Fordham Law Review

Volume 86 | Issue 6 Article 18

2018

The New Writs of Assistance

Ian Samuel
Harvard Law School

THE NEW WRITS OF ASSISTANCE

*Ian Samuel**

The providers of network services (and the makers of network devices) know an enormous amount about our lives. Because they do, these network intermediaries are being asked with increasing frequency to assist the government in solving crimes or gathering intelligence. Given how much they know about us, if the government can secure the assistance of these intermediaries, it will enjoy a huge increase in its theoretical capacity for surveillance—the ability to learn almost anything about anyone. This has the potential to create serious social harm, even assuming that the government continues to adhere to ordinary democratic norms and the rule of law.

One possible solution to this problem is for network intermediaries to refuse government requests for aid and attempt to sustain those refusals in court. Although this proposal has received an enormous amount of attention, there is substantial cause for skepticism about how well it can work. Congress has given the government wide authority to demand information and assistance through tools like subpoenas, the Stored Communications Act, and Title III. Even when the government does not have specific statutory authorization, courts have interpreted the All Writs Act to authorize a great deal of open-ended aid, consistent with the well-settled Anglo-American history of third-party assistance in law enforcement. It is also far from unheard of for the executive to read restrictions on its surveillance authority narrowly, and its own inherent powers broadly, to engage in surveillance that is quasi- or extra-legal.

A superior (or at least complementary) response to the problem is to restrict network intermediaries themselves by limiting how much they can learn about us and how long they can retain it. This approach treats enhanced state surveillance as a problem created by the intermediaries'

* Climenko Fellow and Lecturer on Law, Harvard Law School. Thanks to Rachel Barkow, William Baude, Tricia Bellia, Stephanos Bibas, Dan Epps, Noah Feldman, Barry Friedman, Jack Goldsmith, Michael Klarman, Leah Litman, Bruce Schneier, David Sklansky, Joseph Singer, Jonathan Zittrain, and all of my cofellows in the Climenko program. Thanks, also, to the late Jesse Climenko, both for endowing my fellowship and for his successful representation of one of the defendants in *United States v. Nardone*, discussed *infra*. I am also very grateful for the comments I received when I presented this paper at Drexel University School of Law, Indiana University Maurer School of Law, New York University School of Law, Notre Dame Law School, UCLA School of Law, and to the Colorado Federalist Society. Finally, thanks to Shannon McHugh Samuel, a scholar well suited to the helm of a whole university, let alone a modest household of two bookish academics.

stockpiling of data, and proposes to solve it at the root—which would, as a useful side effect, solve a number of other problems created by that stockpiling, too.

INTRODUCTION

> This is better than real memory, because real memory, at the cost of much effort, learns to remember but not to forget.[1]

In November 2015, a man died at the home of James Bates, in Bentonville, Arkansas, in what was alleged to be a murder.[2] As part of the investigation, the police searched Bates's home and discovered an Amazon Echo[3]—a voice-activated personal assistant that is always listening for users' commands.[4] The police wondered whether that microphone recorded

1. UMBERTO ECO, FOUCAULT'S PENDULUM 25 (William Weaver trans., Harcourt Brace & Co. 1989).

2. Amye Buckley, *Bentonville 34-Year-Old Charged in Hot Tub Death*, ARK. DEMOCRAT-GAZETTE (Feb. 29, 2016, 5:45 AM), http://www.arkansasonline.com/news/2016/feb/29/bentonville-34-year-old-charged-hot-tub-death/ [https://perma.cc/Y22F-NULS].

3. Amy B. Wang, *Can Alexa Help Solve a Murder Case? Police Think So, but Amazon Won't Give Up the Data*, L.A. TIMES (Dec. 28, 2016, 12:45 PM), http://www.latimes.com/business/la-fi-tn-amazon-alexa-police-20161228-story.html [https://perma.cc/LM4K-MX5T].

4. *Id.* (noting that the Echo is "equipped with seven microphones and responds to a 'wake word,'" and that when the device "detects the wake word, it begins streaming audio to the cloud, including a fraction of a second of audio before the wake word"). The Echo is essentially a "voice-controlled household computer," which can do things like play music, order things from Amazon, and read the news. Farhad Manjoo, *The Echo from Amazon Brims with Groundbreaking Promise*, N.Y. TIMES (Mar. 9, 2016), https://www.nytimes.com/

anything of interest on the night of the murder.[5] The Bentonville police got a warrant directed to Amazon, seeking any recordings or transcripts that Amazon had from Bates's Echo during the critical hours of the murder.[6] Amazon resisted,[7] but on the eve of a hearing on a motion to quash the warrant, Bates consented to Amazon turning over whatever data it had from his Echo, and the company promptly did so.[8] Though a legal showdown was averted, the curious case of the Bentonville Echo nonetheless lingered in the public and legal imagination.

With increasing frequency, the makers of networked devices and the providers of network services are being asked to provide interesting sorts of assistance to the government. Retroactively listening in on an alleged murder scene is just the start. The government has asked network service providers to help them listen in on or control people's cars, for example.[9] The police

---

2016/03/10/technology/the-echo-from-amazon-brims-with-groundbreaking-promise.html [https://perma.cc/A6QF-EWWP].

5. Wang, *supra* note 3.

6. Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant Exhibit A-1, at 1–2, Arkansas v. Bates, No. CR-2016-370-2 (Ark. Cir. Ct. Feb. 17, 2017) (Extension for Search Warrant). The attached affidavit notes that the police had searched Bates's house *specifically* to find "electronic devices capable of storing and transmitting any form of data that could be related to this investigation." *Id.* Exhibit A-1, at 5 (Affidavit for Search Warrant).

7. Tom Dotan & Reed Albergotti, *Amazon Echo and the Hot Tub Murder*, INFORMATION (Dec. 27, 2016, 7:01 AM), https://www.theinformation.com/amazon-echo-and-the-hot-tub-murder [https://perma.cc/SQJ8-SXX2]. The story was widely reported in many outlets, disappointingly few of which could resist variations on the same droll headline. *See, e.g.*, Sean Gallagher, *Police Ask: "Alexa, Did You Witness a Murder?,"* ARS TECHNICA (Dec. 28, 2016, 3:45 PM), http://arstechnica.com/tech-policy/2016/12/police-ask-alexa-did-you-witness-a-murder [https://perma.cc/6DQ3-LTT6]; Eliott C. McLaughlin & Keith Allen, *Alexa, Can You Help with This Murder Case?*, CNN (Dec. 28, 2016, 8:48 PM), http://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html [https://perma.cc/K5AC-BKET]; Elizabeth Weise, *Police Ask Alexa: Who Dunnit?*, USA TODAY (Dec. 29, 2016, 8:13 AM), https://www.usatoday.com/story/tech/news/2016/12/27/amazon-alexa-echo-murder-case-bentonville-hot-tub-james-andrew-bates/95879532/ [https://perma.cc/567S-5BEQ].

8. Tracy Neal, *Amazon Will Turn Over Any Data Recorded in Arkansas Man's Hot-Tub Death*, ARK. DEMOCRAT-GAZETTE (Mar. 7, 2017, 2:41 AM), http://www.arkansasonline.com/news/2017/mar/07/amazon-will-turn-over-any-data-recorded/ [https://perma.cc/SB6V-ZD52]. Bates consented, according to his attorneys, because he was "innocent of all charges." Amy Wang, *Can Amazon Echo Help Solve a Murder? Police Will Soon Find Out.*, WASH. POST (Mar. 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/09/can-amazon-echo-help-solve-a-murder-police-will-soon-find-out/ [https://perma.cc/44L8-9TVS]. Another reason could have been that because the Echo does not stream anything to Amazon "without the wake word being detected," Bates thought it unlikely that the device had captured anything of interest. *Id.*

9. *See, e.g.*, Marla Carter, *VIDEO: 12-Year-Old Leads Police on High-Speed Chase*, ABC13 (July 1, 2016), http://abc13.com/news/video-12-year-old-leads-police-on-high-speed-chase/1409974/ [https://perma.cc/C95A-67HD]. The driver of the car was a twelve-year-old girl, who apparently reached speeds of almost 120 miles per hour during a chase, at points squeezing narrowly between cars and into oncoming traffic at rush hour. *Id.*

routinely ask cell phone providers to help track their customers' location.[10] The digital forensic chief of London's Metropolitan Police has openly dreamed of a world where the police can get help from the makers of network-connected doorbells to see "who has rung the door," or even from companies selling network-connected, camera-equipped refrigerators, to disprove claimed alibis.[11] (Who *did* eat those plums in the icebox, anyway?) The government has begun to discover how useful network-attached devices can be, if only the assistance of network service providers can be procured. Gradually at first, and lately much faster, those companies have begun to receive demands that they provide such assistance. These demands take various forms: from routine legal tools like subpoenas and search warrants, to the far more exotic commands possible under the open-ended All Writs Act. For want of an existing umbrella term, this Article refers to them collectively as "the new writs of assistance." Given the ubiquity of network-connected devices, and how much they can learn about our lives, these commands of aid provide the state with potential access to more information than has ever been available before.

This Article argues that the government's use of the new writs of assistance can provide it with nearly unlimited knowledge about our lives, and that this is a serious problem.[12] This Article also argues that direct resistance to these orders by the intermediaries is unlikely to mitigate this problem, and that it is dangerous for these intermediaries to behave as if the government can be reliably prohibited from using private surveillance infrastructure for its own ends. Therefore, this Article proposes that we should plan for the possibility that the government will probably be able to learn anything about us that a network service provider knows, and we should impose limits on what they can learn about us and how long they may retain that knowledge.

The basic forces at work have been recognized for some time. Indeed, there is a vast literature about the private surveillance apparatus.[13] This

10. *See generally* Ian Samuel, Note, *Warrantless Location Tracking*, 83 N.Y.U. L. REV. 1324 (2008) (discussing the now-common practice by police of tracking suspects through their cell phones).

11. Sarah Knapton, *Fridges and Washing Machines Could Be Vital Witnesses in Murder Plots*, TELEGRAPH (Jan. 2, 2017, 9:04 AM), http://www.telegraph.co.uk/science/2017/01/02/fridges-washing-machines-could-vital-witnesses-murder-plots/ [https://perma.cc/JE24-QUM9]. "The crime scene of tomorrow," said the official, "is going to be the internet of things." *Id.*

12. The information that network intermediaries have would make it extremely easy, for example, to construct a database of every Muslim in the United States—including the precise location of every such person in real time.

13. *See, e.g.*, BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 234–38 (2017); BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 47–49 (2015); Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1912–18 (2013); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246 (1998); Alex Kozinski & Eric Nguyen, *Has Technology Killed the Fourth Amendment?*, 2011 CATO SUP. CT. REV. 15, 16–19; Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 112–22 (2018); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1611 (1999); Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 152–55 (2005).

Article aims to add two things to this literature. The first is a descriptive account of just how likely it is that the government will gain use of this apparatus. Here, this Article aims to illustrate just how strong the government's hand is and how historically normal it would be for network intermediaries to be pressed into government assistance. The second is a related normative claim about why direct regulation of network service providers is an attractive alternative solution to this problem.

Part I describes the basic problem. It is now possible to gather, transmit, store, and analyze massive amounts of information about the day-to-day lives of private people, and private businesses have rapidly emerged to collect and monetize that private information. The government has gotten interested in that data, which will soon leave us in a world where the state knows far more about us than was previously possible. Part II argues that the standard response to this problem—ex post resistance to requests for aid by network intermediaries—is unlikely to work. Finally, Part III proposes that the collection and disposal of personal information be regulated on the front end to account for the possibility that the government may be able to learn anything about us that network intermediaries know.

I. AN ACCIDENTAL PANOPTICON

This Part describes the basic problem we are now facing. It is now technically feasible to collect a massive amount of information about the day-to-day lives of ordinary people, far more than has ever been available before. In response, private businesses have begun to gather and monetize that information in enormous quantities. But the government has gotten interested in this trove of user data for its own purposes—a prospect that this Part argues is very dangerous.

A. Material and Commercial Origins of the Private Surveillance State

Rapid advances in a group of technologies have made it possible to collect enormous amounts of personal information about a large number of people.[14] In 1965, Gordon Moore—an electronic engineer and founder of a semiconductor company—observed that the cost curve of integrated circuits was improving exponentially, enabling the computing power of such circuits to roughly double each year.[15] Moore predicted that this would continue,

14. I begin with a material story because I regard the legal and policy issues that this Article addresses as in large part "superstructural, dependent for their form and content upon determining forces emanating from the economic basis of society." HUGH COLLINS, MARXISM AND LAW 22 (1982). There is a robust and interesting debate about the extent to which this can be said to be true for all legal questions, and if so, what the implications are. *See, e.g.*, Mark V. Tushnet, *Marxism as Metaphor*, 68 CORNELL L. REV. 281, 281 (1983) (reviewing COLLINS, *supra*).

15. Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, ELECTRONICS, Apr. 19, 1965, at 114–17. Specifically, Moore observed that the cost-effective number of components on each circuit had been roughly doubling each year, and he expected that to go on for at least another decade. *Id.* at 115. Integrated circuits are "arrays of transistors and other components built from a *single* chip of semiconductor material," as opposed to being

leading to such wonders as home computers and even "personal portable communications equipment."[16] This prediction turned out to be right, and the cost of components on integrated circuits has fallen by "roughly a factor of a billion over the last 50 years."[17] Meanwhile, the costs of storing, collecting, and transmitting information decreased,[18] as our ability to do those things, as well as our ability to collect and transmit information (using inexpensive microphones, cameras, and the like) soared.[19] For example, the number of hosts connected to the internet and the price performance of wireless networking were experiencing similar exponential growth during that period.[20] The overall rate of change in these systems has been exponential and accelerating.[21]

It has therefore become possible, in a very short amount of time, to build and sell cheap, powerful, small computers that collect, transmit, and store vast amounts of information about the world and individuals.[22] Mobile

"circuits constructed from discrete transistors." PAUL HOROWITZ & WINFIELD HILL, THE ART OF ELECTRONICS 61 (2d ed. 1989) (emphasis added).

16. Moore, *supra* note 15, at 114. Even an "electronic wristwatch" would be feasible, Moore thought, at least as soon as a suitable display could be invented. *Id.* Moore saw the biggest potential, however, in the "production of large systems," such as digital filters for telephone communications. *Id.*

17. Rachel Courtland, *How Much Did Early Transistors Cost?*, IEEE SPECTRUM (Apr. 16, 2015, 6:30 PM), http://spectrum.ieee.org/tech-talk/semiconductors/devices/how-much-did-early-transistors-cost [https://perma.cc/SA7B-XTWZ].

