215 phone records collection program, and the instances of even internet companies (arising out of the famously libertarian culture of Silicon Valley) fighting back against third party subpoena requests are rare enough to make news when they happen.[61] Only several months into the Snowden stories–as worries about defection of foreign customers to non-U.S. providers have mounted, particularly in the cloud-storage industry–do we read frequently about outrage at companies with an international consumer market such as Google and Yahoo.[62]

So the debate over enhancing FISC review–in terms of general transparency, adversary process (by appointing a sort of Devil's Advocate to argue *in camera* for the public's or targets' interests), and judicial selection reform and panel seating on that court,[63] should ring a bit hollow: the government doesn't need to go to the FISC to collect any of this metadata. It is sometimes easier to use Section 215 than other authorities, and if the protean past of these programs is any clue, in the future the government may shift towards using various subpoena powers anyway.

---

[60] *See* John O'Neil and Eric Lichtblau, *Qwest's Refusal of N.S.A. Query Is Explained*, N.Y. TIMES (May 12, 2006), http://www.nytimes.com/2006/05/12/washington/12cnd-phone.html. Yahoo also challenged the constitutionality of the 2007 Protect America Act, itself a response to the end of the original NSA Program and the predecessor to the FAA, before the FISC and its Court of Review. *See* Claire Cain Miller, *Secret Court Ruling Put Tech Companies in Data Bind*, N.Y. TIMES (June 13, 2013), http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-data-bind.html?pagewanted=all&_r=0.

[61] E.B. Boyd, *Why Twitter Was the Only Company to Challenge the Secret Wikileaks Subpoena*, FAST COMPANY (Jan. 11, 2011), http://www.fastcompany.com/1716100/why-twitter-was-only-company-challenge-secret-wikileaks-subpoenal; Ryan Singel, *Twitter's Response to WikiLeaks Subpoena Should Be the Industry Standard*, WIRED (Jan. 10, 2011), http://www.wired.com/threatlevel/2011/01/twitter/. For an interesting third perspective on corporate compliance, *cf.* Bruce Schneier, *Snowden, the NSA, and Free Software - Bruce Schneier + Eben Moglen* (Dec. 12, 2013), *available at* http://www.youtube.com/watch?v=N8Sc6pUR1mA&feature=youtu.be ("google was surprised that it was penetrated given it was cooperating in ways it thought it had to, legally").

[62] Barton Gellman and Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Sata Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[63] *See, e.g.*, Bruce Ackerman, *Op-Ed: Surveillance and the FISA court*, L.A. TIMES (Sep. 24, 2013), http://articles.latimes.com/2013/sep/24/opinion/la-oe-ackerman-fisa-reform-20130924.

One stream of metadata by itself can reveal a lot about you. Commentators have already exhaustively catalogued the obvious examples: the records of your calls to your therapist, to a divorce lawyer, to a drug rehab center, all can reveal things about you that you might rather keep secret, and taken together the sum of your communications metadata can form a picture of your inner life and your political beliefs that few of us would want to share with the government.[64] Indeed, the broader, more readily-analyzable picture of an individual created by mass metadata collection and analysis may be more revealing to government than content surveillance, which is inherently more cumbersome to analyze.[65]

Ironically, one particularly corrosive aspect of metadata surveillance that has been drowned out by the Snowden revelations was the previous surveillance scandal of the year, the seizure of the Associated Press' phone records. In an investigation of a leak at the center of a story worked on by seven reporters, the Justice Department authorized seizure of records from 20 lines in four offices used by 100 AP reporters.[66] If the government can see that three government officials spoke to a reporter the day before a story revealing some embarrassing government secret is published, it will

---

[64] For just a small sample of the commentary, *see, e.g.*, Ethan Zuckerman, *Me and my Metadata* (July 3, 2013) (citing various other studies and stories), *available at* http://www.ethanzuckerman.com/blog/2013/07/03/me-and-my-metadata-thoughts-on-online-surveillance/.

[65] *See, e.g., Vindication for Snowden? Obama Panel Backs Major Curbs on NSA Surveillance, Phone Record Data Mining*, DEMOCRACY NOW! (Dec. 19, 2013), http://www.democracynow.org/2013/12/19/vindication_for_snowden_obama_panel_backs (quoting Ben Wizner: "I hear from law enforcement and intelligence officials that they prefer metadata, not just [for] how revealing it is in an individual case, but because they can use their powerful analytic tools. They can mine metadata in a way that they really can't content. People can disguise what they're talking about when they're having conversations with each other, but metadata doesn't lie. Metadata says who contacted who, when and for how long."); *More Intrusive Than Eavesdropping? NSA Collection of Metadata Hands Gov't Sweeping Personal Info*, DEMOCRACY NOW! (June 12, 2013), http://www.democracynow.org/2013/6/12/more_intrusive_than_eavesdropping_nsa_collection (quoting Susan Landau: "metadata of a phone call tells what you do as opposed to what you say"); Alan Rusbridger, *The Snowden Leaks and the Public*, N.Y. REV. OF BOOKS (Nov. 21, 2013) (quoting former NSA General Counsel Stuart Baker: "Metadata absolutely tells you everything about somebody's life....If you have enough metadata you don't really need content").

[66] *See* Sari Horwitz, *Under Sweeping Subpoenas, Justice Department Obtained AP Phone Records in Leak Investigation*, Wash. Post (May 13, 2013), *available at* http://www.washingtonpost.com/world/national-security/under-sweeping-subpoenas-justice-department-obtained-ap-phone-records-in-leak-investigation/2013/05/13/11d1bb82-bc11-11e2-89c9-3be8095fe767_story.html.

not be hard to piece together who the source is. For these most sensitive communications–reporters with sources, attorneys with clients fear of such metadata surveillance will case a massive chilling effect, just as surely as fear of the NSA Program's surveillance of the *content* of communications cast a chill on the communications and therefore on the litigation activity of the CCR and ACLU attorney-plaintiffs in the 2006 litigation.

Like this recent AP phone records seizure, past broad phone records seizures directed at reporters have seemed punitive in scope. Several years ago, John Solomon of AP was a target of a phone records subpoena, after he published a story about the FBI's botched investigation of corrupt New Jersey Senator Robert Torricelli. Two years later Solomon spoke to a number of former sources who told him they stopped calling him because they knew he was a target.[67] The metadata seizures, in other words, had had a chilling effect on the willingness of *others* to use the phone to talk to him–in much the same way as various third parties were no longer willing to speak to the attorney-plaintiffs and amici in the NSA program and FAA litigation.[68]

One might conclude that reporters in this area really need to work like Woodward and Bernstein in the parking garage, or like the drug dealers in *The Wire*: constantly buying and disposing of burners (cheap prepaid cell phones) to communicate. However, even that strategy is at risk given the breadth of the Snowden metadata revelations: it has been reported that one use of the massive phone records databases has been to use calling patterns to identify disposable phones with known targets by identifying their known calling networks and working backwards.[69]

---

[67] *See* Erik Wemple, *AP subpoena: Journo says he lost sources in 2001 case*, WASH. POST (May 14, 2013), *available at* http://www.washingtonpost.com/blogs/erik-wemple/wp/2013/05/14/ap-subpoen//.

[68] *See, e.g.*, Affirmation of Rachel Meeropol at ¶ 17, *Center for Constitutional Rights v. Bush*, No. 06-cv-313, (S.D.N.Y. June 30, 2006), *available at* http://ccrjustice.org/files/CCR_NSA_AffirmationRachelMeeropol_06_06.pdf; Brief of Amici Curiae The Center for Constitutional Rights and Attorneys Involved in National Security Litigation, Supporting Respondents, *Clapper v. Amnesty Int'l USA*, No. 11-1025 (Sep. 24, 2012) at 7, 9 (describing unwillingness of individuals to speak with or be contacted by attorney Tina Foster); *Id.* at 12 (communications with attorney Ramzi Kassem lost due to other party's fear of surveillance).

[69] *See* Bruce Schneier, *Fingerprinting Burner Phones*, SCHNEIER ON SECURITY (Oct. 14, 2013), https://www.schneier.com/blog/archives/2013/10/fingerprinting_5.html (citing NSA document).

