GOVERNMENT DISCRETION IN THE AGE OF BULK DATA COLLECTION: AN INADEQUATE LIMITATION?

JULIAN SANCHEZ*

There are about 3,500 wiretap orders issued every year, at the federal and state levels combined for all criminal investigations.[1] When one company, such as Facebook, has on the order of tens of thousands of accounts flagged for content interception under foreign intelligence orders,[2] the appropriate benchmark is not "millions," but what we do in other contexts.

Even that number is incomplete because much of the government's collection of Internet content is not happening through PRISM.[3] There is also the other component of section 702[4]—the "upstream" collection off the Internet backbone,[5] as well as overseas collection under the authority of Executive Order 12,333.[6] This is not part of FISA, which only covers col-

---

* Senior Fellow, Cato Institute. This essay was adapted from remarks given at the 2014 Federalist Society Annual Student Symposium at the University of Florida in Gainesville, Florida.

1. ADMIN. OFFICE OF THE U.S. COURTS, WIRETAP REPORT 2013 (2014), available at http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx [http://perma.cc/ASG5-7T6G].

2. *See Global Government Requests Reports*, FACEBOOK, https://www.facebook.com/about/government_requests [http://perma.cc/595L-XTV6] (last visited July 28, 2014) (reporting government data requests by country from the first six months of 2013, ending on June 30).

3. Stephen Braun et. al, *PRISM Is Just Part of a Much Larger, Scarier Government Surveillance Program*, BUSINESS INSIDER (Jun. 15, 2013, 9:54 AM), http://www.businessinsider.com/prism-is-just-the-start-of-nsa-spying-2013-6 [http://perma.cc/5BH8-AE82] (noting that PRISM is "a relatively small part of a much more expansive and intrusive eavesdropping effort").

4. 50 U.S.C. § 1881a(b)(3) (2012) [hereinafter FISA § 702].

5. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 7 (2014) (discussing upstream data collection and how it differs from PRISM collection).

6. *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1982).

lection within U.S. borders,[7] but rather the authority the National Security Agency ("NSA") relied upon for bulk interception from the data links between the foreign data centers companies maintain.[8] It is very important to pay careful attention when the Director of National Intelligence, Jim Clapper, says "under this program." That means "we're not doing that under this program . . . currently."[9]

March 2014 is actually the forty-third anniversary of the burglary of an FBI field office in Media, Pennsylvania by a group of anti-war activists.[10] That burglary ultimately led to the exposure of COINTELPRO, the FBI's program spying on and infiltrating domestic dissident groups, peace activists, civil rights groups, and other groups of that sort during the 1960s.[11]

The outing of this program led to the creation of the Church Committee and the Pike Committee, which exposed decades of abuse of intelligence authorities for fundamentally political purposes, under presidents of both parties.[12] One such abuse involved an NSA operation called SHAMROCK. SHAMROCK involved the bulk acquisition of international telegrams, which were then computer searched for names on a government watch

---

7. *See* 50 U.S.C. § 1881a(b)(3).

8. *See* Barton Gellman & Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data 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 [http://perma.cc/N52L-6NTK].

9. *See* Letter from James R. Clapper, Dir. of Nat'l Intelligence, to Senator Ron Wyden (Mar. 28, 2014), http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-090b.pdf [http://perma.cc/83CP-4MK4]; Mike Masnick, *Senators Not Impressed with James Clapper's Carefully Worded Responses*, TECHDIRT (July 29, 2013, 3:34 PM), https://www.techdirt.com/articles/20130729/12223823986/senators-not-impressed-with-james-clappers-carefully-worded-responses.shtml [http://perma.cc/747-FVEB].

10. Ed Pilkington, *Burglars in 1971 FBI office break-in come forward after 43 years*, THE GUARDIAN, Jan. 7, 2014, http://www.theguardian.com/world/2014/jan/07/fbi-office-break-in-1971-come-forward-documents [http://perma.cc/B37Q-GF5U].