18. *See* Matthew Komorowski, *A History of Storage Cost*, MKOMO.COM (Sept. 8, 2009), http://www.mkomo.com/cost-per-gigabyte [https://perma.cc/7BMV-T5ZF]. In December 1981, a nineteen-megabyte Winchester hard disk cost $5495. *Computer Specialties Advertisement*, CREATIVE COMPUTING, Dec. 1981, at 233. By July 2009, it was possible to purchase a one-terabyte hard drive (one million megabytes) for $74.99—a cost of seven cents per gigabyte, around four million times cheaper than twenty-eight years prior. Komorowski, *supra*; *see also Computer Specialties Advertisement*, *supra*.

19. *See* Lee Rainie & Janna Anderson, *The Internet of Things Connectivity Binge: What Are the Implications?*, PEW RES. CTR. (June 6, 2017), http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/ [https://perma.cc/X86C-9EGB].

20. *See* Ray Kurzweil, *The Law of Accelerating Returns*, KURZWEIL ACCELERATING INTELLIGENCE (Mar. 7, 2001), http://www.kurzweilai.net/the-law-of-accelerating-returns [https://perma.cc/FHX2-7M8N].

21. *Id.*; *see also* RAY KURZWEIL, THE AGE OF SPIRITUAL MACHINES 30–32 (1999). Certain of the conclusions that Kurzweil draws from this are controversial, to say the least. *See, e.g.*, Alex Beam, *That Singularity Sensation*, BOS. GLOBE (Feb. 24, 2005), http://archive.boston.com/ae/books/articles/2005/02/24/that_singularity_sensation/ [https://perma.cc/CM96-G4QF] (noting Kurzweil's receipt of "hooting skepticism" for certain of his forward-looking claims). Luckily, one need not sign on to (for example) Kurzweil's prediction of a technological "singularity," in which human consciousness will merge with machine intelligence, to make use of his descriptive data about the rate of historical change to this point.

22. One estimate, published in 2011, of the world's technological capacity to "store, communicate, and compute information" suggested that over the previous several decades, our per-capita capacity to compute information had doubled every fourteen months, our capacity to transmit information had doubled every thirty-four months, and our capacity to store information had doubled every forty months. Martin Hilbert & Priscila López, *The World's Technological Capacity to Store, Communicate, and Compute Information*, 332 SCIENCE 60, 63–64 (2011). To put this in perspective, this means that every year, humans can "carry out roughly 60% of the computations that could have possibly been executed by all

phones, for example, are in constant radio contact with cell towers, generating information about where we are—and where we are likely to go next.[23] The entire nature of computers is to generate information about the world they can sense and what they are doing with the data they work on.[24] It is now routine to carry around a mobile phone with multiple cameras, microphones, and other sensors, which are all attached to a high-speed, always-on network connection.[25]

Rich business opportunities have been created by this new ability to collect and process information about private people—and firms have leapt to seize those opportunities. The term that is generally used to describe this field of burgeoning opportunities is "surveillance capitalism."[26] Behavioral advertising (gathering information about people to more precisely target them with sales pitches) is an enormous business, and it provides the principal revenue for modern juggernauts like Google.[27] Search engine providers "know if you looked into breast cancer symptoms, sought marriage counseling, worried whether your kid was autistic, or wondered how to treat your hemorrhoids," and your cell phone provider "knows where you've been" and "where you are right at this moment."[28] DVRs know whether you watch CNN or Fox News.[29] Sometimes this information gathering is done

existing general-purpose computers before that year." *Id.* at 64. Hilbert and López have, much like Moore did, charts illustrating this growth on a logarithmic scale—all quite steady looking. *See id.* at 62 figs.4–5; *see also* Moore, *supra* note 15, at 115–16.

23. *See* SCHNEIER, *supra* note 13, at 1–4. As Schneier observes, the "accumulated data can probably paint a better picture of how you spend your time than you can, because it doesn't have to rely on human memory," and indeed, "researchers were able to use this data to predict where people would be *24 hours later*, to within 20 meters." *Id.* at 2; *see also* Manlio De Domenico et al., *Interdependence and Predictability of Human Mobility and Social Interactions*, 9 PERVASIVE & MOBILE COMPUTING 798, 798 (2013).

24. SCHNEIER, *supra* note 13, at 13 (arguing that it is the nature of computers to "constantly produce data" as a "by-product of everything they do"). Schneier notes, "Connect to the Internet, and the data you produce multiplies: records of websites you visit, ads you click on, words you type." *Id.*

25. *See* Brian Klug, *Some Thoughts About the iPhone 5S Camera Improvements*, ANANDTECH (Sept. 13, 2013, 1:19 AM), http://www.anandtech.com/show/7329/some-thoughts-about-the-iphone-5s-camera-improvements [https://perma.cc/QH6G-TBY5] (discussing the ever-increasing quality of Apple's iPhone cameras).

26. Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 75 (2015). Zuboff argues that "big data" is "the foundational component in a deeply intentional and highly consequential new logic of accumulation," which "aims to predict and modify human behavior as a means to produce revenue and market control." *Id.*

27. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1938 (2013) (citing DAVID KIRKPATRICK, THE FACEBOOK EFFECT 260–66 (2010); STEVEN LEVY, IN THE PLEX 262–63, 336–37 (2011); SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING 26–30 (2011)).

28. FRIEDMAN, *supra* note 13, at 237 ("In theory it may be possible to go off the grid and avoid opening yourself up to any scrutiny—the Unabomber pulled it off for a while—but for most of us it is impossible to live that way."); *see also* Kozinski & Nguyen, *supra* note 13, at 16 (discussing how very little can remain private in today's world and how people must become aware of the privacy implications of their activities).

29. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 109 (2008).

to make our lives more convenient.[30] Sometimes it is done as a sort of price subsidy: in order to offer a product for free, a network service provider will gather data on its users and then monetize that data. As Bruce Schneier puts it, "Surveillance is the business model of the Internet [because] people like free, and people like convenient."[31]

Consequently, in a relatively short order, we have come to live our lives online, and in the constant presence of network-attached devices, which operate according to rules written by their manufacturers to enhance the profit they can derive from observing us.[32] By itself, this situation presents a legitimate cause for societal concern.[33] But it is even more concerning when the government comes to use the private surveillance system for itself.

B. Leviathan Online

Unsurprisingly, the government has become interested in using this new trove of data for its own reasons. Location data is incredibly useful in crime solving because it can establish *precisely* where a certain person was, and when.[34] But to do this, the government needs the help of the network service providers—help that the providers are not always eager to give. So the government frequently resorts to court orders to obtain this data. These orders can command either the production of information that network intermediaries already have, the collection of information that they do not yet have, and could, in a technical sense, command the construction of new surveillance capabilities for existing devices.

The most basic way the government can use network service intermediaries to learn about us is by asking them for the information they already have. This Article refers to these, generically, "orders of production." In federal court, both the civil and criminal rules provide broad subpoena authority for investigators.[35] Many administrative agencies and

30. Kozinski & Nguyen, *supra* note 13, at 15, 23.

31. SCHNEIER, *supra* note 13, at 49.

32. Henry Farrell, *The Tech Intellectuals*, DEMOCRACY, Fall 2013, at 51, 56 ("Much of our life is conducted online, which is another way of saying that much of our life is conducted under rules set by large private businesses, which are subject neither to much regulation nor much real market competition.").

33. *See id.* at 56–57 ("Facebook users may not like the ways in which Facebook uses their personal information, but their only real choices are to put up with it or to cut themselves off from a large part of their social life.").

34. Samuel, *supra* note 10, at 1324–25 ("Tracking a suspect's precise movements may shatter a claimed alibi: In Scott Peterson's murder trial, for example, Peterson's cell phone records were introduced to establish his whereabouts on the morning of his wife's murder, belying his version of the events of that morning."); *see also* United States v. Carpenter, 819 F.3d 880, 885 (6th Cir. 2016) (detailing how the government used location data to create "maps showing that [the defendants'] phones were within a half-mile to two miles of the location of each of the robberies around the time the robberies happened"), *argued*, No. 16-402 (U.S. Nov. 29, 2017).

35. *See, e.g.*, FED. R. CRIM. P. 17(c)(2) (providing for a subpoena to be quashed or modified when "compliance would be unreasonable or oppressive"); FED. R. CIV. P. 45(d)(3) (providing that a subpoena may be quashed when, among other things, compliance would impose an "undue burden").

law enforcement entities have subpoena authority of their own.[36] Many federal statutes authorize the government to demand ex parte that network service providers hand over information about their customers and records of their customers' activities.[37] Using subpoenas to obtain personal information in this way has been routine for at least a decade.[38] Specialized warrants and other statutory procedures also contemplate network service providers giving over information that they already have.

Even if a network service provider does not already have the information the government needs, the government may attempt to secure an order requiring the provider to collect and transfer that information. This Article calls this sort of order an "order of collection." That is, the government may seek an order requiring the network service provider to use the devices a consumer already has, or the network infrastructure it has built, to gather information for the government. For example, in the course of a Las Vegas corruption investigation,[39] the government wanted to listen in on conversations taking place in a particular car.[40] The owner had an OnStar-like system in the car, of the sort that assists drivers in "activities from the mundane—such as navigating an unfamiliar neighborhood or finding a nearby Chinese restaurant—to the more vital—such as responding to emergencies or obtaining road-side assistance."[41] The government wanted to turn the system's in-car microphone on and listen.[42] Such requests have become fairly routine.[43]

---

36. Several federal statutes authorize "federal intelligence investigators (generally the FBI) to request that communications providers, financial institutions and credit bureaus provide certain types of customer business records, including subscriber and transactional information related to Internet and telephone usage, credit reports, and financial records." BRIAN T. YEH & CHARLES DOYLE, CONG. RESEARCH SERV., RL33332, USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005 (H.R. 3199): A LEGAL ANALYSIS OF THE CONFERENCE BILL 10 (2006). These "national security letters," as these pseudosubpoenas are called, do not require judicial approval, and are subject to nondisclosure provisions that in certain circumstances forbid the recipient from revealing that they have received such a request. *Id.* at 10–12.

37. *Id.* at 10.

38. *See* Slobogin, *supra* note 13, at 140 ("[F]acilitated by the computerization of information and communication, government routinely obtains *personal* medical, financial[,] and email records, in connection with investigations that have nothing to do with business or governmental corruption.").

39. Brief for United States at 3, *In re* Emergency Application for an Order Compelling ATX Technologies, Inc. to Show Cause, No. 2:01-cv-01495 (D. Nev. Dec. 19, 2001), ECF No. 1.

40. *Id.* at 1 (noting that the district court entered an order authorizing "roving interceptions" in a car).

41. Co. v. United States (*In re* Application of the U.S. States for an Order Authorizing the Roving Interception of Oral Commc'ns), 349 F.3d 1132, 1133 (9th Cir. 2003).

42. *See id.* at 1146. The government lost in that case, although on technical grounds. *See id.* ("Because, given the set-up of the System, the surveillance could not be completed with 'a minimum of interference,' the district court erred in ordering the Company's assistance.").

43. *See, e.g.*, State v. Wilson, 2008 Ohio 2863, ¶ 2 (Ct. App. 2008) ("While monitoring the vehicle, the OnStar employee overheard the occupants of the vehicle discussing a possible illegal drug transaction. The employee permitted the Sheriff's dispatcher to listen to the conversation."); Motion to Suppress at 1, United States v. Dantzler, No. 3:10-cr-00024 (W.D.

Finally, there are yet-more exotic scenarios, where the government obtains an order for the network service provider to build something new or enable the collection or production of information that the government wants. This Article calls these "orders of construction." For example, in February 2016, the FBI recovered an iPhone that had belonged to Syed Farook, the object of a high-profile terrorism investigation.[44] The phone had security features designed to stop anyone other than its owner from easily accessing its contents.[45] The FBI asked Apple to develop a new version of the operating system without those security features, which the FBI could then install on Farook's seized phone to access its contents.[46]

As the above taxonomy indicates, my principal focus in this Article is ordinary law enforcement, of the kind conducted through court orders and normal legal process. But the same dynamics are at work with intelligence gathering, as well as what Barry Friedman and Maria Ponomarenko have called the "new policing."[47] This policing refers to police activity that is "proactive and programmatic, rather than reactive and investigative," and it is characterized by universal public surveillance, routine use of administrative searches, checkpoints, and other forms of investigation not designed to unearth evidence of any particular crime.[48] Both intelligence gathering and the "new policing" are similar in that they are not founded on court orders or individualized suspicion.[49] That, if anything, deepens the problem.

Although each of these types of assistance orders is different in important ways, all share a familial relationship[50] in that they all involve network

---

La. Mar. 31, 2010), ECF No. 17-2 (arguing that law enforcement "effectively ordered OnStar to assist law enforcement with locating the car Mr. Dantzler was supposed to be driving").

44. *See* Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/69b903ee-d4d9-11e5-9823-02b905009f99_story.html [https://perma.cc/RCB8-L32R]. The investigation concerned the December 2, 2015, shooting in San Bernardino, California, which killed fourteen people and injured another twenty-two. *Id.*

45. *Id.*

46. *Id.* Specifically, the FBI wanted Apple to develop a version of the operating system iOS that would permit the FBI to "submit passcodes" to the phone without any "delay between passcode attempts," and which would not include the standard "auto-erase function" that wipes the phone after a certain number of unsuccessful passcode attempts. *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, slip op. at 2 (C.D. Cal. Feb. 16, 2016). Put differently, the FBI wanted to be able to guess the passcode by brute force, quickly trying every possible passcode with no undesirable side effects.

47. Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1871 (2015).

48. *Id.*

49. *Id.* at 1871–72 (noting that as the "mission of many law enforcement officials has grown or shifted to include intelligence gathering," the result has been "panvasive dragnets" that "by their very nature intrude upon the privacy and security of large swaths of the law-abiding public").