Having several streams of data (not just calling records) can reveal a lot more: studies have shown that analyzing your friendship group can reliably predict whether you are gay or not.[70] A less-scientific analysis of social club memberships of 254 prominent Massachusetts colonials produced Paul Revere as the most centrally-networked figure of the bunch.[71] And it turns out the NSA is getting a lot of different streams of data and attempting to assemble full "social graphs" (a term probably mostly familiar from Facebook's search-your-friends feature called Graph Search) for targets. But they are also doing it directly: in October it was reported that the NSA is collecting millions of contact lists from email accounts–essentially, grabbing ready-made social network maps.[72]

One unknown area is the extent that the NSA is gathering mobile phone location data.[73] Does it fall in the same third-party category as the other records above?[74] The issue is not yet resolved in the courts. Interestingly, the Supreme Court is clearly sensitive to the notion that government tracking of the movement of citizens may implicate Fourth Amendment interest. In *United States v. Jones*, a case invalidating evidence derived from a GPS tracker physically installed on a suspect's car (and operated in excess of the narrow geographical and temporal scope allowed by warrant), the Court's opinion held Justice Alito's concurrence noted that "longer term GPS monitoring"

---

[70] *See* Zuckerman, *Me and my Metadata*, *supra* note 64.

[71] *See* Kieran Healy, *Using Metadata to Find Paul Revere* (June 9, 2013), http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/.

[72] Barton Gellman and Ashkan Soltani, *NSA Collects Millions of E-mail Addresses Globally*, WASH. POST. (Oct. 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

[73] *See* Patrick C. Toomey, *It Sure Sounds Like the NSA Is Tracking Our Locations*, ACLU BLOG (Sep. 30, 2013), https://www.aclu.org/blog/national-security-technology-and-liberty/it-sure-sounds-nsa-tracking-your-location (noting evasiveness of NSA official' public statements on question).

[74] The courts to decide the issue thus far have generally said "yes": *See In re* United States for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 122 (E.D.N.Y. 2011) ("While cell-phone users do not technically convey their location, they do voluntarily convey their cell-phone signal to the cell towers, and expose that information to cell-phone service provider's equipment in the ordinary course of business....[However,] the court concludes an exception to the third-party-disclosure doctrine should be applied to cumulative cell-site-location records."); United States v. Skinner, 690 F.3d 772, 773 (6th Cir. 2012) (GPS phone data not protected by Fourth Amendment); *In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600 (5th Cir. July 30, 2013) (same).

implicated expectations of privacy, and Justice Sotomayor's concurrence stated more broadly:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. ...This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps ... some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable" ... and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[75]

This may be the rare area that is promising for privacy advocates to bring before the court, as a number of recent Fourth Amendment cases have broken along unpredictable voting lines at the Court–neither democrat-republican nor the other usual variant, pragmatist (Breyer, Roberts) versus formalists (Scalia, Ginsburg).[76] As this piece goes to press, Judge Leon's decision in the first-filed Section 215 phone records challenge[77] reached the issue of whether the third-party

---

[75] United States v. Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[76] *See, e.g.*, Maryland v. King, 133 S.Ct. 1 (2012) (Kennedy, Roberts, Thomas, Breyer, Alito, JJ. in majority; Scalia, Ginsburg, Sotomayor, Kagan, JJ.).

[77] Klayman v. Obama, No. 13-0881, 2013 WL 6571596, at *1 (D.D.C. Dec. 16, 2013).

doctrine applies to remove any Fourth Amendment protection in call databases and decided it against the government, setting up a possible resolution by the Supreme Court should the circuits split the way the two district courts to address the issues have.[78]

B. *Content Surveillance*

I have very little to say about the details of the NSA's contemporary content surveillance programs, in part because they seem to be largely continuous with the NSA Program surveillance that we challenged in 2006, and that was intended to be effectively codified by the 2008 FAA statute that the government has said is the source of legal authority for the PRISM surveillance program.[79] PRISM was the subject of the second major Snowden-sourced story to appear, and was perhaps received with the most outrage because it showed how closely the telecoms and internet companies were cooperating with the NSA.

General Alexander has succinctly characterized these programs by stating that NSA's goal is to collect everything.[80] With PRISM it is collected from the servers of just about every consumer IT company one can think of: Google, Facebook, Apple, Microsoft, YouTube, and others. Even Skype, which used 256 bit encryption to transmit video calls over the internet, was a party–as a consumer, the encryption ensured that your video call was safe even in international transit, but the company that you were trusting to encrypt it might well have been handing over your content data to the government under the FAA.

As for communications in transit, NSA programs such as BLARNEY intercept almost everything as it passes from major hub to major hub on the internet's backbone fiberoptic cables. This is exactly the sort of interception that Mark Klein reported was happening within AT&T switching stations in 2006. (Amazingly, this internet

---

[78] *Cf.* ACLU v. Clapper, No. 13-cv-3994 (S.D.N.Y. Dec. 27, 2013) (finding phone records collection constitutional, relying on *Smith*).

[79] *See Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, DIRECTOR OF NATIONAL INTELLIGENCE (June 8, 2013), http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf.

[80] Ellen Nakashima and Joby Warrick, *For NSA Chief, Terrorist Threat Drives Passion to 'collect it all,' Observers Say*, WASH. POST (July 14, 2013), http://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

traffic can all be searched in real time by NSA analysts using NSA's XKeyscore data retrieval system.)

Because corporate providers typically store large troves of *metadata* (and have commercial incentives to hold on to it for some time and analyze it in some detail), the question of whether it is feasible for the government to seize and store the same is rarely asked. But when stories claim that massive *content* interception and storage is taking place, the public's first reactions always is: is that even technologically feasible? While the answer was uncertain to our technology experts in 2006, the answer today is clearly yes. In their 2011 book *Cypherpunks*, Julian Assange and Jacob Appelbaum conclude that it would cost around €30 million to store all phone content in and out of Germany for a year.[81] Even quadrupling that to adjust for the greater U.S. population is trivial in comparison to the NSA's $12 billion budget. (When East Germany still existed and was trying to achieve this level of surveillance, 100,000 members of the 16 million person population worked for the Stasi, which needed 10,000 staffers simply to transcribe wiretaps. Now an array of iPhones could accomplish the same task.) The cost may be even less now, in 2013: Brewster Kahle estimates it would take under 300 Petabytes (300,000 Terabytes) to hold all U.S. traffic for a year, and that the hardware required to store all that would cost about $20 million.[82] For years there have been stories that the NSA is building a massive storage center in Utah capable of holding 12,000 Petabytes of data.[83] As long as NSA can keep the power running to it (allegedly at a cost of $20 million a year),[84] they have more than the capacity they need. So when

---

[81] JULIAN ASSANGE, JACOB APPELBAUM, ANDY MÜLLER-MAGUHN, AND JEREMIE ZIMMERMANN, CYPHERPUNKS 38, 168 (2012).

[82] *See* Lily Hay Newman, *The NSA Can Afford To Store Data From Years Of Phone Calls*, GIZMODO (June 16, 2013), http://gizmodo.com/the-nsa-can-afford-to-store-data-from-years-of-phone-ca-513693317 (citing Kahle's spreadsheet *available at* https://docs.google.com/spreadsheet/ccc?key=0AuqlWHQKlooOdGJrSzhBVnhoWGlzWHpCZFNVcURkX0E#gid=0).

[83] Kashmir Hill, *Blueprints Of NSA's Ridiculously Expensive Data Center In Utah Suggest It Holds Less Info Than Thought*, FORBES (July 24, 2013), http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/.