11. *Id.*

12. Thomas R. Eddlem, *Greenwald: GOP Official Spied on by NSA Without Warrants*, THE NEW AM. (July 9, 2014, 9:36 AM), http://www.thenewamerican.com/usnews/constitution/item/18655-greenwald-gop-official-spied-on-by-nsa-without-warrants [http://perma.cc/7TPG-NG9E] (noting that discovery of the FBI's CONTINELPRO program led to Congress's creation of the Church and Pike Committees, which shut down unconstitutional surveillance programs).

list.[13] Those lists included such "dangerous characters" as Jane Fonda and Muhammad Ali.[14] Another program exposed by those committees—perhaps the most notorious of them all—was J. Edgar Hoover's decade-long campaign of surveillance and harassment directed at Martin Luther King and the Southern Christian Leadership Conference.[15] Under the auspices of Hoover, the FBI illegally bugged and recorded Dr. King's extramarital assignations.[16] A highlight reel of those extracurricular activities was later sent to his home, along with a note darkly threatening that he would be exposed unless he did the "one thing left for [him] to do" and removed himself from public life, by one means or another.[17] Somewhat more prosaically, Hoover provided enormous amounts of political intelligence derived from those taps to Lyndon Johnson, which was apparently useful in plotting strategy at the Democratic National Convention.[18]

Of course, not all of the abuses that occurred during that time are known. For example, historians have found routing slips of illegal wiretaps conducted by the FBI that were part of larger archives that were otherwise entirely destroyed.[19] Thus, from the

---

13. Catherine Rentz Pernot, *The NSA and the Telecoms*, PBS FRONTLINE (May 15, 2007), http://www.pbs.org/wgbh/pages/frontline/homefront/preemption/telecoms.html [http://perma.cc/PFC6-A36J] (discussing Operation SHAMROCK).

14. Michael X. Heiligenstein, *A Brief History of the NSA: From 1917 to 2014*, SATURDAY EVENING POST, Apr. 17, 2014, http://www.saturdayeveningpost.com/2014/04/17/culture/politics/a-brief-history-of-the-nsa.html [http://perma.cc/WMW2-7Q7R] (discussing project SHAMROCK and how the NSA used it to monitor civil rights leaders and opponents of the Vietnam War, including Jane Fonda and Muhammad Ali).

15. Danielle Cadet, *How The FBI Invaded Martin Luther King Jr.'s Privacy—And Tried To Blackmail Him Into Suicide*, HUFFINGTON POST (Jan. 25, 2014, 4:01 PM), http://www.huffingtonpost.com/2014/01/20/martin-luther-king-fbi_n_4631112.html [http://perma.cc/K7PM-7MX5] (discussing the extent of the FBI's targeting of Martin Luther King, Jr.).

16. *Id.*

17. *Suicide Letter to Martin Luther King, Jr.*, HISTORY GENIUS, http://history.genius.com/Federal-bureau-of-investigation-suicide-letter-to-martin-luther-king-jr-annotated [http://perma.cc/TR8U-3TMF] (last visited Nov. 15, 2014) (reproducing the text of the letter that the FBI sent to Martin Luther King, Jr.).

18. Hugh Sidey, *L.B.J., Hoover and Domestic Spying*, TIME, Feb. 10, 1975, http://jfk.hood.edu/Collection/White%20Materials/Watergate/Watergate%20Items%2020229%20to%2020569/Watergate%2020263.pdf [http://perma.cc/E6Q3-KJ3Y]

19. Athan G. Theoharis, *Introduction* to FBI WIRETAPS, BUGS, AND BREAK-INS: THE NATIONAL SECURITY ELECTRONIC SURVEILLANCE CARD FILE AND THE SURREPTITIOUS ENTRIES FILE, at viii–ix (Athan G. Theoharis ed., 1988), *available at*

existence of a few scraps that escaped destruction, we know the scope of illicit surveillance was larger than the list of confirmed abuses.[20] This is largely because when intelligence agencies deliberately misused the law and their powers for political purposes, elaborate steps were taken to conceal that activity from overseers.[21] For example, there was what was known as the "June Mail" protocol, which essentially meant that reports on activities that they were not supposed to be doing were marked "June."[22] So marked, these reports were routed separately, not filed in the central FBI system, and instead delivered directly to J. Edgar Hoover's personal and confidential file.[23] These included the fruits of Operation Sex Deviate, where Hoover gathered salacious tidbits about the rumored homosexuality or other sexual habits of prominent persons[24]—information that the FBI might find useful for one purpose or another.