50. I mean this in the sense used by Ludwig Wittgenstein. *See* LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS §§ 65–66 (G.E.M. Anscombe trans., Basil Blackwell Oxford 3d ed. 1968) (1958) (arguing that even things that do not all share a single common characteristic may be "*related* to one another in many different ways," describing the classification of board games, Olympic games, and gaming with dice as "games" as an

service providers aiding the government. Thus, this Article refers to them collectively as the "*new writs of assistance*." The writ of assistance used to be a very common method of law enforcement during the seventeenth and eighteenth centuries.[51] The example known best to Americans is the customs writ of assistance—a "document that in the name of the king ordered a wide variety of persons to help the customs man make his search."[52] The customs writ of assistance fell into disrepute and contributed to the coming of the American Revolution because it was generally issued without particularized suspicion.[53] But that is not necessarily the feature of the writ of assistance intended to be invoked with its name here. Some of the new writs of assistance can be issued on very little suspicion, though others require a high showing.[54] Rather, the conceptual similarity is that they require a third party to help—to *assist*—with some aspect of otherwise-authorized law enforcement.

C. A State That Could See Us as God Does

If private network service providers are gathering unprecedented amounts of information about us, and the government is interested in that information, the next question is, is that a problem? Is it a problem for the government to be theoretically able to learn nearly *anything* about us?

Some government officials believe that it is not a problem at all. In fact, some believe that the major looming crisis is that network service providers will not enable *enough* surveillance, thereby hindering crime solving, intelligence gathering, and various other worthwhile objectives.[55] In 2014, James Comey—then the director of the FBI—gave a speech at the Brookings

---

example); *cf.* PGA Tour, Inc. v. Martin, 532 U.S. 661, 700–01 (2001) (Scalia, J., dissenting) (arguing that "the very nature of a game [is] to have no object except amusement (that is what distinguishes games from productive activity)"). In the legal literature, Daniel Solove has argued that privacy is best understood using this "family resemblance" idea. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1099 (2002). Solove also argues that "the quest for a common denominator or essence . . . can sometimes lead to confusion." *Id.* at 1099. The concept has also been applied in property law, *see, e.g.*, J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA L. REV. 711, 783–84 (1996), religion, *see, e.g.*, Kent Greenawalt, *Religion as a Concept in Constitutional Law*, 72 CALIF. L. REV. 753, 763–64 (1984), and many other areas.

51. M.H. SMITH, THE WRITS OF ASSISTANCE CASE 29–30 (1978) (stating that the writ of assistance was "a fairly common feature in the modes of executive rule" then common, and giving as examples the King's subjects being commanded to give assistance in the "impressment of seamen," the "seduction of ordinance workmen," and many other things).

52. *Id.* at 29. For further discussion of the customs writ of assistance, see *infra* notes 178–83.

53. SMITH, *supra* note 51, at 29.

54. *See infra* Part II.A.

55. *See, e.g.*, James B. Comey, Dir., FBI, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Address Before the Brookings Institution (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/G8SC-9SQ8]. Comey argued that we are "online, in one way or another, all day long," and our "phones and computers have become reflections of our personalities, our interests, and our identities." *Id.* But Comey lamented that the government was not "always able to access" this information, which was creating a "significant public safety problem." *Id.*

Institution calling for legislative changes to solve what he called the "Going Dark" problem: the failure, in his view, of the law to "keep up with changing technology and to maintain our ability to actually collect the communications" the government was interested in.[56] This basic idea has been echoed by some in the scholarly literature. Alan Rozenshtein, for example, notes that even if the widespread existence of networked devices enables "a net increase in government surveillance," that surveillance may be nonetheless fettered by serious "constraints."[57]

These arguments, however, have generally not considered the full scope of what is possible to know about us with the compelled cooperation of modern network intermediaries. Such intermediaries have at least theoretical access to everywhere we go;[58] the contents of our communications;[59] what we do and say any time we are within range of a network-attached camera or microphone;[60] everything we purchase, at what price, and from whom; every website we visit, and when, along with our search history; the amount of time we spent on each site; what links we clicked, and what ads interested us;[61] what goes on in our homes;[62] and any other information about us that can be

---

56. *Id.* "Kids," Comey said, have a thing called "FOMO, or 'fear of missing out.'" *Id.* *See generally* Andrew Przybylski et al., *Motivational, Emotional, and Behavioral Correlates of Fear of Missing Out*, 29 COMPUTERS HUM. BEHAV. 1841 (2013) (discussing the FOMO phenomenon). "With Going Dark," said Comey (in an analogy he evidently could not be talked out of ahead of time):

> those of us in law enforcement and public safety have a major fear of missing out—missing out on predators who exploit the most vulnerable among us . . . missing out on violent criminals who target our communities . . . missing out on a terrorist cell using social media to recruit, plan, and execute an attack.

Comey, *supra* note 55 (alterations in original).

57. Rozenshtein, *supra* note 13, at 111. Somewhat relatedly, Orin Kerr has called for "technology neutrality" in development of Fourth Amendment rules for networked communications, to ensure that the government's law enforcement functions are never made worse off by technology—to ensure the degree of privacy the Fourth Amendment requires online does not exceed "the degree of privacy protection that the Fourth Amendment provides in the physical world." Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007 (2010).

58. This information could be inferred from your mobile phone's location data. It is a matter of debate whether such access constitutes a Fourth Amendment "search" and whether this information can be accessed without a warrant or even any constitutional "reasonableness" constraints, such as probable cause. *See* Samuel, *supra* note 10, at 1339–49. The Supreme Court will soon decide whether or not it can be. *See* Carpenter v. United States, No. 16-402 (U.S. argued Nov. 29, 2017).

59. As long as it is retained, this information is available to the government under the Stored Communications Act. Under many circumstances, the government may access a person's communications without notice to him or her. *See* 18 U.S.C. § 2703(b)(1)(A) (2012).

60. *See* ZITTRAIN, *supra* note 29, at 110 ("Mobile phones can be reprogrammed at a distance, allowing their microphones to be secretly turned on even when the phone is powered down. All ambient noise and conversation can then be continuously picked up and relayed back to law enforcement authorities, regardless of whether the phone is being used for a call."); *see also* United States v. Tomero, 462 F. Supp. 2d 565, 569 (S.D.N.Y. 2006) (considering a case of continuous mobile-phone monitoring).

61. This information is gathered and routinely stored for advertising purposes. *See* SCHNEIER, *supra* note 13, at 52–53.

62. There are already many network-attached home security cameras, which retain security footage for some time. *See, e.g.*, *Nest Aware*, NEST, https://nest.com/nest-aware/ [https://perma.cc/5YJE-7UH7] (last visited Apr. 13, 2018) (offering plans that retain video

algorithmically inferred from the above, such as our religion, our political opinions, our sexual orientation, our views on Renaissance versus medieval art, our true opinion about our mothers, or anything else. Essentially all of this is technically possible now, and it will only get easier as the technological and commercial forces described above[63] continue their march. There has never been a state in the history of human civilization with the capability to do these things, which, by itself, is a good reason for caution.[64] But, on the merits, would it be a problem to have a state that could see us as God might? Or is it wise to "make the Leviathan all seeing so that he may protect us all the better"?[65]

Survey evidence indicates that most people would find this world frightening.[66] So does popular literature.[67] Almost no one believes that it would be good to have this kind of all-encompassing record of their life, especially in government hands.[68] The government could never have

---

from ten to thirty days). The "Nest IQ" is apparently powerful enough to "read the title of a book printed on a hardcover spine" from across the room. Darrell Etherington, *Nest's Latest Home Camera Is the Super Smart Nest Cam IQ*, TECHCRUNCH (May 31, 2017), https://techcrunch.com/2017/05/31/nests-latest-home-security-camera-is-the-super-smart-nest-iq/ [https://perma.cc/97QP-4FAH].

63. *See supra* Part I.A.

64. *Cf.* PROTECTING PUBLIC HEALTH & THE ENVIRONMENT: IMPLEMENTING THE PRECAUTIONARY PRINCIPLE (Carolyn Raffensperger & Joel Tickner eds., 1999) (discussing the "precautionary principle"); Nassim Nicholas Taleb et al., The Precautionary Principle (with Application to the Genetic Modification of Organisms) 1 (Sept. 4, 2014) (unpublished working paper) (on file with the Extreme Risk Initiative, N.Y.U. School of Engineering) (arguing that if "an action or policy has a suspected risk of causing severe harm to the public domain (such as general health or the environment)," then "the burden of proof about absence of harm falls on those proposing the action").

65. Oral Dissent of Justice Scalia at 10:45, Maryland v. King, 133 S. Ct. 1958 (2013) (No. 12-207), https://apps.oyez.org/player/#/roberts6/opinion_announcement_audio/22619 [https://perma.cc/M8UA-Z2YL]. *Maryland v. King*, 133 S. Ct. 1958 (2013), concerned the legality of taking a person's DNA without any suspicion that it would reveal evidence of a crime, *id.* at 1965–66. The Court approved the practice. *Id.* Justice Scalia, joined by Justices Ginsburg, Sotomayor, and Kagan, dissented. *Id.* at 1980 (Scalia, J., dissenting). The quotation about an all-seeing Leviathan does not appear in the written dissent—only the Justice's oral statement from the bench—although it was widely reported at the time of the decision. *See, e.g.*, Joan Biskupic, *Analysis: With Trademark Vigor, Justice Scalia Dissents in DNA Case*, REUTERS (June 3, 2013, 3:41 PM), https://www.reuters.com/article/us-usa-court-scalia-analysis/analysis-with-trademark-vigor-justice-scalia-dissents-in-dna-case-idUSBRE95211Y20130603 [https://perma.cc/UJ7Y-CJ52].

66. *See, e.g.*, MARY MADDEN & LEE RAINIE, PEW RESEARCH CTR., AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE 5 (2015), http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf [https://perma.cc/9ZV6-WN2H]. Overwhelming majorities of people regard it as important to be in control of who can get information about them and to be able to speak confidentially about their personal lives with people they trust. *Id.* at 17.

67. At this point, it is so common for dystopian fiction to feature an omniscient surveillance state as to be cliché. *See, e.g.*, CORY DOCTOROW, LITTLE BROTHER (2008); DAVE EGGERS, THE CIRCLE (2013); GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949). But the cliché is the point: it is evidence of a certain kind of fear that is widely held and durable across time.

68. Only 28 percent of people believe that it is reasonable for the government agencies to maintain records or archives of their activities for "[a]s long as they need to." MADDEN & RAINIE, *supra* note 66, at 25. Even fewer believe that about online advertisers, search engine providers, or social media sites. *Id.*

achieved political consensus to install location trackers on the person of every citizen, even subject to a promise that the location tracking would only be activated with a court order.[69] That alone suggests that there is a problem: the government should not be able to acquire a power accidentally that it could never have acquired on purpose. It is one thing to build something dangerous and quite another to build it by accident.

On the merits, there are many practical harms that such a large increase in the government's theoretical capacity for surveillance might cause. For one, a government with such an all-seeing theoretical capacity for surveillance would eliminate the ability of anyone to spend time certain that they were not being observed, and would thereby deny to everyone what Julie Cohen describes as the "breathing room" necessary for normal human flourishing and "the work of self-making."[70] Such a world would be enormously bland and inhibited: our culture would become less rich as experimentation became more costly,[71] and we would be less informed if we knew all of our interests might be available to the state.[72] Self-censorship in a world like that would be inevitable, especially for behaviors or views that were unpopular or politically out of favor.[73] And many of the positive liberties we cherish (such as free speech and assembly) depend on antecedent opportunities to read, generate hunches, speak with friends, and test out ideas, unobserved.[74] This is all the more true for that speech the First Amendment privileges most:

69. *Cf.* SCHNEIER, *supra* note 13, at 47 ("Imagine that the [U.S.] government passed a law requiring all citizens to carry a tracking device. Such a law would immediately be found unconstitutional. Yet we carry our cell phones everywhere.").

70. Cohen, *supra* note 13, at 1911. Cohen argues that once citizens are subject to "pervasively distributed surveillance," they are vulnerable to shaping and modulation by powerful commercial and political interests—which, in turn, could eliminate the conditions that make liberal democracy possible in the first place. *Id.* at 1912. That is an example of a second-order effect of perfect surveillance, and there are undoubtedly many more that are difficult to forecast.

71. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000) (arguing that the possibility that every "first move or false start" will be monitored will tend to drive people's behavior toward the "bland and the mainstream").

72. If you knew the government might get access to your *entire* Google search history one day, would it affect what you looked for?

73. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 488 (2006) (arguing that pervasive surveillance "can alter the way people engage in their activities" by, for example, "making them less likely to attend political rallies or criticize popular views"). Solove's taxonomy argues generally that "[a]bstract incantations of 'privacy' are not nuanced enough to capture the problems involved" because "privacy violations involve a variety of types of harmful or problematic activities." *Id.* at 480–81; *see also* Laird v. Tatum, 408 U.S. 1, 13 (1972) (discussing the concept of a chilling effect); Solove, *supra* note 50, at 1130.

74. Neil Richards has called this "intellectual privacy." *See generally* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015). Richards argues that before we can speak freely, we must be able to read freely and communicate our nascent ideas in confidence. *Id.* at 11–12; *see also* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 114 (2007) (arguing that "First Amendment activities are implicated by a wide array of law enforcement data-gathering activities").

political speech, critical of the government and of officials we might not want learning we had been grousing about them in frank terms.[75]

These concerns are particularly severe when the party observing us is the government. The government is unique in its ability to aggregate knowledge from many other sources, no one of which paints quite as complete a portrait as all of them together.[76] Aggregated information can be particularly dangerous because we are limited in our ability to remember which bits of information we have given to whom, leading us to make mistakes about how much we have exposed ourselves to the world.[77] Moreover, government surveillance poses unique risks because the government may exercise coercive force over us at any time.[78] In particular, it would unacceptably alter the balance of power in our lives by increasing the risks to us of official misbehavior, both in terms of its likelihood and the harm it could do. All of these harms still occur even if the government does not, in fact, monitor all of its citizens at all times, and they can even become *more* severe,[79] as the uncertainty itself functions as a mechanism of social control.[80]

These harms have been recognized for some time, but what is new for the purposes of this Article is the sheer scope of what technology has enabled the government to learn about us—and thus the magnitude of the threat we are facing. For most of our history, this sort of knowledge has been impossible, and so our legal institutions are not designed to account for its harms.[81] To

75. On the proposition that political speech is at the core of traditional First Amendment protections, see, for example, Republican Party of Minn. v. White, 536 U.S. 765, 774 (2002) (holding that "speech about the qualifications of candidates for public office" is "at the core of our First Amendment freedoms").