[84] Kashmir Hill, *The NSA's Hugely Expensive Utah Data Center Has Major Electrical Problems And Basically Isn't Working*, FORBES (July 24, 2013), http://www.forbes.com/sites/kashmirhill/2013/10/07/the-nsas-hugely-expensive-utah-data-center-has-major-electrical-problems-and-basically-isnt-working/; Howard Berkes, *Booting Up: New NSA Data Farm Takes Root In Utah*, NPR: ALL THINGS CONSIDERED (Sep. 23, 2013),

an FBI agent on CNN claims the government will be able to go back and listen to calls Tamerlane Tsarnaev made to his wife *before* the Boston bombing, the claim may be realistic.[85]

The main point to remember about these massive content dragnets is that this is precisely how civil libertarians were saying the 2008 surveillance amendments that Senator Obama signed off on a few months before the election would be implemented when the FAA passed. The ACLU filed *Clapper* an hour after President Bush signed the FAA, arguing that it had almost no practical limitations. The FAA allows content surveillance not based on any individual suspicion presented to the FISC. Instead, the court approves criteria for a whole program of surveillance, and reviews it only to check that the criteria is intended to sweep in communications of people located outside the US. There seems to be next to no after-the-fact review provided for, although cases of the NSA misrepresenting the scope of collection practices seem to have been common based on several FISC opinions declassified (with the intent to reduce public criticism of that court's secretive process) in the wake of the Snowden revelations.

C. *Implications of long-term storage*

One obvious concern for civil liberties in an era where mass surveillance data can be stored for long periods of time is that no one knows who will be president in four years. Nor do we know what political or religious associations may become suspect in the future– the communist ties or Muslim community associations of some future generation. (Again, it is as realistic to think NSA could store all the data it gathers for very long periods as it is to think they could gather it in the first place.)[86]

---

http://www.npr.org/blogs/alltechconsidered/2013/09/23/225381596/booting-up-new-nsa-data-farm-takes-root-in-utah ($20 million annual operational cost).

[85] *See generally* John Villasenor, RECORDING EVERYTHING: DIGITAL STORAGE AS AN ENABLER OF AUTHORITARIAN GOVERNMENTS (Dec. 14, 2011), *available at* http://www.brookings.edu/~/media/research/files/papers/2011/12/14%20digital%20storage%20villasenor/1214_digital_storage_villasenor.pdf (storing 5-minute interval location data for 50 million people for a year would cost less than $3000; phone call audio content storable for 17 cents per person in 2011, two cents per person by 2015).

[86] *See* Barton Gellman and Ashkan Soltani, *NSA Surveillance Program Reaches 'into the past' to Retrieve, Replay Phone Calls*, WASH. POST (Mar. 18, 2014), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (indicating NSA stores all voice calls of one particular target foreign nation over preceding 30 days).

The history of warrantless broad-brush surveillance is extensively documented.[87] I will simply note a few points here: both republican and democratic presidents collected massive amounts of data on their political opponents in the civil rights and anti-Vietnam War movements. If it scares us to think that the FBI had dossiers on civil rights leaders and antiwar protesters in the 50s and 60s, today a far less transparent agency has dossiers on literally everyone. (Ironically, James Comey's FBI directorship is term-limited to ten years because Congress was concerned to never allow the emergence of another J. Edgar Hoover, with dossiers on elected officials.[88] Yet the NSA is using Congressional statutes to collect such information, potentially, on everyone.) Indeed, the new suit that the EFF has filed in federal court in California is centered on this idea: that mass-collection programs are a threat to associational freedom in the same way that Alabama's attempts to obtain the NAACP's membership lists were held to be in *NAACP v. Alabama*.[89]

III. PROTECTIONS (AND THEIR FAILINGS)

So that's what's happening factually. Even in simplified form it can be confusing and overwhelming, and that does mute the voting public's response. But we shouldn't extrapolate from that, that the public doesn't care (and, from that, that Congress will never care either). Public polling data is highly consistent on this front, and it has been since just after 9/11 to the present day: when the American public believes that surveillance is targeted at terrorists or targeted at foreigners, it does not mind that it is happening on a larger-than-expected scale. But the moment the public believes that surveillance–even not-very-deep surveillance like the non-content programs discussed above–has a chance to touch on *their* communications, a strong reaction follows. So the public's reaction to these programs is

---

[87] *See, e.g.*, FINAL REPORT OF THE SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES 16 (Apr. 26, 1976) ("Duplication, waste, inertia and ineffectiveness in the intelligence community has been one of the costs of insulating the intelligence bureaucracy from the rigors of Congressional and public scrutiny."); Memorandum of Law of Amici Curiae NAACP et al. at 6-11, 14-15, Center for Constitutional Rights v. Bush, No. 06-cv-313 (S.D.N.Y. Apr. 20, 2006), (describing evidence of surveillance targeting anti-war and civil rights activists), *available at* http://ccrjustice.org/files/CCR_NSA_NAACPetalbriefBrennanCenter_04_06.pdf.

[88] *See* Mark Silva, *FBI's Comey: 'Tethered' to Fidelity*, BLOOMBERG NEWS (Oct. 28, 2013), http://go.bloomberg.com/political-capital/2013-10-28/fbis-comey-tethered-to-fidelity/.

[89] *See First Unitarian Church of Los Angeles v. NSA*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa.

actually nuanced and stronger at times than many seasoned observers would anticipate.

Perhaps the best example of this in practice is the reaction to John Poindexter's Total Information Awareness (TIA) program–which aspired to conduct mass surveillance from various data streams and filter that mound of big data in revealing ways. When its existence came to light in 2003, the public was horrified.[90] (Though surely choosing a disgraced Iran-Contra figure as the program's leader didn't help, the fact that the program itself touched the communications of many ordinary Americans seemed to provoke most of the revulsion.) Congress felt the pressure from the voting public enough to (at least gesturally)[91] pull the funding for the program shortly after it became publicized.

Of course, for people like journalists and attorneys whose communications are especially vulnerable, all the serious chilling effects noted in *Clapper* and the 2006 lawsuits continue to exist in light of both the content and metadata programs that we know continue (albeit under occasionally varying legal authority) today. Surely these chilling effects exist with members of the general public as well: just ask any recent college graduate whether they limit what they post on social media out of fear of what some future employer may find there, and extrapolate that to political associations that some future government may find criminally suspect–Palestinian activists, radical environmentalists, etc.

What, then, are the safeguards that concerned members of the public might look to? And do they really offer any comfort?

---

[90] *See, e.g.*, William Safire, *You Are a Suspect*, N.Y. TIMES (Nov. 14, 2002), http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html (characterizing and criticizing program); Press Release, ACLU, Congress Dismantles Total Information Awareness Spy Program; ACLU Applauds Victory, Calls for Continued Vigilance Against Snoop Programs (Sep. 25, 2003), *available at* https://www.aclu.org/national-security/congress-dismantles-total-information-awareness-spy-program-aclu-applauds-victory- [hereinafter ACLU Press Release] (quoting ACLU Legislative Counsel Timothy Edgar: "This was a hugely unpopular program with a mission far outside what most Americans would consider acceptable in our democracy").

[91] *See* ACLU Press Release, *supra* note 89; *Pentagon's 'Terror Information Awareness' program will end,* USA TODAY (Sep. 25, 2003), http://usatoday30.usatoday.com/news/washington/2003-09-25-pentagon-office_x.htm (Congress "shifted some of the high-powered software under development to different government offices, to be used to gather intelligence from U.S. citizens abroad and foreigners").

A. *Judicial Review*

On the metadata front, commentary has focused on the failings of the FISC (especially after, later in the summer, a pretty poor opinion was released justifying the call records program written by a judge renewing the 215 order that was published in the *Guardian*). But again, the most important point to note is that the government believes, because of the third party doctrine, it does not even need court orders if it chooses to gather this material with subpoenas (and NSLs are really just a Congressionally-created type of very broad subpoena). When the government next shifts legal theories for its metadata collection, it will not matter what Congress' precise intent with Section 215 was.