A couple of things come out of knowing this history. One is that abuses of surveillance authorities might not be immediately apparent when they occur, as part of highly secret intelligence programs. Inadvertent violations of law will be detected, but people who are *deliberately* misusing their authority will take steps—because they are not stupid—to cover their tracks.

What follows is that it is not enough to critically inspect this program or that program for overt signs of misuse. We also need to think architecturally about what surveillance systems we as citizens are comfortable with the government constructing, given the possibility of oversight failure. Are there architectures that would fundamentally undermine democracy if they fell into the hands of someone like Hoover, or some successor deter-

---

http://cisupa.proquest.com/ksc_assets/catalog/10755_FBIFileWiretapsBugs.pdf [http://perma.cc/97ZY-YFUQ].

20. *See id*. at viii–ix.

21. *See* Ronald Kessler, *Hoover's Secret File*, THE DAILY BEAST (Aug. 22, 2011), http://www.thedailybeast.com/articles/2011/08/02/fbi-director-hoover-s-dirty-files-excerpt-from-ronald-kessler-s-the-secrets-of-the-fbi.html [http://perma.cc/4SU9-5DYG].

22. Theoharis, *supra* note 19, at i, vii.

23. *Id.*

24. Dudley Clendinen, *J. Edgar Hoover, 'Sex Deviates' and My Godfather*, N.Y. TIMES, Nov. 27, 2011, http://www.nytimes.com/2011/11/27/opinion/sunday/j-edgar-hoover-outed-my-godfather.html [http://perma.cc/WQT6-7GLL].

mined to misuse them for political purposes and able to block scrutiny of that misuse for several years?

Additionally, history shows we may need to think in less individualistic terms about privacy rights. By way of analogy, understand there are really two distinct dimensions to the expressive rights protected by the First Amendment. There is the interest that we have in protecting the right of an individual to speak, rooted in his dignity and autonomy as an individual.[25] But there is also the kind of structural or collective interest we all have in preserving free and open debate in a society where the people collectively determine public policy, at least indirectly. We all, as citizens of a democratic society, benefit from a government that does not determine which speakers are heard, even if we do not personally have anything controversial to say, and we are not interested in listening to speakers who do.

When we think in these more structural terms, we are much more likely to be lulled into complacency by that familiar question: "What do I have to worry about if I don't have anything to hide?" It is probably true that the NSA is not that interested in you if you are not Martin Luther King. But if they are spying on Martin Luther King, that should perhaps be of interest to you as a citizen, whether or not your conversations are picked up in the process.

On the flip side, when talking about our security interests, we should be much more precise in the way we talk about "balancing" them against privacy.[26] Typically the way these "balancing" arguments proceed is that we have, on the one side, the particular invasion at issue under a particular program—the collection of telephone records or the collection of international communications—and on the other side, the full weight of the entire national security interest in preventing catastrophic terrorist attacks.[27] This is not a serious way to do cost-benefit analysis. If every particularized invasion is always weighed against the full interest in pre-

---

25. *See, e.g.*, Erin Daly, *Human Dignity in the Roberts Court: A Story of Inchoate Institutions, Autonomous Individuals, and the Reluctant Recognition of a Right*, 37 OHIO N.U. L. REV. 381, 412 (2011).

26. *See* Leslie Harris, *Restoring the Balance Between Privacy and Security*, HUFFINGTON POST (July 10, 2013, 11:40 AM), http://www.huffingtonpost.com/leslie-harris/privacy-and-security_b_3573403.html [http://perma.cc/NUB7-7A9T].

27. *Id.*

venting a nuclear bomb from going off in New York, privacy will lose on every occasion.[28]

A more helpful way to frame the policy question would be something like this: If the annualized risk for an American of dying in a terror attack is 1 in 3.5 million,[29] does a particular program—let's say the bulk collection of telephone records—reduce that risk at the margin, compared with more targeted collection of telephone records, by enough to justify that invasion? Is it a reduction from 1 in 3.5 million to 1 in 4 million or 1 in 3.51 million? That would be a more useful discussion to have, in large part because when we look back at the track record of the programs we have seen disclosed over the past decade, they often do not live up to their initial billing.[30]