76. *See* Solove, *supra* note 73, at 506–11; *see also* FRIEDMAN, *supra* note 13, at 5 ("Policing is just one function of government, and yet it is special. Policing officials are granted remarkable powers. They are allowed to use force on us."). To the extent that this aggregation concern is taken seriously, it would also raise serious issues involving market concentration by network service providers, who could also be expected to aggregate a great deal of information about private people. Antitrust law in the United States has traditionally not regarded such effects as relevant as they do not relate to prices, though there is a re-emerging strain in the antitrust literature, known as "economic structuralism," that questions an exclusive focus on price. *See, e.g.*, Lina M. Khan, Note, *Amazon's Antitrust Paradox*, 126 YALE L.J. 712, 717 (2017).

77. Solove, *supra* note 73, at 507–08. Solove notes that "aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected"—upsetting people's expectations in "unanticipated ways," as we all "give out bits of information in different settings," with at least some expectation that "in each disclosure, [we] are revealing relatively little about [ourselves]." *Id.*

78. *Cf. id.* at 487–88 (noting a quintessentially "modern" kind of problem that involves not immediate insult or harm to a person but a greatly enhanced risk that "a person might be harmed in the future").

79. *Id.* at 495 (discussing harms resulting from situations where "people are generally aware of the *possibility* of surveillance, but are never sure if they are being watched at any particular moment").

80. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH 200 (1977). That was the essence of Jeremy Bentham's proposal for a "*Panopticon*," a prison designed such that any guard *could* see any prisoner at any given moment, but no prisoner could be sure whether he was or was not being watched. *Id.* Bentham really meant it; Foucault's account is less warm.

81. As Justice Alito has observed, "In the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring in the judgment).

monitor even a single person's movements, for example, would once have required vast resources in the physical world—agents, helicopters, cars, and binoculars, all working endlessly.[82] Today it requires a single court order directed to a phone company. The technical and practical constraints on government surveillance are gone—all that remains are legal ones.

We need not agree at this stage on what precisely the state ought not to be able to learn about us. You might be bothered by the idea of a modern-day "pink file,"[83] documenting the sexual orientation of everyone in the country.[84] I might be bothered by a database of people's movements. A third person might object to a government database of our website-reading habits. What precisely is too dangerous to give to the state is a substantive question that will be relevant later, but for now what matters is that we are barreling rapidly toward a world in which the state can learn anything about anyone. If that is a problem, how do we stop it?

II. A PESSIMISTIC VIEW OF EX POST RESISTANCE

But what is the danger? Can't the companies that store so much of our data simply refuse government requests for assistance—*won't* they, surely, in this post-Snowden era? Won't they have powerful allies in courts, staffed by neutral, life-tenured judges skeptical of executive overreach? And won't their combined lobbying powers in Congress, at any rate, ensure that their valuable private-surveillance model is protected at any cost? Alan Rozenshtein argues for something like this view: that network intermediaries have significant practical ability to resist helping the government with law enforcement and surveillance.[85] Rozenshtein calls these actors, in what is perhaps a bit of deck stacking, "surveillance intermediaries."[86] He argues that they are incentivized to resist state demands for aid, and, more importantly, that they will be effective in that resistance.[87] Rozenshtein argues that refusing to voluntarily give up users' information and instead

82. *Id.* (noting that pervasive location surveillance "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," which would only be undertaken in unusual circumstances).

83. *See* Lukasz Szulc, *Operation Hyacinth and Poland's Pink Files*, NOTCHES (Feb. 2, 2016), http://notchesblog.com/2016/02/02/operation-hyacinth-and-polands-pink-files/ [https://perma.cc/P6X7-YNCS].

84. In the 1980s, the Polish security services set out to create a database of all the gay people in Poland. Iwona Zielinska, *Who Is Afraid of Sexual Minorities? Homosexuals, Moral Panic, and the Exercise of Social Control* 4 (Ctr. for Criminological Research, Sheffield Univ., Occasional Paper 1, 2005), https://www.sheffield.ac.uk/polopoly_fs/1.784!/file/Iwona_paper2.pdf [https://perma.cc/R9GA-2NE9]. It was called Operation Hyacinth, and it resulted in the creation of many bureaucratic dossiers. Szulc, *supra* note 83. One leader in a Warsaw gay-rights organization recalls that he was arrested and interrogated, and "the investigators filled in a document entitled 'The Dossier of a Homosexual.'" *Id.* "Above all," he recalls, "they asked for names" of other gay people in Poland, but they also asked about a great deal more (including "preferred types of lovers"). *Id.*

85. Rozenshtein, *supra* note 13, at 122–44.

86. *Id.* Though, in fairness, "the new writs of assistance" is not exactly a study in neutrality, either.

87. *Id.* at 116.

insisting that the government prove some legal entitlement to it will generally hamper the government's efforts in a serious way.[88]

This strategy (collect the information now, resist handing it over later) was prominently on display during Apple's 2016 dispute with the FBI.[89] Apple very publicly refused to build the software that the government wanted.[90] The government sought a court order, and dozens of technology companies rushed to Apple's side.[91] A high-profile showdown on the extent of a company's responsibility to assist the government was averted, however, because the government, without Apple's help, was able to access the data stored on Farook's iPhone, and so dropped its request.[92] Ultimate resolution of the scope of third-party assistance duties was therefore forestalled, but the litigation strategy obviously reflected at least a reasonable assessment of its chances by the network companies involved.

This Part calls for greater skepticism of the prospects for this sort of ex post resistance. The government's hand in such disputes is much stronger than is widely recognized. Current law is incredibly favorable to the new writs of assistance, and the legislature has repeatedly demonstrated its willingness to change the law to ensure that the government gets the help it needs. Even absent specific statutory authorization, courts—relying on our long history of compelled private assistance for law enforcement—generally require aid to the government anyway. And even on those occasions where courts and legislatures have tried to keep information out of the government's hands, the executive has generally been able to get what it wants anyway, by generously interpreting its inherent powers, reading the limits imposed on it narrowly, and avoiding court involvement where possible. This "threat model"[93] illustrates how fragile an ex post resistance strategy really is, and

88. *Id.* at 122–34. Rozenshtein calls this "proceduralism and litigiousness." *Id.* at 122.

89. *See supra* notes 44–46 and accompanying text.

90. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ [https://perma.cc/W9BJ-AL8V]. Cook, the CEO of Apple, explained that iPhone users, including him, store "an incredible amount of personal information, from our private conversations to our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going," and that what the FBI wanted, in Apple's view, was for the company to build "something we simply do not have, and something we consider too dangerous to create": "a backdoor to the iPhone." *Id.*

91. Amicus briefs in support of Apple were filed by (among others) Facebook, Google, Amazon, Kickstarter, Reddit, Twitter, Dropbox, Evernote, Nest, Slack, the ACLU, AT&T, the Electronic Frontier Foundation, Jesse Jackson, and (most august of all) thirty-two law professors. *See* Press Release, Apple, Amicus Briefs in Support of Apple (Mar. 2, 2016), https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple/ [https://perma.cc/H5T4-4C5F].

92. Government's Status Report, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. 16-cm-10 (C.D. Cal. Mar. 28, 2016).

93. *See* Kendra Albert, *Computer Security Tools & Concepts for Lawyers*, 20 GREEN BAG 2D 127, 130 (2017) ("Basically, the idea behind threat modeling is that different risks require different protections. The steps to prevent or mitigate a thief stealing one's laptop to resell it are very different from the steps taken to prevent a litigation opponent from hacking into one's email server. Identifying one's threats is the key towards successful security practices.").

the compelling need to develop something superior to it if we are concerned about the problem outlined in Part I.

A. Legislative Accommodation of Government Aid

This Part argues that the government today enjoys wide-ranging legislative authorizations to get information and assistance from third-party network service providers. When courts have read those authorizations narrowly, legislatures have generally amended them to make clear that the government can get whatever help it needs.

Legislative authorization for "orders of production"[94] is already quite broad. If the government wants a network service provider to give it information it has about a customer, all it generally has to do is ask. The easiest of these tools is a subpoena. The Federal Rules of Criminal Procedure require clerks of court to issue blank subpoenas to prosecutors, which they then fill out themselves;[95] such subpoenas may order the production of any "documents, data, or other objects the subpoena designates."[96] Criminal subpoenas are judged by incredibly loose standards. The government is often deemed to be entitled "to every man's evidence,"[97] and in grand jury proceedings, the object of a subpoena is not even permitted to argue that the information sought is irrelevant.[98] Subpoenas need not be supported by probable cause,[99] and they may be issued on the mere suspicion that the law is being violated, "or even just [to obtain] assurance that it is not."[100] There are only a small number of grounds for resisting a subpoena,[101] none of which are robust enough to deal with the danger we are concerned with here. A claim of privilege is usually not available to a third-party network service provider,[102] and a claim that assembling the records is too burdensome is

94. *See supra* Part I.B.

95. FED. R. CRIM. P. 17(a).

96. *Id.* r. 17(c)(1).

97. United States v. Calandra, 414 U.S. 338, 345 (1974) (quoting Branzburg v. Hayes, 408 U.S. 665, 688 (1972)).

98. *Id.* (noting that the object of a grand jury subpoena is not "entitled to urge objections of incompetency or irrelevancy" or "'challenge the authority of the court or of the grand jury' or 'to set limits to the investigation that the grand jury may conduct'" (quoting Blair v. United States, 250 U.S. 273, 282 (1919))).

99. *In re* Subpoena Duces Tecum, 228 F.3d 341, 348 (4th Cir. 2000) ("Thus, unless subpoenas are warrants, they are limited by the general reasonableness standard of the Fourth Amendment (protecting the people against 'unreasonable searches and seizures'), not by the probable cause requirement.").

100. United States v. Morton Salt Co., 338 U.S. 632, 642–43 (1950); *see also* United States v. R. Enters., Inc., 498 U.S. 292, 297 (1991) (noting that the "function of the grand jury is to inquire into all information that might possibly bear on its investigation until it has identified an offense or has satisfied itself that none has occurred"); *Branzburg*, 408 U.S. at 701 ("A grand jury investigation 'is not fully carried out until every available clue has been run down and all witnesses examined in every proper way to find if a crime has been committed.'" (quoting United States v. Stone, 429 F.2d 138, 140 (2d Cir. 1970))).

101. *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 806 (2005) (enumerating essentially "three grounds for resisting a subpoena: privilege, burdensomeness, and irrelevance" and explaining that none are typically successful).

102. *Id.* at 822–26 (noting that Fourth and Fifth Amendment protections for information held by third parties are "virtually nonexistent"). As Slobogin notes and as this Article argues

"almost always doomed to failure."[103] This low standard is generally justified on the ground that it would be impossible to ever generate probable cause for more intrusive searches and seizures (or formal charges) if investigators could not require the production of information from parties of interest.[104] Even absent a grand jury, the government is authorized to issue administrative subpoenas directly in many contexts, which are judged by similarly loose standards.[105] Most notoriously, Congress has authorized the FBI to issue so-called "national security letters," which order the production of certain information if the government merely certifies it is *relevant* to an ongoing terrorism or intelligence investigation.[106]

With regard to network service providers specifically, Congress has authorized the government to seek production of customer information under the Stored Communications Act (SCA).[107] Enacted as part of the Electronic Communications Privacy Act of 1986[108] and amended several times since,[109] the law authorizes the government to "require the disclosure by a provider of electronic communication service of the *contents* of a wire or electronic communication . . . pursuant to a warrant,"[110] and to "require a provider of

above, the "historical change in this setting has not been in the law, but in the extent to which personal information is now housed with third parties." *Id.* at 826; *see also supra* Part I.

103. 3 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 135 (2d ed. 1999); *see also* Slobogin, *supra* note 101, at 806.

104. *See, e.g.*, Hale v. Henkel, 201 U.S. 43, 70 (1906) ("Of what use would it be for the legislature to declare these [acts] unlawful if the judicial power may close the door of access to every available source of information upon the subject?"); Parks v. FDIC, 65 F.3d 207, 218 (1st Cir. 1995) (Selya, J., dissenting) ("This incipient problem—the need to hitch the horse in front of the cart—is frequently exacerbated because the subpoena power has great significance for most administrative agencies in the conduct of important public business.").

105. *Morton Salt Co.*, 338 U.S. at 643 (noting that when "investigative and accusatory duties are delegated by statute to an administrative body, it, too, may take steps to inform itself as to whether there is probable violation of the law"); *see* United States v. Powell, 379 U.S. 48, 57–58 (1964) (noting that administrative subpoenas need only be founded on a "legitimate purpose"); *see also* Slobogin, *supra* note 101, at 815 (discussing the "move toward the current regime of virtually unlimited subpoena power"). For an example of a statute authorizing administrative subpoenas, see 18 U.S.C. § 3486 (2012); *see also* Doe v. United States, 253 F.3d 256, 262–65 (6th Cir. 2001) (determining what is required under the statute to issue an administrative subpoena).

106. For an overview of the development of national security letters (NSLs), see Andrew E. Nieland, Note, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1201, 1206–13 (2007). Authority for NSLs is codified at 18 U.S.C. § 2709.

107. 18 U.S.C. §§ 2701–2712 (2012). The Act applies to "remote computing service[s]," defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2).

108. Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860–68 (1986) (codified as amended at 18 U.S.C. §§ 2701–2711).

109. For an overview of the Act and how it has changed, see generally Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

110. 18 U.S.C. § 2703(a) (emphasis added). The Act draws a distinction between the contents of a communication stored for more or less than 180 days. *Id.* Some courts have held that this distinction cannot be squared with the Fourth Amendment. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 903 (9th Cir. 2008), *rev'd on other grounds sub nom.* City of Ontario v. Quon, 560 U.S. 746 (2010).

electronic communication service or remote computing service to disclose a record or other information *pertaining to* a subscriber" upon a showing of "reasonable grounds" to believe that the information is "relevant and material" to an ongoing investigation.[111] Anything other than the contents of a communication, in other words, must be produced only upon a showing of relevance to some ongoing investigation.[112]

The government can and does use its power under the SCA to force the disclosure of enormous amounts of sensitive information about the users of network services. An example is the government's showdown with Twitter over WikiLeaks.[113] As part of the investigation into Chelsea Manning's leak of classified information, the government requested an order under the SCA for information about three users, none of whom was Manning.[114] The government wanted "account names and user IDs, all personal addresses, payment information, session times, and IP addresses for devices from which tweets were sent,"[115] all of which could be "intensely revealing."[116] And in the end, the government won.[117]

Current law is also broadly accommodating of "orders of collection." The Communications Assistance for Law Enforcement Act (CALEA) requires any "telecommunications carrier" to "ensure that its equipment, facilities, or services . . . are capable of" being used by "the government, pursuant to a court order or other lawful authorization, to intercept . . . all wire and electronic communications" transmitted by those services.[118] CALEA left "information services" out of its scope,[119] and specifically provided that a service provider had no responsibility for "decrypting, or ensuring the government's ability to decrypt, any communication."[120] But those are statutory affordances that reflected a political compromise in 1994—one many would like to see altered today. Rozenshtein, for example, has suggested that it may be necessary to "demand technological impact assessments before a technology company develops a product or service that disrupts a key government function like effective surveillance."[121] Network service providers of any meaningful size would likely obey such changes if

111. 18 U.S.C. § 2703(c)–(d) (emphasis added).