It's also clear the FISC does not often get the information it needs. A number of its decisions were released in unclassified form after Snowden; previously there had not been any from the FISC itself, though a few opinions of its appellate court had been released. One 2009 decision said the government had "repeatedly submitted inaccurate descriptions" of the program the FISC was reviewing; two years later, a 2011 opinion noted the government had disclosed a "third instance in less than three years... [of] a substantial misrepresentation concerning the scope of a major collection program." But each time the NSA tinkered with its internal controls and procedures, and was allowed to keep going by the Court.[92]

Of course the way the court hears matters–*ex parte*, like any court hearing warrant applications–is not conducive to rejecting many applications, and the composition of the court (with judges selected by Chief Justice Roberts, all but one of whom were appointed by republican presidents) and the government is able to choose the first judge it approaches whenever a new form of surveillance is proposed (presumably a factor in the January 2007 order(s) that were quickly reversed on renewal review by other FISC judges), one would not expect it to produce much.[93] But my own impression is that many reform proposals circulating currently are merely "tinkering with the machinery of mass surveillance" (to paraphrase Harry Blackmun);[94]

---

[92] It is unclear whether FISC ever performed a comprehensive analysis of Section 215 and its application to the phone records program until after the Snowden disclosures became public. *See, e.g.*, Marcy Wheeler, *By "Secret Law" Did They Mean "Not Written Down"?*, EMPTYWHEEL BLOG (Sep. 18, 2013).

[93] *See* Benkler, *How the NSA and FBI Foil Weak Oversight*, *supra* note 29. Judge Mary A. McLaughlin was appointed by President Clinton; all other current FISC judges were named by Presidents Reagan, George H.W. Bush or George W. Bush.

[94] Callins v. Collins, 510 U.S. 1141, 114 S. Ct. 1127, 1130 (1994) (Blackman, J., dissenting).

the overbroad scope of the FAA statute[95] and the statutes governing third-party records requests (NSLs, Section 215 orders, and their like) is the true problem, and one that would go unaddressed even if the public had an *in camera* advocate, the judges sat in banks of three, were not hand-picked by the Chief Justice, and the court enjoyed more transparency than exists now. Moreover, most metadata collection lies entirely outside of FISC review–for example, the email address-book collection program revealed in mid-October occurs outside the U.S. and so is only subject to the NSA's internal "checks and balances."[96]

Finally, the traditional model of judicial review loses all meaning when it's applied to mass surveillance *programs*. If extending the physical search warrant to wiretapping posed the difficult conceptual problems presaged in *Berger*, the Title III individualized-suspicion model of judicial review seems completely incompatible with mass surveillance. Particularity is at the center of judicial review of warrant applications; there is no equivalent when a court is asked to review a proposed program of surveillance, a set of criteria for targeting. It's a bit like applying strict scrutiny's narrow tailoring test to the (inherently broad) compelling interest of diversity. The ACLU was correct to portray the FISC's review of FAA applications as absurdly shallow in *Clapper*, especially in light of the apparent absence of any strong judicial oversight of the minimization procedures meant to ensure that domestic conversations (and, as we wrongly assumed, *infra* part C, privileged conversations) were in fact being filtered out notwithstanding that they might have met the broad criteria for information gathering under the proposed programs. This has led many commentators to assume that any review of such broad programs will turn on the first half of the Fourth Amendment–on "reasonableness," standing alone–ignoring the second half (the particularity requirement for issuance of warrants, which the modern court has generally grafted onto the first half in holding warrantless searches *per se* unreasonable).

---

[95] Interestingly, in denying standing in *Clapper*, the Court assumed the robustness of FISC review. The Court cited five factors that ought to have given the plaintiffs some comfort, most notably of which was the fact that, under the statute, the FISC was supposed to review FAA content-collection applications to ensure compliance with the 4th Amendment. So the weakness of FISA Court review would seem to make the chilling effect felt by plaintiffs there more reasonable.

[96] Barton Gellman and Ashkan Soltani, *NSA collects millions of e-mail address books globally*, WASH. POST (Oct. 14, 2013) http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.14.

B. *Congressional oversight*

The well-catalogued duplicity of NSA officials has certainly contributed something to Congress' failure to limit the agency's activities over the years. Put to one side glaring examples such as DNI James Clapper's response to Senator Wyden's question "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?"–"Not wittingly"–which Clapper later characterized as the "least untruthful" answer he could in open session.[97]

But an underreported aspect of the problem is the fact that by constantly shifting the *legal authority* used to conduct substantively-consistent mass content and metadata surveillance, the agency presents an always-shifting target for Congressional oversight. So by the time a hidden OLC opinion comes to light, the mass content surveillance is being conducted under a FISC order. Hearings about one form of NSL usage bog down in details and repeated, time-consuming requests for better data; by the next year, the same records may be being gathered via a 215 order.

The high classification levels of these programs (and Congressional deference to such designations) have also negatively impacted oversight. The NSA Program was, notoriously, described in top secret briefings to the members of the intelligence committees, including many democrats. But they were not allowed to bring their legal staffers into those briefings due to classification/need-to-know concerns asserted by the administration. Jay Rockefeller went as far as to protect this in a (classified) letter (that itself was allowed to be released only after the program was disclosed by the *Times*) to the administration, noting that without his staffers he was unable to make sense of what he was briefed on, and presumably whether it was legal in light of Congress' 1978 FISA statute or not. Of course, once the programs were revealed, the administration defended itself against a central criticism–that it had never so much as asked for modification of the FISA statute–by noting that key democrats in Congress were

---

[97] Of course, Wyden had let him know the questions in advance, so the idea that Clapper had to lie on his feet to protect classified information defies credulity; his own defense, in fact, was that "collect" means something technical to a surveillance junkie like himself, and so he was simply confused by what otherwise seemed like a straightforward question. *See* Press Release, Office of Senator Ron Wyden, Wyden Statement Responding to Director Clapper's Statements About Collection on Americans (June 11, 2013), *available at* http://www.wyden.senate.gov/news/press-releases/wyden-statement-responding-to-director-clappers-statements-about-collection-on-americans; Oliver Knox, *Intelligence chief Clapper: I gave 'least untruthful' answer on U.S. spying*, YAHOO NEWS (June 10, 2013, 12:47 PM), http://news.yahoo.com/blogs/ticket/intel-chief-clapper-gave-least-untruthful-answer-u-164742798.html.

aware of the Program and raised no objection; Rockefeller's rather practical objection was easily overlooked by the public, and the classified briefing seemed in retrospect to be a clever way to preemptively tar natural opponents of the Program by association.

Finally, as noted previously, the fact that the leader of the Democratic party switched positions on the FAA statute in the summer of 2008 has meant that there is no partisan incentive to make surveillance an issue–instead, libertarian factions in both parties are pushing against their own members (Ron Wyden versus Diane Feinstein, Rand Paul versus Mike Rogers), in sharp contrast to the partisan and libertarian furor over the NSA Program in 2006. Nonetheless, the closeness of recent votes in the House–likely a consequence of the polling patterns described above–indicates that Congress is not a lost cause notwithstanding all of these negatives.

C. *Minimization*

The Supreme Court's extension of Fourth Amendment protection to the content of phone calls is a relatively modern thing. Prior to 1967, precedent held that if the government did not trespass onto your property in installing the bug there was no Fourth Amendment violation. The 1967 *Katz* decision changed this, holding that the content of a call was protected because individuals had a reasonable "expectation of privacy" in it (to use the formulation of Justice Harlan's famous concurrence).[98]

Congress responded to *Katz* by creating a statute to create ground rules whereby courts could issue warrants for wiretaps, but one basic problem was that, being a somewhat novel creature, the shape of what a Fourth-Amendment complaint warrant should look like was unclear. Whereas a traditional search warrant named the particular place to be searched and the specific items to be seized, a wiretap usually named a phone line to be bugged. And bugging a line is inherently a lot more open-ended and intrusive than searching a place for evidence related to a crime. Multiple people besides the target may use a line, the target may speak about private things unrelated to the crime under investigation, and in fact may even speak about privileged matters–conversations with his attorney being a prime example. And of course the tap is in place 24/7, and usually results in recording.