In the aftermath of that initial *New York Times* story about the warrantless wiretap component of the larger STELLARWIND program—authorized by President Bush[31]—Dick Cheney (among others) said that this was a program that had doubtlessly saved thousands of lives and averted numerous catastrophic terror attacks.[32] About five years later, the inspectors general of the intelligence community looked into it and found that the intelligence officials they spoke to were hard pressed to identify concrete intelligence successes attributable to the program.[33] In other anonymous interviews, many officials connected to that program suggested that it did not produce any really unique intelligence, and that the success stories cited publicly on behalf

---

28. *See id.*

29. *See* John Mueller & Mark G. Stewart, *The Terrorism Delusion: America's Overwrought Response to September 11*, 37 INT'L SECURITY 81, 96 (2012).

30. *See* Julian Sanchez, *The War on Terror's Jedi Mind Trick*, THE ATLANTIC (Dec. 23, 2013, 4:49 PM), http://www.theatlantic.com/politics/archive/2013/12/the-war-on-terrors-jedi-mind-trick/282620/ [http://perma.cc/7P2V-6SUS].

31. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html [http://perma.cc/V9TF-JJVE]; *see also* Barton Gellman et al., *Surveillance Net Yields Few Suspects*, WASH. POST, Feb. 5, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373.html [http://perma.cc/9SKD-P7ES].

32. Richard W. Stevenson & Adam Liptak, *Cheney Defends Eavesdropping Without Warrants*, N.Y. TIMES (Dec. 21, 2005), *available at* http://www.nytimes.com/2005/12/21/politics/21cheney.html [http://perma.cc/XMA7-KDBL].

33. *See Unclassified Report on the President's Surveillance Program, Report No. 2009-0013-AS*, DEP'T OF DEFENSE (JULY 10, 2009), *available at* http://fas.org/irp/eprint/psp.pdf [http://perma.cc/73F3-UGWZ].

of this program involved people who were already under surveillance by traditional methods, targeted by the warrants that the FBI had applied for and secured.[34]

This is a pattern seen over and over again with respect to "fusion centers," which are information sharing hubs created by federal-state partnerships.[35] For years they were touted as the centerpiece of our counterterrorism strategy and an invaluable and proven tool,[36] until a two-year Senate investigation concluded that they had effectively never produced any important intelligence leads, and, in fact, were mostly generating reports unrelated to the subject of terrorism.[37] To the extent that they did produce such reports, it was mostly red herrings that wasted investigative resources.[38]

Or consider the Section 215 program, which was initially touted as being responsible, *along with other programs*, for disrupting 54 terrorist incidents.[39] This is sort of like saying my cancer was cured by quartz crystals . . . along with chemotherapy. It later turned out that, in fact, the Section 215 program was used in about a dozen of those cases.[40] For the most part, the Section 215 program did not actually provide any new or useful intelligence

---

34. Sanchez, *supra* note 30.

35. *Press Release*, U.S. HOUSE COMMITTEE ON HOMELAND SECURITY, *McCaul, King Release Report on National Network of Fusion Centers*, July 26, 2013, *available at* http://homeland.house.gov/press-release/mccaul-king-release-report-national-network-fusion-centers [http://perma.cc/R4SN-8M2B].

36. *See* S. COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS, 10–17 (2012) (describing the history and governmental support for fusion centers as counterterrorism tools).

37. *See id.* at 32–35 (discussing multiple examples of reports that were unhelpful and unrelated to terrorism).

38. *See id.* at 32 (stating that when reports were reviewed, they were deemed useless).

39. *See* Ellen Nakashima, *NSA cites case as success of phone data-collection program*, WASH. POST, Aug. 8, 2013, http://www.washingtonpost.com/world/national-security/nsa-cites-case-as-success-of-phone-data-collection-program/2013/08/08/fc915e5a-feda-11e2-96a8-d3b921c0924a_story.html [http://perma.cc/FL63-8ZWV] (stating that the NSA surveillance has helped identify suspects or disrupt plots in 54 cases).