112. Of course, to the extent that such production would represent a "search" under the Fourth Amendment, the Act could not alter relevant constitutional requirements. In *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *argued*, No. 16-402 (U.S. Nov. 29, 2017), the government sought the disclosure of a subscriber's location records, *id.* at 884. The Supreme Court will soon decide whether or not disclosing that information constitutes a Fourth Amendment "search," and if so, whether a warrant is required. *See* Carpenter v. United States, No. 16-402 (U.S. argued Nov. 29, 2017).

113. For an in-depth discussion of this incident, see FRIEDMAN, *supra* note 13, at 235–38.

114. *Id.* at 236.

115. *Id.*

116. *Id.* (quoting *In re* § 2703(d) Order, 787 F. Supp. 2d 430, 439 (E.D. Va. 2011)).

117. *Id.*

118. 47 U.S.C. § 1002(a) (2012).

119. *Id.* § 1002(b)(2)(A).

120. *Id.* § 1002(b)(3).

121. Rozenshtein, *supra* note 13, at 182.

they were implemented.[122] Federal law also permits court orders requiring the activation of microphones in people's personal devices to listen in on their oral communications.[123] And the Pen Register Act similarly requires the provision of "all information, facilities, and technical assistance necessary to accomplish the installation of the pen register."[124]

Legislatures, moreover, have displayed an enormous willingness to modify the law to ensure that the government can get the assistance it needs for authorized investigations. In the middle of the twentieth century, the U.S. Supreme Court decided two cases that—doctrinally—provided an enormous amount of protection for the users of telephones. Decades earlier, the Court had held in *Olmstead v. United States*[125] that government wiretaps were not "searches" for purposes of the Fourth Amendment because they are accomplished without physical intrusions into the home.[126] But in *Berger v. New York*,[127] the Court changed course, invalidating New York's wiretapping statute on the ground that it did not require an adequate showing by the government before the wiretap was installed.[128] And in *Katz v. United States*,[129] the Court formally overruled *Olmstead*, concluding that "electronically listening to and recording [a person's] words" constituted "a

122. By way of analogy, before the relaxation of export controls on cryptography in the United States, commercial software providers almost universally obeyed such controls. *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 433–41 (2012) (detailing the history of the "crypto wars"). Interestingly, however, even during this period, free software that implemented strong encryption was "widely available on the Internet." *Id.* at 439 & n.48 (discussing PGP—short for "Pretty Good Privacy"). The extent to which pseudo-*samizdat* free software could again preserve a measure of privacy even in a world of strict design limits is an interesting question, but beyond the scope of this Article.

123. 18 U.S.C. § 2518 (2012); *see also* United States v. Oliva, 686 F.3d 1106, 1110–11 (9th Cir. 2012) (discussing 18 U.S.C. § 2518); United States v. Tomero, 462 F. Supp. 2d 565, 568 (S.D.N.Y. 2006) (same).

124. 18 U.S.C. § 3124(a) (2012).

125. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

126. *Id.* at 466. This happened, it is worth noting, over the vigorous objection of the telephone companies—the network intermediaries of their day—who filed a crisp eight-page amicus brief in support of Olmstead. *See generally* Brief in Support of Petitioners' Contention, *Olmstead*, 277 U.S. 438 (Nos. 493, 532, 533). It was the "very nature" of the telephone service to be private, the companies argued, and the "wire tapper destroy[ed] this privacy." *Id.* at 4. Foreshadowing *Kyllo v. United States*, 533 U.S. 27 (2001), the companies even argued that a wiretap must surely count as a search because it invaded a person's home without a warrant: "[h]aving regard to the substance of things," a wiretapper "would not do this more truly if he secreted himself in the home of the citizen." Brief in Support of Petitioners' Contention, *supra*, at 4–5; *cf. Kyllo*, 533 U.S. at 34 (holding that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained" without a physical intrusion is a Fourth Amendment search).

127. 388 U.S. 41 (1967).

128. *Id.* at 57–59. Specifically, the Court objected that New York's statute authorized the "indiscriminate use" of wiretaps: it authorized wiretapping "without requiring belief that any particular offense has been or is being committed" and without requiring the conversations sought to be "particularly described," it permitted long interceptions with indefinite extensions, and it provided neither notice to the target (!) nor any showing of "exigent circumstances" to excuse the requirement of notice. *Id.* at 58–60.

129. 389 U.S. 347 (1967).

'search and seizure' within the meaning of the Fourth Amendment."[130] The effect of *Berger* and *Katz* together was to seriously restrict, on constitutional grounds, the government's ability to intercept telephone calls—an almost total reversal of *Olmstead* and a doctrinal victory for the telephone companies and their users.

But legislatures responded by modifying the law to accommodate the constitutional concerns while still permitting the government to collect the information it wished to have. The day after *Berger* was decided, the Speaker of the New York State Assembly pledged to modify New York's wiretapping laws to comply with *Berger* and ensure that the government could continue to intercept calls.[131] In June 1968, the state did just that, imposing new procedural safeguards that set a low bar (such as naming the person being investigated, the crime of which they were suspected, and the site at which the wiretapping order was to be used).[132] And in June 1968—almost a year to the day after the Court's decision in *Berger*—Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968[133] (the Wiretap Act), which created a warrant system for wiretapping to comply with both *Katz* and *Berger* and to ensure the government could still collect the information it wished.[134]

When court decisions limiting government access to information are based on statutory interpretation rather than constitutional interpretation, a legislature can swiftly act to change the law on which the decision is based, as the events after Title III's enactment illustrate. Title III gave the government the authority to eavesdrop on telephone conversations, at least upon an appropriate showing. But what if it needed help from the phone companies to do it? In 1970, the FBI sought an order authorizing it to listen

130. *Id.* at 353. Katz was charged with transmitting illegal gambling wagers across state lines by using a telephone booth; FBI agents attached a listening device to the outside of the booth, and introduced the recordings at Katz's trial. *Id.* at 348.

131. *See, e.g.*, Sidney E. Zion, *Travia Foresees New Bugging Law: Expects Albany to Provide 'Adequate Safeguards,'* N.Y. TIMES, June 13, 1967, at 25. Zion's article hedges that whether such a statute would be possible was "in doubt," partly because "the majority decision was unclear," *id.*, and partly because Justice Byron White's dissent insisted that the majority's conditions would be "almost impossible to satisfy," *id.* (quoting *Berger*, 388 U.S. at 113 (White, J., dissenting)). Anthony J. Travia, then Speaker of the New York State Assembly, was more optimistic (although admirably candid about his ignorance), telling Zion: "I haven't read the decision yet, but from what I am told it appears to me that they haven't declared eavesdropping and wiretapping unconstitutional per se, just that this particular statute did not provide adequate safeguards." *Id.*

132. *Rockefeller Signs Bill That Permits Police Wiretapping*, N.Y. TIMES, June 12, 1968, at 49. In a signing statement, Governor Rockefeller enthusiastically endorsed electronic surveillance as the "'single most effective' weapon against organized crime." *Id.*

133. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801–804, 82 Stat. 197, 211–225 (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)). The legislation included findings from Congress that "[t]he interception of [wire and oral] communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice." *Id.* § 801(c), 82 Stat. at 211.

134. *Id.* § 802, 82 Stat. at 216 (creating a new statute, 18 U.S.C. § 2516, entitled "Authorization for Interception of Wire or Oral Communications").

in on conversations taking place on a telephone line.[135] The FBI sought a further order requiring the telephone company to give it "facilities, services and assistance" necessary to "effectuate the interception."[136] The government asked for the phone company's "consent" to the entry of the order of assistance, but was refused.[137] The district court denied the government's request, concluding that the Wiretap Act did not authorize such assistance,[138] and the Ninth Circuit affirmed.[139] On appeal, the government invoked "the ancient principle, still recognized and applied, that law enforcement officers may assemble a *posse comitatus*, whereby private citizens may be required to help the police to keep the peace, and to pursue and arrest law violators."[140] But the Ninth Circuit disagreed.[141] The court observed that the Wiretap Act was "extensive," stating "in precise terms" what wiretaps were prohibited and which were permissible, and making "meticulous provision" for the manner of obtaining approval, making use of the information obtained, etc.[142] Given that, and the conceded "total absence of any provision even hinting that the court is to have authority to enter such a unique order as the Government here seeks," the court of appeals concluded that Congress had meant to "limit approved interceptions to those which could be accomplished without the active assistance of the carrier, or at least to those in which that assistance would be forthcoming on a voluntary basis."[143] As for *posse comitatus*, the Ninth Circuit said only that it was "not convinced" that the power "to compel a telephone company to assist in the investigation of suspected law violators" was analogous to the power that law enforcement had "to assemble a *posse comitatus* to keep the peace and to pursue and arrest law violators."[144]

The government was not pleased with this result, however plausible the Ninth Circuit's reconstruction of legislative intent may have been, and Congress's reaction was "immediate."[145] President Nixon signed the District of Columbia Court Reform and Criminal Procedure Act of 1970 on July 29, 1970, just two months after the Ninth Circuit's decision, amending Title III to reverse the outcome of *In re United States*.[146] Section 2518 was amended to require that a phone company furnish the government "all information,

135. *In re* United States, 427 F.2d 639, 640 (9th Cir. 1970).

136. *Id.* For example, the FBI wanted the telephone company to supply "leased lines and connecting wires or bridges." *Id.* at 640 n.1.

137. *Id.* at 640.

138. *Id.* at 640–41.

139. *Id.* at 644.

140. *Id.* at 642.

141. *Id.* at 644.

142. *Id.* at 643. At this point, the Supreme Court's decision in *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), was still a few years in the future. It is a fair question whether the Ninth Circuit's decision could or would have come out the same way had *New York Telephone Co.* already been on the books. Nonetheless, whatever the weaknesses of the Ninth Circuit's decision doctrinally, the legislative response detailed in the text establishes the main point: that victory in the courts may presage legislative defeat.

143. *In re United States*, 427 F.2d at 643–44.

144. *Id.* at 644.

145. United States v. Mountain States Tel. & Tel. Co., 616 F.2d 1122, 1131 (9th Cir. 1980).

146. 427 F.2d 639 (9th Cir. 1970).

facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services" provided.[147] The new provision was enacted with "little debate."[148] Indeed, in the bill itself, this change is simply labeled a "conforming amendment."[149] The result is that the Wiretap Act now commands, in explicit terms, the technical assistance necessary to accomplish the interception of communications "unobtrusively and with a minimum of interference" to the provider's services.[150] The Pen Register Act now contains a similar provision.[151] These requirements are not particularly specific, and do not resolve crucial questions: how much interference with the provider's services is too much? Is there any outer limit on how much technical assistance (or of what sorts) a company would have to provide? Presumably, yes—but the matter is not addressed in the statute itself, which is another way of saying Congress had no interest in spelling out such a limit.

When it comes to the new writs of assistance, the government has already begun to push for legislative solutions to anticipated court-based resistance. That was the upshot of James Comey's 2014 "Going Dark" speech, as discussed earlier[152]: Comey noted that "[o]ur phones and computers have become reflections of our personalities, our interests, and our identities."[153] But he lamented that the government was not "always able to access" this information, which was creating a "significant public safety problem."[154] He called for legislative changes to "keep up with changing technology and to maintain our ability to actually collect the communications" the government was interested in.[155] Specifically, Comey proposed that the network service providers be required to build in "intercept solutions during the design phase"—that is, to ensure that their products could always, in principle, be used for surveillance.[156] Although no such legislation has yet been enacted, the government has continued to press Congress for action: for example, during the FBI's dispute with Apple over the San Bernardino shooting, Comey testified before the House Intelligence Committee that the question of third-party assistance "isn't going to be answered in the courts, and shouldn't be"; rather, it was Congress "that should be determining the

147. Pub. L. No. 91-358, § 211(b), 84 Stat. 473, 654 (1970) (codified as amended at 18 U.S.C. § 2518(4) (2012)). A later amendment also provided that the telephone company was to be "compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance." 18 U.S.C. § 2518(4).

148. H.R. REP. NO. 103-827, at 13 (1994). The 1994 report also confirms that the 1970 amendment was a response to *In re United States*. *Id.*

149. Pub. L. No. 91-358, § 211, 84 Stat. at 654.

150. 18 U.S.C. § 2518(4).

151. *See* 18 U.S.C. § 3124(a)–(b) (2012).

152. *See supra* notes 55–56 and accompanying text.

153. Comey, *supra* note 55.

154. *Id.*

155. *Id.*

156. *Id.*

answers."[157] Comey's prior remarks, of course, left no doubt about what that answer should be: a change in the law to enable greater government surveillance than present doctrine might permit.[158]

In sum, Congress has already afforded the government enormous power to issue and enforce the new writs of assistance and has generally demonstrated its willingness to extend those powers when asked. Of course, many of the new writs of assistance are (after all) new, and so many of them do not have specific statutory authorization. What then? What about when the government wants to get a court to order assistance of a kind that is *not* contemplated by any statute?

B. The Historically Normal Roots of Compelled Third-Party Assistance

Even when it comes to more exotic orders of construction (like the Apple case), or when the government wants orders of collection or production where there may not be specific statutory authority, the Supreme Court has held that the All Writs Act[159] authorizes courts to require third-party assistance as necessary to carry out otherwise-authorized investigations.[160] Such commands may issue only under "appropriate circumstances,"[161] a term the Court has not much elaborated on—observing only that a third party should not be too far removed from the underlying controversy, and that it is best if the assistance is not too burdensome.[162] But from early English law to the present, the government has sought and received both compelled and active assistance from private parties—even when those third parties did not

157. Eric Lichtblau & Nick Wingfield, *F.B.I. Chief Presses Congress to Act on Data Privacy*, N.Y. TIMES (Feb. 25, 2016), https://www.nytimes.com/2016/02/26/technology/fbi-chief-presses-congress-to-act-on-data-privacy.html [https://perma.cc/NLF4-EVUC].