---

[98] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

In a case called *Berger v New York*,[99] decided a few months before *Katz*, the Court specifically mentioned most of these problems and suggested that any warrant for wiretapping would need to meet higher standards, to be a super-warrant of sorts: wiretaps, being inherently intrusive, might only be justifiable at all in investigations of *serious* crimes. And they would require a variety of safeguards to ensure they were as narrow in concept as the physical search warrants the Founders envisioned: they would need to include time limits, the application should establish why no other method of evidence gathering would work, and, most importantly here, the application would need to provide for "minimization"–meaning, there would need to be procedures proposed for implementing the warrant that would protect against intercepting and recording things outside the scope of the warrant–irrelevant conversations–which would obviously include *privileged* conversations, like those of the target with his attorney.[100]

Minimization was a key to CCR's claims of standing for its legal staff plaintiffs in our 2006 litigation. The government argued that FISA surveillance would have been secret but just as harmful to us as surveillance under the NSA Program; our response was that even if the government could have convinced a judge to give it a warrant against the people we were communicating with abroad, there would have to be minimization procedures implemented that would protect our work-product or attorney-client privileged communications.[101] Despite the over 300 pages of briefing in the case, the government never responded to this argument.

---

[99] Berger v. New York, 388 U.S. 41, 57-60, 63-64 (1967) (first suggesting such a constitutional requirement to minimize scope of wire intercepts). The government has conceded before the Foreign Intelligence Surveillance Court of Review that courts have constitutionalized the minimization requirement. *See* Supplemental Brief of the United States, Appendix A: Comparison of FISA and Title III, *In re* Sealed Case, No. 02-001 (FISA Ct. Rev. filed Sep. 25, 2002) at n.1.

[100] Courts have interpreted minimization requirements to include, at a minimum, a duty to institute procedures to protect the confidentiality of privileged communications. *See, e.g.*, United States v. Chavez, 533 F.2d 491, 494 (9th Cir. 1976) (approving minimization limited to attorney-client and priest-penitent calls); United States v. Turner, 528 F.2d 143, 157 (9th Cir. 1975) (approving minimization, even in light of broad scope of monitoring, where privileged calls were excluded); Kilgore v. Mitchell, 623 F.2d 631, 635 (9th Cir. 1980) (noting that even prior to *Scott*, DOJ Title III policy mandated minimization of privileged calls); United States v. Rizzo, 491 F.2d 215, 217 (2d Cir. 1974) (minimization requirement met where officers instructed not to–and did not–monitor, record or spot-check privileged conversations).

[101] Note that attorneys are protected by various legal communications privileges, but journalists are not. We had only attorney plaintiffs in our suits; the ACLU's similar suit included journalists. Consequently, the briefs (and thus the judicial rulings) in their case emphasized the minimization point somewhat less than our briefs did.

Now we may know why: a DOJ memo published by the *Guardian*[102] indicates that the government's legal position seems to be that for foreign intelligence wiretaps, it only needs to minimize attorney-client conversations when the client is actually under indictment. So talking to family or fact or expert witnesses or co-counsel in, say, a Guantanamo habeas case, or in a pre-indictment counseling for someone located abroad like Julian Assange–these attorney communications, despite being clearly within the work-product or attorney-client privileges respectively, would not be subject to minimization. Indeed, there seems to be no reason this policy would prevent interception of conversations taking place during calls and in-person meetings with foreign-national clients detained at Guantánamo (which is, famously, technically outside the United States). Rereading the various bits of evidence indicating that the NSA Program involved surveillance of attorneys in light of this narrow interpretation of legal privilege minimization simply amplifies our initial concerns. In sum, the likelihood is that the executive branch's implementation of minimization procedures provides far less protection for the most sensitive sorts of communications–attorneys with clients and other litigation participants–than we had previously believed was the case. And that in turn will continue to make it harder for litigators like us, working on national security cases of international scope, to sue over other illegal behavior of the executive branch.

Finally, it is worth noting that since the advent of Title III, the actual minimization procedures used by the FBI and other agencies have always been classified. This provides yet another avenue for the intelligence agencies to hide behind slippery, shape-shifting legal rationales: the idea that hidden minimization provisions exist and limit the application of a leaked surveillance order allows for a ready public-relations escape valve for the government anytime part of a legal rationale for surveillance comes to light, for the government can always claim that some hidden minimization procedures are at work narrowing how often a human agent views records. Indeed, David Kris speculated that the January 2007 orders that allowed the Bush

---

[102] *See* Glenn Greenwald and James Ball, *The Top Secret Rules that Allow NSA to Use US data Without a Warrant*, THE GUARDIAN (June 20, 2013), http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant; ATTORNEY GENERAL OF THE UNITED STATES, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (Oct. 31, 2011), *available at* https://www.aclu.org/files/assets/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf (declassified version, officially released Aug. 21, 2013).

administration to continue the initial NSA Program under FISC authorization were made possible only by strict minimization criteria implemented by the court (but, like the orders themselves, entirely unseen by the public).[103] The paired Section 215 orders are an example of how a second order may contain provisions minimizing the impact of the first, broad collection order allowing compilation of the phone records database; the odd fact that the one first published by the *Guardian* contained no indication that the second order existed or limited its application will surely generate a certain amount of uncertainty about whether some as-yet-unseen minimization procedures mitigate in practice the impact of future leaked surveillance orders.

D. *The intelligence/law-enforcement wall*

Proponents of untrammeled intelligence gathering by outward-directed foreign intelligence agencies like NSA have often claimed that one major protection our system offers targets is the "wall" built between intelligence gathering surveillance operations and surveillance carried out in support of criminal investigations. Putting to one side the complex question of what the nature of this separation is in the post-9/11 era, this claim boils down to the idea that that information gathered by these broadest NSA programs may never be used in court against the targets.

I would offer two responses: First, lawyers have an absolute obligation to protect client confidentiality, not just protect against the use of their communications in court against a client. As the various expert affidavits in our case and the ACLU chilling-effect cases indicated, we are obliged to protect confidentiality regardless of whether the confidence is ever used against the client in any forum: "The decision [to refrain from use of vulnerable forms of electronic communication] is not discretionary. It is obligatory....It is no answer to say that suppression is available as a remedy for any improperly intercepted communication. Intercepted communications may be exploited to the disadvantage of clients with no one the wiser....It is

---

[103] Robert Chesney, *Can You Understand These Data Collection Stories Without Understanding the Minimization Procedures?*, LAWFARE BLOG (June 6, 2013), http://www.lawfareblog.com/2013/06/minimization-procedures-data-collection/ (quoting David Kris, *A Guide to the New FISA Bill, Part II*, BALKINIZATION (June 22, 2008), *available at* http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-ii.html).

disclosure itself that is the evil against which lawyers must protect clients, regardless of any additional consequences of the disclosure."[104]

Second, the fact that intelligence is liable to be shared internationally raises separate concerns. To use an example from out 2006 case briefs: imagine we lawyers speak to family members of a Guantanamo detainee in Egypt. His family states that he is categorically opposed to violence, and was merely a political opponent of the Mubarak regime. The U.S. intercepts and relays that information to Mubarak's government. The consequences would be dire, despite the fact that nothing discussed involves anything we would characterize as criminal behavior (at least in a *malum in se* sense). Clients and witnesses sensitive about either concern may simply not wish to participate in litigation, and cease communicating with us.[105]

E. *Foreign government resistance as a check on U.S. spying*

Many of the most spectacular Snowden stories have involved accounts of NSA surveillance cracking into the email accounts of UN officials or foreign leaders like Felipe Calderón, or tapping into Angela Merkel's beloved and ever-present mobile handset.[106] To the extent people believe a lack of European cooperation with American surveillance will result, I suspect that is unlikely to happen for several reasons: first, many of these countries' executives may be happy to have the NSA share with them intelligence that they are restricted from gathering under their own laws. The likely outlet for the frustration over the Merkel scandal will likely be negotiation of some

---

[104] Affirmation of Professor Stephen Gillers, Ctr. for Constitutional Rights v. Bush, Docket 58, No. 06-cv-313 (S.D.N.Y. June 30, 2006) at 5, paras. 9-10.

[105] For examples of related concerns, *see, e.g.*, Maria McFarland Sanchez-Moreno, *What is the NSA sharing with other countries?*, AL JAZEERA AMERICA (Jan. 24, 2014), http://america.aljazeera.com/opinions/2014/1/what-is-the-nsa-sharingwithothercountrieso.html.