40. *See Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs: Hearing before the S. Jud. Comm.*, 113th Cong. (2013) (statement of John C. Inglis, Deputy Dir., Nat'l. Sec. Agency) (stating the program helped in about twelve of thirteen cases).

in those cases.[41] There is exactly one case, involving someone who had donated a few thousand dollars to the Somalian terror group Al-Shabaab and was later convicted on a material support charge, where a suspect was probably identified somewhat more quickly as the result of the metadata program than he would have been without it.[42] One has to question whether one material support conviction over the course of a decade is actually a sufficiently robust track record to justify the bulk acquisition of millions of Americans' telephone records.[43]

There are more examples,[44] but the pattern is that the benefits of the most controversial programs are touted in very dramatic terms initially. Yet, over time, their added value is much less impressive.

In regard to the telephone metadata program, the report produced by the Privacy and Civil Liberties Oversight Board[45] is both legally and empirically extremely thorough. In particular, it decisively undermines claims that the program was necessary to provide intelligence that could have been obtained via the more conventional targeted acquisition of telephone records.[46] Those claims are really just one instance of the more general argument that modern intelligence requires us to abandon the kind of traditional model of targeted, particular-

---

41. *See* Keynote Address by General Keith Alexander, Director, National Security Agency, Black Hat USA 2013, FEDERAL NEWS SERVICE, July 31, 2013 (stating that in the twelve cases, only eight produced leads for the FBI).

42. *See* United States v. Moalin, No. 10cr4246 JM, 2013 WL 6079518, *3 (S.D. Cal. Nov. 18, 2013) (stating that the defendant's charges, including material support, were based largely on the NSA information provided from the Section 215 program).

43. *See* Nakashima, *supra* note 39, at 1 (stating that the NSA "collects tens of millions of phone records from Americans").

44. *See, e.g.*, S. COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS, 101–05 (2012) (describing examples of intelligence reports that failed).

45. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 2 (2014) (hereinafter Report on Telephone Records) (stating that the report contains conclusions from a study of the Section 215 program and analysis regarding FISC's operation).

46. *See id.* at 146 ("[I]n those few cases where some information not already known to the government was generated through the use of Section 215 records, we have seen little indication that the same result could not have been obtained through traditional, targeted collection of telephone records.").

ized acquisition of information about people in favor of large-scale bulk acquisition of information designed to detect which individuals require further scrutiny. It is a departure that is already well underway, and one I find pretty troubling given the absence of evidence that the more traditional and targeted method is inadequate for the task.

This shift to a "wholesale" model of surveillance is particularly pronounced with respect to communications metadata, and it has been facilitated by the third-party doctrine.[47] Back in the late 1970s, the Supreme Court decided two seminal cases, *Smith v. Maryland*[48] and *United States v. Miller*,[49] on the premise that individuals surrender their privacy interest in information they provide to third parties like the telephone company[50]—or, now, Internet Service Providers.[51] This is a strange premise indeed. If, by allowing anyone else access to your data you have "assumed the risk" that they will turn it over to the government—with the consequence that there is no Fourth Amendment violation even when the government *compels* them to turn it over—why does the same principle not permit warrantless searches of homes, so long as you have a spouse or a roommate who *could* let the police in, if they decided to?[52]

Even if we were to accept this strange premise in the context of the late 1970s, technological changes have radically altered the implications of the third-party doctrine for our Fourth Amendment rights. There is an incredible amount of sensitive potential information in metadata, even considered at the indi-

---

47. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564–65 (2009) (defending the third party doctrine).

48. 442 U.S. 735 (1979).

49. 425 U.S. 435 (1976).

50. *See Smith*, 442 U.S. at 745–46 (finding no privacy interest in dialed phone numbers); *Miller*, 425 U.S. at 443 ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

51. *See* United States v. Beckett, 369 F. App'x 52, 56 (11th Cir. 2010) (stating criminal defendant did not have expectation of privacy for information obtained through ISPs or phone records).

52. *Contra* Georgia v. Randolph, 547 U.S. 103, 122–23 (2006) (stating consent by present wife was not enough to overcome non-consenting husband).

vidual level.[53] So long as the NSA has a phone book and can associate the numbers in those records with names, it allows them to know who has phoned a divorce lawyer, a suicide hotline, substance abuse counselor, an abortion provider, or who is making cellphone calls and sending texts at two in the morning, perhaps suggesting an illicit affair. Our social network activity can easily reveal our religious or political affiliations. In addition to the kind of information kept by Internet providers,[54] or the far greater quantity of data flowing through the Internet backbone—which includes, in effect, a record of almost everything you read,[55] as well as where you are physically on a moment-to-moment basis[56]—the unanticipated effect of that ruling is to strip Fourth Amendment protection from data that is, in many ways, more sensitive than the contents of the communications themselves.