158. Some legislators seemed perfectly happy to indulge the FBI. Representative Jim Sensenbrenner "guarantee[d]" at one hearing that Apple would not "like what comes out of Congress." Roger Cheng, *Apple, FBI Face Off Before Congress over iPhone Encryption*, CNET (Mar. 1, 2016, 3:30 PM), https://www.cnet.com/news/apple-fbi-face-off-before-congress-over-iphone-encryption-san-bernardino-terrorist/ [https://perma.cc/T696-RERW]. Meanwhile, two Senators reportedly developed legislation that would have implemented the FBI's preferred solution. *See* Cory Bennett, *Senate Encryption Bill Draft Mandates 'Technical Assistance*,*'* HILL (Apr. 7, 2016, 10:49 PM), http://thehill.com/policy/cybersecurity/275567-senate-intel-encryption-bill-mandates-technical-assistance [https://perma.cc/J9YH-F9TP].

159. The All Writs Act was enacted by the first Congress as part of the Judiciary Act of 1789. Judiciary Act of 1789, ch. 20, § 14, 1 Stat. 73, 81 (codified as amended at 28 U.S.C. § 1651(a) (2012)). In its original form, it provided that the "courts of the United States, shall have power to issue writs of *scire facias*, *habeas corpus*, and all other writs not specially provided for by statute, which may be necessary for the exercise of their respective jurisdictions, and agreeable to the principles and usages of law." *Id.* § 14, 1 Stat. at 81–82. It is codified today in substantially the same form. *See* 28 U.S.C. § 1651(a).

160. United States v. N.Y. Tel. Co., 434 U.S. 159, 172–74 (1977) (holding that courts may "issue such commands" to third parties "as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued" when those third parties, "though not parties to the original action or engaged in wrongdoing," are in "a position to frustrate the implementation of a court order or the proper administration of justice").

161. *Id.* at 174. This reflects the text of the All Writs Act itself, which requires that whatever writs are issued be "agreeable to the usages and principles of law." 28 U.S.C. § 1651(a).

162. *Cf. N.Y. Tel. Co.*, 434 U.S. at 174–78.

wish to help and even when their reasons for not helping were entirely legitimate. This history is relevant because the All Writs Act and precedent interpreting it are open ended, leaving courts to turn to history as a baseline against which to measure their decisions.[163] The history of the common law is doctrinally relevant,[164] and might be thought especially so when the doctrine itself is unclear or open ended. The fact that it is historically normal for third parties to be required to aid the government is therefore a serious problem for the ex post resistance strategy. This Part explores that history in some detail.

At the time of King Edward I's reign in England, in the thirteenth century, there were no professional police forces;[165] rather, when a felony was committed, what was called the "hue and cry" was to be raised.[166] If an ordinary resident of a town came upon a dead body, he was *required* to raise the hue[167]—and if he did not, he was committing a separate offense, for which he could be fined.[168] The hue would be transmitted from village to village by shouting and horn-blowing until the felon was apprehended.[169] And private people were not just expected to help apprehend criminals—they were required to keep equipment handy for the job.[170] Upon hearing the hue, all were required to come forth with weapons.[171] A 1285 statute required the King's wealthier subjects to keep items such as a "Hauberke, [a Breastplate] of Iron, a Sword, a Knife, and an Horse."[172] In general, the rule was that

163. That is often just what the doctrine requires. As Justice Oliver Wendell Holmes put it, "if a thing has been practised for two hundred years by common consent, it will need a strong case" to challenge it. Jackman v. Rosenbaum Co., 260 U.S. 22, 31 (1922). Of course, Justice Holmes also wrote that it would be "revolting to have no better reason for a rule of law than that so it was laid down in the time of Henry IV." O.W. Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 469 (1897).

164. *See, e.g.*, Pac. Mut. Life Ins. Co. v. Haslip, 499 U.S. 1, 17 (1991); *see also id.* at 24 (Scalia, J., concurring in the judgment) (arguing for the relevance of "the traditional practice of American courts").

165. 2 FREDERICK POLLOCK & FREDERIC WILLIAM MAITLAND, THE HISTORY OF ENGLISH LAW BEFORE THE TIME OF EDWARD I 582 (1898).

166. *Id.* at 578.

167. *Id.* Not only that, of course, but he also would likely "lay[] himself open to ugly suspicions." *Id.* The proper cry seems to have been "Out! Out!" or possibly "Haro" ("Hither"). *Id.* at 578–79 & 579 n.1.

168. *Id.* at 578. Pollock and Maitland describe it as an "amerciable" offense, *id.*, which means one carrying a financial penalty, *see Amerce*, BLACK'S LAW DICTIONARY (10th ed. 2014).

169. POLLOCK & MAITLAND, *supra* note 165, at 579.

170. Babington v. Yellow Taxi Corp., 164 N.E. 726, 727 (N.Y. 1928) (describing how in early English law, men were requested to maintain "instruments sufficient for the task").

171. POLLOCK & MAITLAND, *supra* note 165, at 579 (noting that people were required at the raising of the hue to "turn out with the bows, arrows, [and] knives that they [were] bound to keep").

172. Statute of Winchester 1285, 13 Edw. 1 c. 4–6 (Eng.) (alteration in original). A hauberk is a sort of armor—think Conan the Barbarian. *See, e.g.*, Conan Props., Inc. v. Mattel, Inc., 712 F. Supp. 353, 357 (S.D.N.Y. 1989) (describing Conan's attire as including a "hauberk [of] leather and mail mesh").

"felons ought to be summarily arrested and put in gaol," and all "true men ought to take part in this work and are punishable if they neglect it."[173]

This principle of mandatory public assistance in law enforcement was transmitted to the American colonies and survived into the seventeenth century even as law enforcement started to become more professionalized. In 1641, Massachusetts enacted a law providing that "all Hue & cries shall be duly received and diligently pursued to full effect,"[174] and a few years later, provided that anyone who "wilfully, obstinately or contemptuously refuse[d] or neglect[ed] to assist any Constable" would be fined forty shillings.[175] Connecticut enacted a similar law in 1650.[176] Although these laws differed from their Edwardian antecedents by contemplating the existence of a constabulary (and affording more process to anyone apprehended),[177] the fundamental principle was the same: ordinary people were required to assist with law enforcement when commanded to do so.

The revolutionary-era controversy over the customs writs of assistance also illustrates this principle.[178] In 1767, England directed American admiralty judges to issue writs "to authorize and impower the Officers of his Majesty's Customs" to "enter and go into" any place to "search for and seize prohibited or uncustomed Goods."[179] This was the customs writ of assistance, which got its name from the fact that it ordered a "wide variety of persons to help"—that is, assist—"the customs man make his search."[180] Local officers, yes, but also "all manner of functionaries and private folk

173. POLLOCK & MAITLAND, *supra* note 165, at 582. Note that there was a species of strict liability attached to this process—Pollock and Maitland doubt that "a charge of false imprisonment could have been met by an allegation that there was reasonable cause for suspicion," such that the "ordinary man seems to have been expected to be very active in the pursuit of malefactors and yet to 'act at his peril.'" *Id.* at 582–83.

174. THE BOOK OF THE GENERAL LAWES AND LIBERTYES CONCERNING THE INHABITANTS OF MASSACHUSETTS 13 (1648). For a very good discussion of this early history, to which I am indebted for many of the original sources cited here, see Jon C. Blue, High Noon *Revisited: Commands of Assistance by Peace Officers in the Age of the Fourth Amendment*, 101 YALE L.J. 1475, 1479–82 (1992).

175. THE BOOK OF THE GENERAL LAWES AND LIBERTYES CONCERNING THE INHABITANTS OF MASSACHUSETTS, *supra* note 174, at 13. In order for everyone to know who exactly they had to obey, the law required that every constable carry "a black staffe of five foot long, tipped at the upper end, about five inches with brasse, as a badge of his office, which he shal take with him when he goeth to discharge any part of his office." *Id.*

176. J. HAMMOND TRUMBULL, THE PUBLIC RECORDS OF THE COLONY OF CONNECTICUT 522 (1850); *see also* Blue, *supra* note 174, at 1482.

177. The original hue and cry offered rather "barbaric justice." POLLOCK & MAITLAND, *supra* note 165, at 579. In some "sea-port towns," the criminal might be "tied to a stake below high-water mark and left to drown." *Id.* at 496 n.7. And process was often summary, especially if the felon was caught red-handed. *See id.* at 579–80.

178. *See generally* SMITH, *supra* note 51.

179. *Id.* at 1. "In 1766, the authorities in London concluded that the statutory authority for the use of the writ in the American colonies was inadequate, so Parliament reauthorized use of the writ in the Townshend Act of 1767." Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 566 n.26 (1999) (citing Townshend Act 1767, 7 Geo. 3 c. 46, § 10 (Eng.)).

180. SMITH, *supra* note 51, at 29.

besides."[181] But although the customs writ of assistance caused an enormous controversy, especially in Boston, it was not its third-party assistance requirement that did so. Rather, the objection was to the fact that the writs permitted searches without a showing of individualized suspicion.[182] That is, it was the absence of cause that was a problem, not the fact that it contemplated the assistance of private people. The idea that a private person could be dragooned into law enforcement was normal and by then, centuries old.[183]

The principle of private assistance for the public good was sufficiently embedded in early American society such that it survived even the Revolution, the ratification of the Fourth Amendment, and similar provisions in the constitutions of the new states. An 1813 New York case, *Coyles v. Hurtin*,[184] is illustrative. The sheriff in *Coyles* went to a house with a warrant to arrest several of the occupants but was resisted and outnumbered.[185] The men were "collected in a room above stairs, making a great noise, and threatened to sacrifice any person who should come up."[186] When the sheriff asked the owner of the house to go to the room and convince the men to give themselves up, he replied that he would not do so "for a thousand dollars"; nor would he give "the names of the persons collected in the room up stairs."[187] Instead, the owner of the house welcomed the sheriff to "do his duty," and promised that he would not interfere, but did nothing more.[188] Understandably reluctant to try and apprehend several rowdy laborers on his own, the sheriff ordered the owner of the house (along with three other men) to stand guard while he went to get help, and to "prevent the escape of the men."[189] The men eventually escaped while the sheriff was gone, and the

181. *Id.* As Smith notes, requiring such assistance was "not new," as "[c]ommunal responsibility for maintenance of the public peace went back long before the Norman Conquest" in the eleventh century. *Id.*

182. *See* O.M. Dickerson, *Writs of Assistance as a Cause of the Revolution*, *in* THE ERA OF THE AMERICAN REVOLUTION 40, 43–44 (Richard B. Morris ed., 1939). The customs writ of assistance was also controversial in Boston for other reasons. Charles Paxton, the government official at the center of the Boston writs-of-assistance controversy, was described by Sam Adams as "the most *insincere*, *plausible*, and *insinuating* of mankind." 1 THE WRITINGS OF SAMUEL ADAMS 1764–1769, at 259–64 (Harry Alonzo Cushing ed., 1904); *see also* SMITH, *supra* note 51, at 101 (discussing Adams's remark, as well as Paxton's epithet as "every man's humble servant, but no man's friend," and concluding that there were "few figures in the revolutionary period" who could have had a worse public image).

183. *But see* Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53, 77–78 (1996) (describing this assistance power as having added "a vague and possibly tyrannical new layer of bodily intrusion and unchecked discretion into the system"). It may well seem that way to us. But as the text indicates, this layer of intrusion, tyrannical and vague though it may have been, was not as new as Professor Amar suggests.

184. 10 Johns. 85 (N.Y. Sup. Ct. 1813).

185. *Id.* at 85. The objects of the arrest warrant had apparently "taken refuge" in a house near the evocatively named "*Drowned Lands*" and were "determined to resist, by force, the execution of the warrant." *Id.*

186. *Id.* at 86.

187. *Id.*

188. *Id.*

189. *Id.*

sheriff arrested the owner of the house for not being helpful enough, for which the owner sued the sheriff for assault and battery and false imprisonment.[190] The owner won the lawsuit, but was reversed on appeal,[191] with the reversing court holding that "[e]very man is bound to be aiding and assisting, upon order or summons, in preserving the peace and apprehending offenders, and is punishable, if he refuses."[192]

Coyles is representative of the early American tradition requiring private people to assist the government with law enforcement when commanded.[193] That tradition continued into the nineteenth century where, for example, public regulation of slavery in the American South required even those who did not own slaves to join so-called "slave patrols"—groups charged with enforcing slave laws.[194] These patrols were explicitly modeled on the tradition of "the 'hue and cry' that a constable would bellow in the wake of elusive criminals," and were a direct descendent of "the *posse comitatus*, the bands of men called out in early modern England to chase down and arrest fleeing felons."[195] In 1845, the governor of South Carolina explained to a leading English abolitionist that "[w]ith us, every citizen is concerned in the maintenance of order" among what he called "the lowest class who are our slaves."[196]

Summarizing the doctrine in the early part of the twentieth century, Benjamin Cardozo, then Chief Judge of the New York Court of Appeals, put it this way: "Still, as in the days of Edward I, the citizenry may be called upon to enforce the justice of the State, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand."[197] Even today, most states continue to authorize police officers to demand the assistance of bystanders as they carry out their

190. *Id.* at 85–86.

191. *Id.* at 87, 89.

192. *Id.* at 88.

193. Until the nineteenth century, the power to compel private citizens to assist with enforcement of the law was often thought to be reserved to state and local governments. *See* Gautham Rao, *The Federal* Posse Comitatus *Doctrine: Slavery, Compulsion, and Statecraft in Mid-Nineteenth-Century America*, 26 LAW & HIST. REV. 1, 15–19 (2008). Though the "principle of compulsory service" was "deeply embedded in the fabric of state and local governance," it was "almost altogether lacking at the federal level." *Id.* at 15. As with many features of the federal-state relationship, however, there was a profound alteration in this understanding after the Civil War, which is discussed further below. *See infra* notes 197–215 and accompanying text.