[106] *See, e.g.*, James Ball and Nick Hopkins, *GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief*, THE GUARDIAN (Dec. 20, 2013), http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner; Jens Glüsing, Laura Poitras, Marcel Rosenbach and Holger Stark, *Fresh Leak on US Spying: NSA Accessed Mexican President's Email*, DER SPIEGEL (Oct. 20, 2013), http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html; Kevin Rawlinson, *NSA Surveillance: Merkel's Phone May Have Been Monitored 'for over 10 years'*, THE OBSERVER (Oct. 26, 2013), http://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution.

sort of bilateral no-spying-on-each-others-leaders arrangement[107] rather than a general effort to make it harder for NSA to spy within their countries generally. In addition, much of the infrastructure of global wired communications has been set up over the years such that major network pipelines transit the U.S., the geographical straightest-line-route rarely being a consideration when data flies at the speed of light. So, for instance, most communications from the Middle East to Asia move through U.S. based switches.[108] Even if political will existed across the globe to resist NSA surveillance, the hardwiring of the system would take time to rework. And for mobile communications, which travel wirelessly over radio frequencies, resistance is nearly futile; U.S. spy stations in England can pick up signals from cell phones all throughout the continent.[109]

F. *Ineffectiveness: A natural check?*

President Obama has proclaimed himself eager to debate the "balance of liberty and security" implicated by these surveillance programs. Of course, the very terms of that debate presume that there is always a tradeoff involved–that safeguards, typically coming in the form of judicial review, always will operate to diminish security.[110] The public tends to think of courts as primarily serving to throw a monkey wrench into the gears of law enforcement's efforts to gather evidence, as yet another mechanism whereby one branch slows down the work of another.

Even putting aside all practical experience, it is odd to believe this in theory. When we require the executive to show up in court and

---

[107] *But see*, Howard LaFranchi, *US Spying scandal: Why Germany and France Won't Get Britain's Deal*, CHRISTIAN SCIENCE MONITOR, (Oct. 28, 2013), http://www.csmonitor.com/World/Security-Watch/2013/1028/US-spying-scandal-Why-Germany-and-France-won-t-get-Britain-s-deal-video (on the likelihood of such an arrangement with Germany or other non-historical intelligence allies); Ashley Deeks, *The German Intelligence Agencies Are Coming To Town*, LAWFARE BLOG, http://www.lawfareblog.com/2013/10/the-german-intelligence-agencies-are-coming-to-town/.

[108] JAMES RISEN, STATE OF WAR 51 (2006).

[109] *See generally* BBC, *Q&A: What You Need to Know About Echelon* (May 29, 2001), http://news.bbc.co.uk/2/hi/science/nature/1357513.stm; on Echelon generally, *see* PATRICK RADDEN KEEFE, CHATTER 168 (2005).

[110] *But Cf.* Bruce Schneier, *How the NSA Threatens National Security*, THE ATLANTIC (Jan. 6, 2014), *available at* http://www.theatlantic.com/technology/archive/2014/01/how-the-nsa-threatens-national-security/282822/.

prove with some small quantum of evidence that there is reason to suspect the target of being worthy of surveillance, judicial oversight isn't a burden to the system–instead, it results in more efficient law enforcement because it focuses law enforcement's efforts on threats that are real.[111] For 200-plus years having judges review the evidence for "probable cause" before issuing search warrants is a system that has worked to ensure not only that the innocent don't get searched, but also that law enforcement doesn't waste its time with irrational profiling.

Our historical experience with warrantless surveillance confirms this. Inefficiency has been a hallmark of warrantless surveillance since the Church Committee reports, which showed that Presidents Nixon and Johnson targeted their political opponents (in the civil rights and Vietnam War protest movements).[112] "Duplication, waste, and inertia" were the conclusions of one part of the Committee's reports on what happened when the agencies were allowed to gather information without any effective outside oversight.[113] Whenever we removed courts as agents of accountability and oversight, we got lazy law enforcement.

Mass surveillance of the scope described in the Snowden documents should present other problems in theory as well. General Alexander's claim that the NSA seeks to "collect everything" implicitly assumes that size of the data pool gathered equals success. But intelligence experts themselves have long warned of the danger that the more data you collect, the more chaff there is hiding the kernels of wheat, the more haystack hiding the needle.[114] (Alexander's response to this before Congress was: "You need the haystack to find the needle," which perhaps only proves that the actual meaning of farm metaphors is lost on high-tech executives.)

---

[111] *But Cf.* Snowden: "When your working process every morning starts with poking around a haystack of seven billion innocent lives, you're going to miss things....We're blinding people with data we don't need." Julia Angwin, *NSA Struggles to Make Sense of Flood of Surveillance Data*, WALL ST. J. (Dec. 25, 2013).

[112] *See* Memorandum of Law of Amici Curiae NAACP et al., *supra* note 87.

[113] FINAL REPORT OF THE SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. REP. NO. 94-755, at 16 (Apr. 26, 1976) ("Duplication, waste, inertia and ineffectiveness in the intelligence community has been one of the costs of insulating the intelligence bureaucracy from the rigors of Congressional and public scrutiny.").

[114] See *Vindication for Snowden, supra* note 65 (ACLU's Ben Wizner, characterizing NSA's argument: "In other words, we need to have a whole haystack, because one day someone's going to drop a needle into it.").

The *New York Times* and *Washington Post* reported very early on in 2006 that the *targeted* NSA Program produced lots of bad leads that were passed on to the FBI for further investigation, resulting in both dead ends–"more calls to Pizza Hut," in the words of an FBI agent quoted in the Times' story–and, of course, the lost opportunity costs of the wasted effort in pursuing those leads to being with.[115] (Curiously, the only reason this evidence of the poor practical efficacy of the NSA Program came out in 2006 was likely that natural interagency rivalries gave the FBI an incentive to leak information to reporters–a dynamic that seems to have played out between the FBI and CIA throughout various torture-related FOIA releases.) The *Washington Post* has similarly unearthed and published a slide revealing some of the NSA's current over-collection problems: because spammers got into an email account the agency was surveilling, the web of connections from sent emails out of that compromised account became so huge it was flooding their entire collection system, eventually forcing NSA to cut off that target from surveillance. (Perhaps the lesson for civil libertarians here is to periodically click on those Nigerian emails to protect your Gmail account from surveillance.)[116]

In 2006 only a small handful of dubious success stories were advertised by the NSA as proof that the Program worked (with claims that dossiers on amateurish jihadists Mohammed Junaid Babar and Iyman Faris were augmented in part through the program).[117] Similarly, there are very few examples that the NSA has even tried to hold out as successes for what are surely multi-billion dollar programs. The NSA claims that the identification of 2009 subway bomb plotter Najibullah Zazi traces back to an intercepted email he sent to the Yahoo account of a known al Qaeda figure in Pakistan–in other words, an account the pre-2007 version of FISA would have readily facilitated surveillance of, and one already being watched by

---

[115] Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr., *Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends*, N.Y. TIMES (Jan. 17, 2006) at A1; Barton Gellman, Dafna Linzer and Carol D. Leonnig, *Surveillance Net Yields Few Suspects*, WASH. POST (Feb. 5, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373.html.

[116] *The NSA's Problem? Too Much Data,* WASH. POST (Oct. 14, 2013), http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/.

[117] Eric Lichtblau and James Risen, *Defense Lawyers in Terror Cases Plan Challenges Over Spy Efforts*, N.Y. TIMES (Dec. 28, 2005), http://www.nytimes.com/2005/12/28/politics/28legal.html?pagewanted=all&_r=0.