Section 702 of the FISA Amendments Act permits blanket surveillance authorizations. Those are general warrants, plain and simple.[57] We are meant to feel reassured by the fact that Americans cannot be "targeted" under these authorizations,[58] even though our communications are intercepted.[59] But of

---

53. *See* Michael W. Loudenslager, *Why Shouldn't Attorneys Be Allowed to View Metadata?*, 15 J. TECH. L. & POL'Y 159, 162–70 (2010) (describing what metadata is and the information stored within metadata).

54. *See* Steven R. Morrison, *What the Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents*, 16 VA. J.L. & TECH. 253, 261 (2011) (describing email information kept by Internet Service Providers).

55. Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011) ("E-mails, web-surfing histories, credit card and address information, and search term records are all routinely stored by online entities and are potentially available to the government, or even to private parties that purchase customer information for marketing purposes.").

56. Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 567, 586 (2012) (explaining that geolocation tools can determine where an Internet user is physically located).

57. *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1646 (2010) ("[T]he [FISA Amendments Act] does not limit the government to surveillance of particular, known persons reasonably believed to be outside the United States, but instead authorizes so-called 'basket warrants' for surveillance and eventual data mining.").

58. *See* 50 U.S.C. § 1881a(b)(1)–(4) (2012).

59. *See* Barton Gellman, Julie Tate, & Ashkan Soltani, *In NSA-intercepted data, those not targeted far outnumber the foreigners who are*, WASH. POST, July 5, 2014, http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-

course, no particular person is the specific target of any general warrant—*that is what makes it a general warrant*. That is not much of a consolation if your communications can nevertheless be intercepted, not pursuant to the order of a neutral magistrate but at the discretion of an NSA analyst.[60] The scale of collection under these authorities,[61] makes it very difficult to police the system for misuse of that data.

It is also increasingly clear that the public's initial understanding of how these programs operated was fundamentally inaccurate.[62] Even the understanding of the Supreme Court, which formed the basis of the ruling in *Clapper v. Amnesty International USA*,[63] was grounded in a significant misunderstanding of how "targeting" under section 702 authorities operated.[64] Both the Court and most members of the public presumed that an American's communications could be intercepted without a warrant, but only if they were in contact with a foreign surveillance target.[65] But, in fact, your communications could *also* be intercepted if your communication *mentioned* a "selector," such as an e-mail address, that the NSA had tasked for collection.[66] So the NSA is essentially filtering all in-

---

data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [http://perma.cc/D3LJ-M6US].

60. *See id.*

61. *Id.* ("[T]he Office of the Director of National Intelligence disclosed that 89,138 people were targets of last year's collection under FISA Section 702. At the 9-to-1 ratio of incidental collection in Snowden's sample, the office's figure would correspond to nearly 900,000 accounts, targeted or not, under surveillance.").

62. *See* Timothy B. Lee, *Here's everything we know about PRISM to date*, WASH. POST, June 12, 2013, http:// www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ [http://perma.cc/GU3E-S2YD] (demonstrating the lack of information the public has had of the intricacies of PRISM).

63. 133 S. Ct. 1138 (2013).

64. *See* Alan Butler, *Standing Up to* Clapper*: How to Increase Transparency and Oversight of FISA Surveillance*, 48 NEW ENG. L. REV. 55, 75–76 (2013) (arguing that the harms characterized by the Court as "speculative" were proven by Edward Snowden's document release in June 2013).