194. SALLY E. HADDEN, SLAVE PATROLS: LAW AND VIOLENCE IN VIRGINIA AND THE CAROLINAS 1–2 (2001).

195. *Id.* at 3; *see also supra* notes 165–73. What made slave patrols distinct in America was their "reliance upon race as a defining feature"; although the patrols included non-slave-owners, they "did not include free blacks," a "singular difference that set slave patrols apart." HADDEN, *supra* note 194, at 2, 4.

196. *Slavery at the South*, 7 DEBOW'S REV. 289, 296 (1849).

197. Babington v. Yellow Taxi Corp., 164 N.E. 726, 727 (N.Y. 1928). Babington was a chauffeur, who was in his car when a police officer "jumped on the running board [of his car] and ordered [him] to chase another car in order to arrest its occupant." *Id.* at 726. Suddenly, another vehicle cut across Babington's path, which caused an accident killing Babington. *Id.*

duties.[198] In New York, it is a crime to unreasonably refuse aid to a police officer in effecting an arrest or preventing the commission of a crime.[199]

In *United States v. New York Telephone Co.*,[200] the Supreme Court considered the government's power to compel assistance in the installation of pen registers, devices attached to a telephone line that recorded numbers dialed.[201] In the 1970s, unlike today, no law explicitly required telephone companies to assist in the installation of such devices.[202] Lower courts had split on the question of whether such assistance was therefore required.[203] In its brief to the Supreme Court, New York Telephone Co. made arguments much like the ones made by network service providers today.[204] "[O]utside of Title III," the company argued, there is "no express statutory authority which provides that unwilling third parties, such as Respondent, may be directed to affirmatively assist law enforcement in effecting a pen register interception."[205] "The most disturbing aspect of the Government's position," the company continued, was its claim that courts "can, without statutory specification, direct orders to private citizens to participate in law enforcement without the extent of such power being spelled out in clearly

198. *See* Blue, *supra* note 174, at 1475 n.2, 1476 n.3 (collecting statutes). Some states authorize the officer to make the command but do not apparently criminalize the refusal; others do, with varying punishments. *Id.*

199. N.Y. PENAL LAW § 195.10 (McKinney 2018). The practice commentary suggests that this is only a crime if it is possible to safely assist, but cites nothing in support of this proposition. *See id.* § 195.10 note (McKinney 2010) (William C. Donnino, Practice Commentary). At any rate, it is difficult to imagine how it could ever be genuinely safe to help a police officer arrest someone.

200. 434 U.S. 159 (1977).

201. *Id.* at 161 & n.1; *see also* United States v. Giordano, 416 U.S. 505, 549 n.1 (1974) (Powell, J., concurring in part and dissenting in part) (noting that such devices do not "involve any monitoring of telephone conversations"); United States v. Focarile, 340 F. Supp. 1033, 1038 n.1 (D. Md. 1972) (describing a pen register as a device that, at least in 1972, "record[ed] on a paper tape dashes equal in number to the number dialed" (quoting United States v. Caplan, 255 F. Supp. 805, 807 (E.D. Mich. 1966))).

202. As discussed at greater length below, for a wiretap, there was an explicit statutory duty to assist. *See supra* notes 225–64, 292 and accompanying text. But a pen register is not a wiretap. *See* 18 U.S.C. § 2510(4) (2012) (defining a wiretap intercept as "the aural or other acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" (emphasis added)). Therefore, the installation of a pen register was not subject to the statute requiring assistance in the "interception of any wire, oral, or electronic communication." *Id.* § 2518(4).

203. The Seventh Circuit found it "more congruent with both reason and Congressional intent to have courts, rather than the telephone company, decide if a pen register should or should not be used," and so thought that the "authority to compel the cooperation of the telephone company [was] in a sense concomitant of the power to authorize the installation of a pen register, for without the former the latter would be worthless." United States v. Ill. Bell Tel. Co., 531 F.2d 809, 814 (7th Cir. 1976). The Second Circuit (in a similar case) concluded that a district court's command of assistance represented an abuse of discretion: absent explicit "Congressional authority, such an order could establish a most undesirable, if not dangerous and unwise, precedent for the authority of federal courts to impress unwilling aid on private third parties." *In re* United States, 538 F.2d 956, 962 (2d Cir. 1976).

204. *See generally* Brief for New York Telephone Co., *N.Y. Tel. Co.*, 434 U.S. 159 (No. 76-835), 1977 WL 189311.

205. *Id.* at 25.

defined statutes."[206] "It is one thing," in other words, "for courts to act to prevent an obstruction of their orders; it is quite another to dragoon unwilling private parties into affirmative participation."[207]

But the phone company lost.[208] It was a close decision—five to four—but in the end, the government proved that it did not need specific statutory authorization to compel private companies to aid it in surveillance.[209] Rather, the assistance order was "clearly authorized by the All Writs Act."[210] In dissent, Justice John Paul Stevens argued that if "the All Writs Act confers authority to order persons to aid the Government in the performance of its duties," then it "provides a sweeping grant of authority entirely without precedent in our Nation's history."[211] But that is just the problem: such dragooned assistance is historically normal, and presents serious doctrinal risks to the ex post resistance strategy to these new writs of assistance.

Today, the government's use of the All Writs Act to compel third-party aid is very common.[212] The government recently disclosed that it has used the Act to order the unlocking of Apple phones alone "at least" seventy times since 2008.[213] That is not to say that this use has gone unquestioned: Magistrate Judge James Orenstein explicitly raised separation-of-powers concerns about the government's use of the Act in a 2016 Brooklyn hearing in a drug case, and eventually ruled against the government.[214] But the broad trend toward government surveillance is quite clear, and it is consistent with the historical evidence laid out above.[215]

To be sure, there are doctrinal limits on the responsibilities of third parties to assist law enforcement—though the present contours of those limits are imprecise and fact dependent. The Supreme Court held in *New York Telephone Co.* that courts may only compel third-party assistance under the All Writs Act in "appropriate circumstances," such as where a third party is not too far "removed from the underlying controversy," and where an order of assistance is not too "burdensome."[216] Similarly vague bounds exist on

206. *Id.* at 34.
207. *Id.*
208. *N.Y. Tel. Co.*, 434 U.S. at 176–78.
209. *Id.*
210. *Id.* at 172.
211. *Id.* at 190 (Stevens, J., dissenting in part).
212. The ACLU has constructed a map detailing modern cases involving the Act and cell phones, and it has counted sixty-three confirmed cases as of 2016. Eliza Sweren-Becker, *This Map Shows How the Apple-FBI Fight Was About Much More Than One Phone*, ACLU (Mar. 30, 2016, 9:00 AM), https://www.aclu.org/blog/speak-freely/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone [https://perma.cc/FAW5-RLU5].
213. Lorenzo Franceschi-Bicchierai, *Feds Say Apple Has Unlocked Suspects' iPhones 'At Least' 70 Times in the Past*, MOTHERBOARD (Oct. 26, 2015, 5:00 PM), https://motherboard.vice.com/en_us/article/4xagvq/feds-say-apple-has-unlocked-suspects-iphones-at-least-70-times-in-the-past [https://perma.cc/V2UW-C3FK].
214. *In re* Apple, Inc., 149 F. Supp. 3d 341, 361–63, 376 (E.D.N.Y. 2016).
215. *See supra* Part I.B.
216. *N.Y. Tel. Co.*, 434 U.S. at 174–75 (majority opinion). The opinion by Justice White is a bit of a hash: it does not say, or attempt to, which of the many "facts of this case" are the crucial ones. For instance, the Court's opinion observes that New York Telephone Co. was a

subpoenas and other means of compelled private assistance. It is therefore plausible to imagine courts sustaining objections to the new writs of assistance (or at least the most radical of them) on doctrinal grounds, and the briefs of network service providers have generally called for exactly that.[217] But such arguments must grapple with the formidable historical precedents discussed above.[218]

Doctrine can also change, which might be appropriate precisely because these new writs of assistance are new: they call for forms of assistance previously unheard of or, at minimum, for the collection of information that has never before existed. In these circumstances, doctrinal change may well be required. The Supreme Court held in *Kyllo v. United States*,[219] for example, that the Fourth Amendment should be construed to ensure at least "that degree of privacy against government that existed when the Fourth Amendment was adopted."[220] Thus, the Fourth Amendment regards as a "search" not just physical intrusions into the home, but even the "obtaining by sense-enhancing technology [of] any information regarding the interior of the home that could not otherwise have been obtained."[221] If the new writs of assistance diminish individual privacy, and current doctrine does not proscribe such diminishment, then one available argument is that cases like *Kyllo* require the current doctrine to change. Doctrinal response and adjustment to technological change is part of American legal doctrine (at least in the Fourth Amendment).[222] And, apart from the technological issues at play in this Article, the general presumption in favor of third-party assistance has also been questioned on doctrinal grounds.[223] At least one scholar has argued that the Constitution should be understood to place important limits on commands of assistance.[224]

"highly regulated public utility with a duty to serve the public." *Id.* Is that important, or simply a helpful atmospheric fact? The Court does not say.

217. *See, e.g.*, Apple, Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant, No. CM-16-10 (E.D. Cal. Feb. 25, 2016), ECF No. 16. This brief argues that the All Writs Act does not confer the authority to compel Apple's assistance, *id.* at 15–19, that *New York Telephone Co.* is not to the contrary, *id.* at 20, and (more esoterically) that compelled assistance in these circumstances would violate the First and Fifth Amendments, *id.* at 32–34.

218. *See supra* Part II.B.

219. 533 U.S. 27 (2001).

220. *Id.* at 34. At issue in *Kyllo* was the use of "a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home." *Id.* at 29. The question presented was whether this was a search of the home under the Fourth Amendment. *Id.* The Court held that it was. *Id.* at 40.

221. *Id.* at 34.

222. It is equally true, though, that the "law, though jealous of individual privacy," has not always "kept pace with . . . advances in scientific knowledge." Berger v. New York, 388 U.S. 41, 49 (1967); *see also* Olmstead v. United States, 277 U.S. 438, 466 (1928) (concluding that government wiretaps were not searches for purposes of the Fourth Amendment because they are accomplished without physically intruding into the home), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

223. *See generally* Blue, *supra* note 174.

224. *Id.* at 1484–86. Judge Jon C. Blue argues that the Fourth Amendment is implicated wherever "an officer by a show of authority 'has in some way restrained the liberty of a

Nonetheless, the doctrinal obstacles for ex post resistance are formidable. Even absent specific legislative authorization, for centuries courts have generally been willing to force third parties to assist the government in law enforcement and surveillance. Therefore, even if the legislature does not act to expand the government's powers, existing doctrine is likely more than enough to help the government learn everything it needs.

C. Executive Circumvention of Surveillance Limitations

Even if legislatures and courts purport to constrain the executive's power to access information stored on networked devices and services, there is still a final danger: that the government may attempt to acquire information from network intermediaries without court approval and in contravention of statutory authority. Historically, this is not in any sense farfetched. This does not necessarily require the government to knowingly break the law in the ordinary sense although there are ample instances where that occurs. What it requires is some combination of (1) a generous view of the government's inherent powers to conduct necessary surveillance; (2) a narrow view of restrictions on those powers; and (3) as much secrecy, and as little court involvement, as possible to ensure that those generous and narrow views are not subject to public or coordinate-branch oversight. This Part details this phenomenon.

At least as far back as Franklin Roosevelt, presidents have asserted the ability to engage in surveillance beyond what courts and legislatures have authorized them to engage in—and even in contravention of their proscriptions. When Roosevelt became president, *Olmstead* was the law of the land, and wiretapping was unregulated for Fourth Amendment purposes. But *Olmstead* had also drawn considerable negative public attention,[225] and almost immediately after it was decided, members of Congress began to introduce legislation to curb wiretapping.[226] Congress first prohibited the

---

citizen.'" *Id.* at 1485 (quoting Terry v. Ohio, 392 U.S. 1, 19 n.16 (1968)). The implications of that rule, Judge Blue argues, are "reasonably clear" for "commands of assistance." *Id.* A person given such a command has been seized for Fourth Amendment purposes, and that seizure must be reasonable—an unlikely proposal when an "attempt by an unarmed civilian to apprehend a suspected criminal" is, in many circumstances, "a form of Russian roulette." *Id.* at 1486.

225. *See* Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 STAN. L. REV. 1023, 1036 (2008). Katyal and Caplan quote a representative *New York Times* editorial: "Prohibition, having bred crimes innumerable, has succeeded in making the Government the instigator, abettor and accomplice of crime. It has now made universal snooping possible." *Id.* (quoting Editorial, *Government Lawbreaking*, N.Y. TIMES, June 6, 1928, at 24). Katyal and Caplan, *supra*, discuss many of the historical materials cited here at greater length, and I commend their account of the Roosevelt-era materials to interested readers.

226. 74 CONG. REC. 3, 2901–02 (1931); *see also* Katyal & Caplan, *supra* note 225, at 1036–37 (briefly detailing some congressional debates on the subject). There was not much need for such legislation initially because the Justice Department insisted that it did not engage in wiretapping—J. Edgar Hoover, at least, publicly insisted as much. 74 CONG. REC. 2901–02 (1931). The head of the Prohibition Bureau at the time, Amos Woodcock, had no such qualms, however; when asked if he engaged in wiretapping, Woodcock said, "We do; and the Supreme Court has approved that practice." WALTER F. MURPHY, WIRETAPPING ON TRIAL: A CASE

use of appropriated funds for wiretaps by the Prohibition Bureau,[227] and soon after, enacted the Communications Act of 1934,[228] which forbade interception of any "interstate or foreign communication by wire or radio."[229] Although the Roosevelt administration argued that the Communications Act did not forbid wiretapping,[230] the Supreme Court rejected that reading by concluding that "the plain words of [section] 605 forbid anyone, unless authorized by the sender, to intercept a telephone message."[231] The government initially complied with the Court's ruling, although not without some reluctance.[232] And after a few more decisions on the Act's scope, then-Attorney General Robert Jackson announced that he understood the Congress and the Supreme Court to have forbidden the practice of wiretapping altogether.[233]

J. Edgar Hoover, then the director of the FBI, strongly disagreed with Jackson's conclusions,[234] and he told President Roosevelt that he "desperately" needed wiretapping authority to engage in surveillance of suspected Nazi spies.[235] Roosevelt then authorized the surveillance in a

---

STUDY IN THE JUDICIAL PROCESS 128 (1965); *see also* Katyal & Caplan, *supra* note 225, at 1036–37 (canvassing this history). Woodcock evidently came to change his mind about wiretapping, or so reported at least one St. Louis newspaper editorial noted in the Congressional Record. 75 CONG. REC. 4733 (1932).