British intelligence.[118] British intelligence also first found David Coleman Headley, another find claimed for the NSA. NSA claimed the call records database helped lead them to Basaaly Moalin, convicted of material support for sending funds to al Shabab; like Zazi, the agency used a Shabab member's number as the starting point, and could have done a conventional investigation via particularized court order from that first clue. Finally, an FBI official told CBS that several Americans, one of whom plead guilty three years ago to material support for al-Qaeda, had plotted to bomb the New York Stock Exchange, an attack detected in advance by NSA–but there is no evidence beyond that statement that this plot was in any way real.[119] This very thin case for efficacy is probably why by September, General Alexander had begun to frequently advertise national "cyber security" as an additional justification for the mass collection programs, and why the government had backed off initial aggressive claims about the call records program's efficacy in court filings later in the fall.[120] The first judicial decision to address the call records program also seems quite skeptical of its efficacy.[121]

Alexander has spoken of the "peace of mind metric"[122] with respect to mass surveillance: at least we have everything, even if it's not easy to use! But even saying that seems in a way an acknowledgment that the current system doesn't work well. Surely the agency understands this at some level. Why keep doing it, then? On possibility–which we proposed even back in 2006–is that the goal of gathering these

---

[118] Matt Apuzzo and Adam Goldman, *NYC Bomb Plot Details Settle Little in NSA Debate*, ASSOCIATED PRESS (June 13, 2013) http://bigstory.ap.org/article/nyc-bomb-plot-details-settle-little-nsa-debate.

[119] Justin Elliott and Theodoric Meyer, *Claim on "Attacks Thwarted" by NSA Spreads Despite Lack of Evidence*, PROPUBLICA (Oct. 23, 2013), www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence.

[120] *See* Jameel Jaffer, *The Basis for the NSA's Call-Tracking Program Has Disappeared, If It Ever Existed* [Updated], JUST SECURITY (Nov. 7, 2013), *available at* http://justsecurity.org/2013/11/07/basis-nsas-call-tracking-program-disappeared-existed/ (noting claims to FISC in 2008 that program was "necessary" have evolved to program being "one method" that it "may not be feasible" to do without).

[121] *See* Klayman v. Obama, No. 13-0881, 2013 WL 6571596 *1, *24, Slip Op. at 61 (Dec. 16, 2013) ("the Government does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature.")

[122] Dave Gonigam, *Cybersecurity: The NSA's Big Budget Action Movie*, DAILY RECKONING (Jan. 21, 2014), *available at* http://dailyreckoning.com/cybersecurity-the-nsas-big-budget-action-movie/ ("[Alexander said] the NSA needs the ability to spot 'a cyberpacket that's about to destroy Wall Street.'")

haystacks is to enable the retrospective testing of technologies developed in the future to sort them. On this theory, these databases are gathered mainly so as to allow the NSA to test various algorithms designed to spot possible threats based on nothing more than patterns of communication–that one call from Afghanistan in the middle of night followed by ten calls out described *supra*. Such algorithms can only really be tested to see if they "work" by running them against a past database and seeing if they spot threats that proved to exist when an attack happened or was preempted by more traditional intelligence gathering and law enforcement techniques.

Such an aspiration would fit into one long-term dream of the intelligence agencies: to replace the human element of intelligence operations, which has historically proven to be inherently flaky, expensive, and prone to working for the enemy, with machine intelligence–ever-refined until it proves foolproof, the Manchurian candidate of the intelligence field. The mindset would also be consistent with the entrepreneurial atmosphere that seems to prevail within the NSA, based on the Snowden documents: multiple programs, constantly turning over, competing over similar functionality, brassily advertising themselves. The revolutionary promise of "big data" is trumpeted everywhere today, but machine intelligence might also have seemed like a ready solution to one of the many intelligence crises posed by 9/11: that we had far too few human intelligence resources already in place in the Arab world the day after the attacks.

Such a system, when perfected, would in theory aspire to intercept as much data of every variety in bulk first and find suspects later, rather than starting with evidence generating suspicion and investigating those specific targets–the traditional preemptive law enforcement model of seeking out the tip of the conspiratorial iceberg and then throwing more assets at traditional techniques (targeted intercepts, tailing, infiltration) to uncover the hidden mass below the waterline. The problem with this aspiration *in theory* is that it assumes an algorithm can be found which generates almost no false positives. An algorithm that produces an infinitesimal rate of false positives, when applied to a massive database, will overwhelm any system with "more calls to Pizza Hut." Indeed any algorithm, to be useful in practice, must produce an almost negligible false positive rate because the ratio of false positives against hits must be small, and the number of actual terrorist conspirators in any society is itself infinitesimal.[123]

---

[123] *See* Bruce Schneier, *Data Mining for Terrorists*, SCHNEIER ON SECURITY (Mar. 9, 2006) ("All data mining systems fail in two different ways: false positives and false negatives. A false positive is when the system identifies a terrorist plot that really isn't one. A false

I have already noted above that many commentators believe that because the Fourth Amendment warrant clause and its particularity requirements are so inherently incompatible with mass surveillance, such data mining programs will eventually only be reviewed for "reasonableness" under the first generally-applicable clause of the Amendment, which states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." But there is also an antecedent question, which is whether a *computer* searching your data without ever flagging it for review by a human operator even constitutes a "search."[124] Those who believe the answer is "no" would likely hold that, if NSA is only exposing a record to scrutiny by human agents after it has been flagged by a computer algorithm, then the millions of records *the algorithm* scans and rejects have not been searched, and even the reasonableness requirement may not apply to them. The ACLU call-records plaintiffs base their standing on the fact that *all* records of subscribers to their telecom provider have been turned over to the NSA, including their's. But if all those records have only been scanned by a computer for ties to one of the 300 target numbers queried, then under this theory for exempting machine searches, it is unclear that their records have been "searched" for Fourth Amendment purposes.[125]

Finally, any such system, no matter how sophisticated, would be easy to avoid if terrorist conspirators simply took a low-tech approach.

---

negative is when the system misses an actual terrorist plot. Depending on how you "tune" your detection algorithms, you can err on one side or the other: you can increase the number of false positives to ensure that you are less likely to miss an actual terrorist plot, or you can reduce the number of false positives at the expense of missing terrorist plots... To reduce both those numbers, you need a well-defined profile. And that's a problem when it comes to terrorism. In hindsight, it was really easy to connect the 9/11 dots and point to the warning signs, but it's much harder before the fact... assume the system has a 1 in 100 false positive rate (99% accurate), and a 1 in 1,000 false negative rate (99.9% accurate). Assume one trillion possible indicators to sift through: that's about ten events □ e-mails, phone calls, purchases, web surfings, whatever □ per person in the U.S. per day. Also assume that 10 of them are actually terrorists plotting. This unrealistically-accurate system will generate one billion false alarms for every real terrorist plot it uncovers."); Carl Bialik, *Ethics Aside, Is NSA's Spy Tool Efficient?*, WALL. ST. J. (June 14, 2013), *http://online.wsj.com/news/articles/SB10001424127887324049504578543542258054884*; Carl Bialik, *Do the Numbers Behind Prism Add Up?*, WALL. ST. J. (June 14, 2013 9:53 PM), http://blogs.wsj.com/numbersguy/do-the-numbers-behind-prism-add-up-1249/ (citing prediction of 10,000:1 false positive ratio).

[124] *See, e.g.*, Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 547-54 (2005).

[125] Judge Leon's decision in Klayman rather summarily dismisses this argument: *see* Klayman v. Obama, 957 F.Supp.2d 1, 29 n.39 (D.D.C. 2013).

Recall that by the afternoon of 9/11 there were already pundits on the networks announcing that soon the public would hear about how the plotters pulled it off with encryption. Instead, they used the most primitive of techniques: staying off-grid, communicating in code when they did use email (from public computer terminals), etc.[126] As *Newsweek* summarized it, "[t]he NSA's top brass assumes that if a threat does not show up in its databases, it doesn't exist. As one woman who lives online, Marcy Wheeler, said, the next terrorist attack will come from a group that stays offline 'and we're going to be hit bad by it because we have this hubris about the degree to which all people live online.'"[127]

G. *Self-help*

"Encryption works":[128] no less an authority than the famously-paranoid Edward Snowden has said as much.[129] While almost all commercial software packages must be assumed to be vulnerable in the same way the 256-bit AES encrypted Skype is, simple, negligible-cost combinations of open-source programs like Jabber (chat) and Jitsi (video) paired with PGP encryption can replace most commercial means of electronic communication. Whereas the previous suspicion that encrypting communications simply flagged them for the NSA (which, according to some reports, stores all the encrypted communications it encounters for such date in the future as computing power makes it more convenient to decode them), one

---

[126] In fairness, Zazi did as well, but got caught, his email correspondent already being a marked man and his choice of code words too commonplace. *See* Goldman and Apuzzo, *supra* note 118.