65. *See Clapper*, 133 S. Ct. at 1148. Writing for the majority, Justice Alito's reasoning assumed that Amnesty International's communications could have only been intercepted without a warrant if the organization was (1) directly communicating with (2) non-U.S. persons (3) that the government decided to target. *See id.*

66. DIR. OF CIVIL LIBERTIES AND PRIVACY OFFICE, NAT'L SEC. AGENCY, NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 5 (2014), *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified

ternational communication, searching their contents by computer, and flagging those e-mails and other digital communications that reference a target, whether or not that target is actually a party to the conversation.[67]

When we consider that a "target" as defined by FISA can also be a corporate entity[68]—or an entire website, when the target is an entity like The Pirate Bay or Wikileaks[69]—the potential for large-scale interception of American communications is made fairly clear. Returning again to the question of "balancing," what we should be asking is not what particular abuses we have found out about to date. Although the suggestion is disturbing in one set of leaked NSA documents that "radicalizers" who are *not* terrorists, but who speak critically about the U.S. and justify violence against it in writing, could be targeted for smear campaigns using signals intelligence about their private online sexual activity.[70] Rather, the question we need to ask is: If someone with the intentions of a Hoover once again gained his powerful position, what effective limits would there be on his ability to use this intelligence gathering architecture in anti-democratic ways? Are there, and can there be, appropriate and necessary limits on the mass collection of Internet communications? What about enormous collection of telephone, financial, and other types of data that can paint an incredibly detailed portrait of anyone's life? There can be no meaningful

---

%20Document.pdf [http://perma.cc/U74N-4HPB] (noting that under Upstream, Internet service providers must help intercept "electronic communications . . . *about* tasked selectors" (emphasis added)).

67. *See* Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. TIMES, Aug. 8, 2013, http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all&_r=2& [http://perma.cc/U45S-3HRL].

68. 50 U.S.C. § 1881 (2012) (adopting the definition of 50 U.S.C. § 1801(m) to define "person" as "any group, entity, association, corporation, or foreign power"). With this definition, 50 U.S.C. § 1881a allows for the targeting of any corporation located outside of the United States. *See* 50 U.S.C. § 1881a(a) (2012).

69. *See* Massimo Calabresi, *WikiLeaks' War on Secrecy: Truth's Consequences*, TIME, Dec. 2, 2010, http://content.time.com/time/magazine/article/0,9171,2034488,00.html [http://perma.cc/5K8D-45LB] (detailing the WikiLeaks controversy of 2010 where the website released over 250,000 classified diplomatic cables).

70. *See* Glenn Greenwald, Ryan Gallagher, & Ryan Grim, *Top-Secret Document Reveals NSA Spied on Porn Habits As Part Of Plan To Discredit 'Radicalizers,'* HUFFINGTON POST (Nov. 26, 2013, 11:20 PM), http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html?1385526024 [http://perma.cc/Z328-YMKE].

guarantee of privacy—not "security" against unreasonable search—when this information is indiscriminately collected. Even if it is simply sitting in a database today,[71] it remains waiting to be scrutinized and searched.

Indeed, even if the initial "targeting" of NSA's collection is limited to foreigners, those databases can subsequently be searched using "selectors" associated with U.S. persons.[72] In other words, once that information is collected under a sweeping authority justified by the exigencies of foreign intelligence and counterterrorism, the NSA and the FBI are allowed to go in and search for an American's name, even though they would have needed a particularized warrant to do initial collection targeting that person.[73] What are the practical constraints on the misuse of that vast store of data? Given that the FISA court has itself been repeatedly misinformed about the technical details of how these programs operate, in some cases for years at a time,[74] the only realistic answer is that there are not any. We are effectively relying on the probity of intelligence officials.[75] We can hope they have been deserving of that trust so far—but in the long run, hope is not an acceptable strategy.

---

71. *See* NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, *supra* note 66, at 8 (noting that content and metadata for PRISM may be stored for up to five years, while Upstream data is retained for up to two years).

72. *See* Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet,'* THE GUARDIAN, July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [http://perma.cc/JJ3E-9ZNK] (detailing how an NSA program called XKeyscore "provides the technological capability, if not the legal authority, to target even US persons for extensive electronic surveillance without a warrant provided that some identifying information, such as their email or IP address, is known to the analyst.").

73. *See id.* ("While the FISA Amendments Act of 2008 requires an individualized warrant for the targeting of US persons, NSA analysts are permitted to intercept the communications of such individuals without a warrant if they are in contact with one of the NSA's foreign targets.").

74. *In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13, 2009 WL 9150913, at *5 (FISA Ct. Mar. 2, 2009) ("In summary . . . it has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR [bulk records] metadata.").

75. Cadet, *supra* note 15 (discussing how FBI Director J. Edgar Hoover expended significant Bureau resources spying on Dr. Martin Luther King, Jr. in order to delegitimize him).