[127] Pema Levy, *The Woman Who Knows NSA's Secrets Trawling for Needles in A Haystack* (Oct. 04, 2013) NEWSWEEK, *available at* http://mag.newsweek.com/2013/10/04/the-woman-who-knows-the-nsa-s-secrets.html.

[128] *Edward Snowden: NSA Whistleblower Answers Reader Questions*, THE GUARDIAN (June 17, 2013), http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower ("Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.").

[129] *See also* Bruce Schneier, *Snowden, the NSA, and Free Software - Bruce Schneier + Eben Moglen* (Dec. 12, 2013), *available at* http://www.youtube.com/watch?v=N8Sc6pUR1mA&feature=youtu.be ("the most important headline is that crypto works"; to the extent that reporting notes instances on NSA supposedly breaking encrypted systems, "[t]hey're not breaking it by breaking the math, they're breaking it by cheating"–i.e. by weakening random number generators, penetrating internal transfers at unencrypted points, etc.).

consequence of Snowden's revelations will likely be that larger numbers of commercial and noncommercial users routinely encrypt electronic communications. At the very least, encryption buys time against the government.[130]

H. *Statutory limits, Congressional self-interest, and some concluding thoughts*

While I have voiced skepticism about the potential for FISC reform to significantly affect our current situation, Congress could certainly impose meaningful limits on the NSA by statute. It could revoke the broad authority granted by the FAA, impose a warrant progress for government access to third-party records, bar long-term storage of data–almost every problem noted above could be addressed by statute. FISA itself occupied an effectively unregulated space when it was passed in 1978. Nor is it fantasy to think such things might happen in the near term. The first post-Snowden bill, pushed by Representatives Amash, Conyers and Nadler in the House, came close to passing,[131] and some Tea Party libertarians seem to be promising (if unfamiliar) bedfellows for them on these issues.

That brings me to one final thought on checks-and-balances: To what extent are judges, members of Congress and other elected officials exempted from NSA surveillance? If they are not, the chilling effect that afflicts attorneys and journalists applies here as well and has similarly-enormous potential to corrupt the political process. Imagine Anthony Weiner had not accidentally mass-tweeted that fateful photograph,[132] and had remained in the House, but knew that

---

[130] Steven Rich and Barton Gellman, *NSA Seeks to Build Quantum Computer that could Crack Most Types of Encryption*, WASH. POST (Jan. 2, 2014), http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html ("'I don't think we're likely to have the type of quantum computer the NSA wants within at least five years, in the absence of a significant breakthrough maybe much longer'" (quoting MIT's Seth Lloyd)); *id.* ("In 2009, computer scientists using classical methods were able to discover the primes within a 768-bit number, but it took almost two years and hundreds of computers to factor it. The scientists estimated that it would take 1,000 times longer to break a 1,024-bit encryption key, which is commonly used for online transactions.").

[131] *See* Jonathan Weisman, *House Defeats Effort to Rein In N.S.A. Data Gathering*, N.Y. TIMES (July 24, 2013), http://www.nytimes.com/2013/07/25/us/politics/house-defeats-effort-to-rein-in-nsa-data-gathering.html?_r=0.

[132] *See Weinergate*, THE VILLAGE VOICE (May 26, 2011), http://blogs.villagevoice.com/runninscared/weinergate%20dick%20shot.png.

the NSA knew about his habits–and was casting the deciding vote on a bill limiting the powers of the NSA?

Such a scenario is not entirely the stuff of fiction: FBI director J. Edgar Hoover had accumulated dossiers on all sorts of elected officials, which is why James Comey's term in that same office has been limited to ten years by statute–to avoid allowing any future FBI director to accumulate that much dirt on (and accompanying passive leverage over) Congressmen.[133] Even Supreme Court justices had been surveilled in the past, as the Church Committee discovered.[134] Perhaps one consequence of the accumulation of private conversations from foreign leaders' cell phones and email accounts will be not to undermine their negotiating positions at the G20 or the UN directly, but to allow the accumulation of leverage by discovering embarrassing secrets in their closets. Either way, the potential for surveillance corrupting the political process extends to multinational negotiations between democracies as well.

Interestingly, Snowden did a two-hour-long live chat with *Guardian* readers from Hong Kong, which he ended by noting (in response to Glenn Greenwald's final "anything else you'd like to add" question) that: "The US Person/foreigner distinction is not a reasonable substitute for individualized suspicion, and is only applied to improve [political] support for the program. This is the precise reason that NSA provides Congress with a special immunity to its surveillance."[135]

Snowden's first sentence neatly summarizes the polling data I described earlier.[136] The second illustrates the potential scope for corruption of the democratic process posed by sweeping content and

---

[133] Pornography-viewing habits are in fact a special area of interest for the NSA with respect to "jihadist" "radicalizers": *see* Glenn Greenwald, Ryan Gallagher, and Ryan Grim, *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'*, HUFFINGTON POST (updated Dec. 2, 2013), http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html?1385526024.

[134] *See generally* Curt Gentry, J. Edgar Hoover: The Man and His Secrets 630-31 (2001).

[135] *Edward Snowden: NSA whistleblower answers reader questions, supra* note 128.

[136] Indeed, if the main reason for the foreigner/U.S.-person distinction is domestic political optics (and not legal principle or technical issues), one would presume changing political winds and diplomatic pressures might make NSA willing to abandon this fundamental distinction that traces back to the origins of FISA. *Cf.* Jennifer Granick, *Foreigners and the Review Group Report: Part 2* (Dec. 19, 2013) (describing Recommendation 13 of the President's Review Group on Intelligence and Communications Technologies, which would extend various protections to foreigners), *available at* http://justsecurity.org/2013/12/19/foreigners-review-group-report-part-2/.

metadata surveillance, whether or not Congress is exempted from some or all of it. Mass surveillance of this all-seeing scale, with the government able to assemble together everything about us that exists outside of our heads–all of our consumer activities, all of our communication patterns and other social connection–is arguably fundamentally incompatible with democratic self-governance. One reason the Framers paid so much attention to protecting property rights from the state is that they thought private property ensured autonomy from the state; give the government sufficient power to control wealth and the means to produce it, and the people would not be independent enough to control the government. Essentially, to have a democracy, you need the citizenry to be somewhat autonomous from government, independent of all-encompassing government control. Mass surveillance threatens that independence enough to corrupt democracy itself. When the government "can literally see your thoughts form as you type,"[137] your degree of control over government is at the very least limited by the same sort of self-censorship that afflicts the lawyers and journalists who first sued over these NSA Program in 2006.

I think voters today actually understand that at some deep level. So that makes it strange that the most commonplace excuse for not caring about mass surveillance is that old saw: "ordinary Americans have nothing to fear." And I suppose at some level, that's just it: The existence of a program like this is a tremendous disincentive to participate in anything this government does not like, or, for the more far-sighted, that some future government may not like.[138] Put another way, it's a huge incentive to become more ordinary in one's political, socioeconomic, and even religious beliefs. Why go to an animal rights conference, join a Google group of like-minded people opposed to the WTO, protest the next war in the streets, knowing that tomorrow the government may regard these associations as suspect and track them back to you? The most succinct statement of the homogenizing potential of such an all-seeing government was made by Umair

---

[137] Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

[138] *But Cf.* REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 114 (Dec. 12, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("we cannot discount the risk, in light of the lessons of our own history, that at some point in the future, high-level government officials will decide that this massive database of extraordinarily sensitive private information is there for the plucking.").

Haque, who asked: "Can there be a more chilling message to conform than 'America is not interested in spying on *ordinary* people'?"[139]

[139] Umair Haque, TWITTER (Aug. 9, 2013, 7:59 PM), https://twitter.com/umairh/status/366031032337698816 (@umairh: "Can there be a more chilling message to conform than 'America is not interested in spying on ordinary people'?"). (It seems appropriate at this point to mention that the Library of Congress is apparently archiving all of Twitter. *See Library of Congress Is Archiving All Of America's Tweets*, THE TELEGRAPH (Jan. 22, 2013)).