227. Pub. L. No. 72-387, tit. II, 47 Stat. 1371, 1381 (1933). Congress appropriated $8,440,000 in all to the Prohibition Bureau, provided that "no part of this appropriation [would] be used for or in connection with 'wire tapping' to procure evidence of violations of the National Prohibition Act." *Id.* The appropriation also banned the use of these funds for "the purchase of intoxicating liquors which are consumed by the investigator or anyone with him," *id.*, an intriguing proviso that is, unfortunately, well beyond the scope of this Article.

228. Pub. L. No. 73-416, 48 Stat. 1064 (1934) (codified at 47 U.S.C. §§ 151–162 (2012)).

229. *Id.* § 605, 48 Stat. at 1103.

230. JOSEPH E. PERSICO, ROOSEVELT'S SECRET WAR 35 (2001). Katyal and Caplan elliptically criticize this reading as one arrived at "[d]espite the Act's text." *See* Katyal & Caplan, *supra* note 225, at 1038. I am more sympathetic to it, at least as an initial textual matter: the section is titled "Unauthorized *Publication* of Communications," for one thing. § 605, 48 Stat. at 1103 (emphasis added). Nonetheless, the Supreme Court concluded otherwise, *see* Nardone v. United States, 302 U.S. 379, 382–83 (1937), and that is what matters for purposes of the argument here.

231. *Nardone*, 302 U.S. at 382. The case concerned (what else?) bootlegging, specifically, a plan to smuggle about 1600 cases of liquor into the Port of New York. United States v. Nardone, 90 F.2d 630, 630–31 (2d Cir. 1937) (Hand, J.), *rev'd*, 302 U.S. 379. The Supreme Court reasoned that "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty." *Nardone*, 302 U.S. at 383. The Supreme Court weighed in twice more on the scope of the 1934 Act: first, to confirm that the government could not make derivative use of the substance of the recorded calls, Nardone v. United States, 308 U.S. 338, 340 (1939); and second, to hold that the Act banned wiretapping of intrastate, as well as interstate, calls, Weiss v. United States, 308 U.S. 321, 329 (1939).

232. The day after the decision, the *New York Times* quoted anonymous Justice Department officials suggesting that the Court's opinion (when read carefully) did not, in fact, prohibit wiretapping. *High Court Bars Testimony Based on Wire-Tapping*, N.Y. TIMES, Dec. 21, 1937, at 1. The *Times* reported that there was "a question in the minds of some Department of Justice officials whether listening in on telephone conversations was not still permissible." *Id.*

233. *See* CURT GENTRY, J. EDGAR HOOVER: THE MAN AND THE SECRETS 231 (1991).

234. *See id.* (discussing Hoover's leaks to the press about the ways in which Jackson's ban was harming investigations).

235. Katyal & Caplan, *supra* note 225, at 1050 (quoting PERSICO, *supra* note 230, at 35).

memorandum stating that he was "convinced" that the Court's decisions interpreting the 1934 prohibition did not apply "to grave matters involving the defense of the nation,"[236] and accordingly approved wiretaps of "persons suspected of subversive activities against the Government of the United States."[237] Roosevelt phrased his analysis as consistent with Supreme Court precedent, and so retained a fig leaf of legality. The memorandum's analysis was "to put it mildly, weak,"[238] but that did not matter as the memorandum was also secret.[239]

The scope of the wiretapping was not confined, in practice, to the sorts of Nazi saboteur situations that might have been at the forefront of Roosevelt's mind: Jackson admitted that he had authorized it in a case involving a routine domestic kidnapping.[240] Hoover wanted to, and did, spy on labor organizations.[241] One newspaper columnist was suspected of a "most subtle type of espionage activity" against the United States, and wiretapped on that basis.[242] Though the investigation turned up no such evidence, it did reveal that the columnist was engaged in an affair with a young John F. Kennedy, evidence that remained in Hoover's files until his death.[243]

The decades after World War II saw further abuses. From the 1950s to the 1970s, the CIA secretly intercepted, opened, and read postal mail without a warrant (ostensibly to gather foreign intelligence),[244] despite this being

---

236. *Id.* (quoting Memorandum from President Franklin Roosevelt to Attorney Gen. Robert H. Jackson (May 21, 1940) (on file with the Library of Congress, Robert H. Jackson Papers, Box 94, Folder 6)).

237. *Id.* at 1025 (quoting U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 7).

238. *Id.* at 1050.

239. *Id.*; *see also id.* at 1051 ("There was no wiggle room in the Court's opinions, as members of FDR's Administration themselves told Congress when they sought changes to the 1934 Act in the wake of *Nardone I* and *II*. But FDR got away with his legal maneuvering because, after all, his memo was secret.").

240. *To Authorize Wire Tapping: Hearings on H.R. 2266 and H.R. 3099 Before Subcomm. No. 1 of the H. Comm. on the Judiciary*, 77th Cong. 17, 19 (1941) (printing letters from Hon. Robert H. Jackson, United States Attorney General, regarding H.R. 2266 and 3099).

241. FROM THE SECRET FILES OF J. EDGAR HOOVER 187–93 (Athan Theoharis ed., 1991). As Katyal and Caplan note, it is now "quite clear" that surveillance of labor and other affiliated groups took place. Katyal & Caplan, *supra* note 225, at 1058. They included

> wiretaps of organizations and businesses as varied as the NAACP, Kyffhaeuser Bund, and the Revolutionary Workers League. In addition, many unions were surveilled, including the CIO Maritime Committee, CIO Food, Tobacco, Agricultural & Allied Workers of America, International Longshoremen's and Warehousemen's Union (CIO), National Maritime Union, National Negro Labor Council, National Union of Marine Cooks & Stewards, United Electrical Radio & Machine Workers of America, and the United Public Workers of America—CIO.

Id.

242. FROM THE SECRET FILES OF J. EDGAR HOOVER, *supra* note 241, at 15.

243. *Id.* at 15–16; Katyal & Caplan, *supra* note 225, at 1059; *see also* Athan Theoharis, *FBI Wiretapping: A Case Study of Bureaucratic Autonomy*, 107 POL. SCI. Q. 101, 111 (1992) (detailing Roosevelt's somewhat bizarre personal involvement in this particular incident).

244. *See* David Wise, *The CIA Burglar Who Went Rogue*, SMITHSONIAN MAG. (Oct. 2012), http://www.smithsonianmag.com/history/the-cia-burglar-who-went-rogue-36739394/ [https://perma.cc/B4DG-SC8A] ("[T]he CIA screened more than 28 million first-class letters and opened 215,000 of them between 1953 and 1973, even though . . . the Fourth Amendment bars third parties from opening first-class mail without a warrant.").

firmly established as illegal for nearly a century.[245] Just as before, the investigations soon went beyond that purpose, and eventually the CIA began reading mail to or from figures such as Hubert Humphrey, John Steinbeck, and Martin Luther King.[246] Other similar intelligence abuses eventually led to the creation of the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities[247]—popularly known as the "Church Committee," after its chair.[248] Senator Church summarized his fears in a 1975 episode of *Meet the Press*:

> If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know.[249]

Church feared a one-way ratchet: past a certain point, there is a degree of government surveillance that begins to operate on the norms of democracy itself.[250]

More recently, the Bush administration authorized the National Security Agency to intercept communications into and out of the United States when the agency believed that at least one party was a member of Al Qaeda or a related terrorist organization.[251] These interceptions were carried out without

---

245. *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant."); *see also* United States v. Van Leeuwen, 397 U.S. 249, 251 (1970) ("It has long been held that first-class mail such as letters and sealed packages subject to letter postage—as distinguished from newspapers, magazines, pamphlets, and other printed matter—is free from inspection by postal authorities, except in the manner provided by the Fourth Amendment.").

246. MICHAEL HOLZMAN, JAMES JESUS ANGLETON, THE CIA, AND THE CRAFT OF COUNTERINTELLIGENCE 171–72 (2008). The justification for this program was so perverse as to be almost admirable: "precisely because the enemy regarded America's mails as inviolate," inspection of the mail was thought "likely to provide clues to the identities of Soviet agents." *Id.* at 172 (emphasis omitted) (quoting MARK RIEBLING, WEDGE 148 (1994)). The program was justified along the same lines Roosevelt envisioned: surely, "any restrictions on government mail-opening must . . . have read into them an exception that would allow CIA to cover mail in time of secret war." *Id.* (quoting RIEBLING, *supra*, at 148).

247. *See* S. REP. NO. 94-755, at III (1976).

248. *See, e.g.*, *Church Committee Created*, U.S. SENATE, https://www.senate.gov/artandhistory/history/minute/Church_Committee_Created.htm [https://perma.cc/UE2P-5C9P] (last visited Apr. 13, 2018) (describing the creation of the Committee on January 27, 1975).

249. NBCUniversal Archives, *The Intelligence Gathering Debate—www.NBCUniversalArchives.com*, YOUTUBE (Jan. 23, 2014), https://www.youtube.com/watch?v=YAG1N4a84Dk [https://perma.cc/ME7L-FSZH] (showing an excerpt of a *Meet the Press* episode from August 17, 1975).

250. This is also essentially the fear of Professor Cohen. *See* Cohen, *supra* note 13, at 1912 ("Under such conditions, liberal democracy as a form of government is replaced, gradually but surely, by a different form of government that I will call modulated democracy because it relies on a form of surveillance that operates by modulation.").

251. *See generally* OFFICES OF INSPECTORS GEN., REPORT NO. 2009-0013-AS, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM (2009). What exactly to call this program is a politically charged question. The Bush administration referred to it

any court authorization, simply done on the President's say-so.[252] Nor were they authorized by any legislation, instead being reauthorized by the President every forty-five days.[253] The Bush administration officials who implemented this surveillance program did not regard themselves as acting extralegally—just as Roosevelt had not. But, just as with Roosevelt, it is hard to conclude that the bulk interception of telecommunications without a warrant was anything other than a flagrant violation of both judicial doctrine and legislative command—or so the vast majority of commentators, on the left and the right, concluded.[254] Even the program's internal constraints were controversial and prompted near-resignation of nearly the entire senior leadership of the Justice Department.[255]

When Congress legislatively authorized the Bush-era surveillance (consistent, note, with the argument that the legislature is generally a willing partner in government collection of private information), the government interpreted the authority incredibly broadly—again, in secret. Section 702 of the FISA Amendments Act of 2008 authorized electronic surveillance of "persons reasonably believed to be located outside the United States."[256] The executive branch interpreted that authority to permit acquisition of communications about people who were outside the United States, not just to or from them,[257] and of anyone who was not affirmatively known to be inside

---

publicly as the "Terrorist Surveillance Program." *Id.* at 1, 6. The legislation passed in 2008 to address the program refers to it as "the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005." FISA Amendments Act of 2008, Pub. L. No. 110-261, § 301(a)(3), 122 Stat. 2436, 2471 (2008) (codified in scattered sections of 18, 50 U.S.C.). David Addington (a prominent administration lawyer and close aide to Vice President Cheney) apparently referred to it simply as "the president's program." BARTON GELLMAN, ANGLER: THE CHENEY VICE PRESIDENCY 280 (2008).

252. The government acknowledged as much. *See* OFFICES OF INSPECTORS GEN., *supra* note 251, at 6 ("[T]he President and other Administration officials acknowledged that these activities included the interception without a court order."); *see also* James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES (Dec. 21, 2005), http://www.nytimes.com/2005/12/21/politics/spying-program-snared-us-calls.html [https://perma.cc/ST2W-JVP3] (describing the program as one "approved by President Bush to conduct eavesdropping without warrants").

253. OFFICES OF INSPECTORS GEN., *supra* note 251, at 6 ("The Presidential Authorizations were issued at intervals of approximately every 45 days.").

254. *See* John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 567 (2007) ("Fire rained down not only from the left, but also from the right.").

255. *Preserving Prosecutorial Independence: Is the Department of Justice Politicizing the Hiring and Firing of U.S. Attorneys?—Part IV: Hearing of the S. Comm. on the Judiciary*, 110th Cong. 218–21 (2007) (statement of James B. Comey, former Deputy U.S. Attorney General, Department of Justice) (testifying that at least a large segment of the senior leadership of the Department of Justice, including then-FBI Director (Robert Mueller III) and Attorney General (John Ashcroft) had at the time contemplated resigning because the President was not obeying legal restrictions on the program).

256. 50 U.S.C. § 1881a (2012).

257. Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 158 (2015) (describing how the National Security Agency adopted "procedures that allow analysts to acquire information 'about' selectors (that is, communications modes used by targets) or targets, and not merely

the United States—with no duty to investigate whether they were or not.[258] The result was "widespread" interception of communications made by Americans,[259] along with public misrepresentations to the Supreme Court about how the government was implementing the program.[260]

The government might well attempt to get private user data information from network intermediaries absent legislative authorization *or* court order. A cooperative intermediary might gladly go along.[261] But even an uncooperative intermediary might find its cooperation ordered, in secret, without any practical method to challenge it in court, or its user data simply intercepted at some other point on the internet as it is transmitted. This would pose certain technical challenges, the most important of which would be the acquisition of the intermediary's private encryption keys. It is the government's view, however, that it can demand those keys with a subpoena or the Stored Communications Act, which, as discussed above,[262] do not require a warrant or probable cause.[263]

This sort of executive legality risk should be the final nail in the coffin for an ex post resistance strategy. Even if courts protect our data under current law and legislatures back them up, that is no guarantee that a motivated member of the executive branch at whatever level will not simply go and get the information it wants anyway, however it can.

The above summarizes risks. Its pessimistic account is one of what *could* happen if network intermediaries continue to collect large amounts of private

---

communications to or from targets (or selectors employed by targets), or information held by targets themselves").

258. *Id.* (describing the government's "presumption of non-U.S. person status").

259. *See* Hon. Sandra L. Lynch, *Constitutional Integrity: Lessons from the Shadows*, 92 N.Y.U. L. REV. 623, 625 (2017); *see also* Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html [https://perma.cc/QDP5-Z4AE] (noting that "the Justice Department had secretly obtained phone logs for reporters at The Associated Press and Fox News").

260. Lynch, *supra* note 259, at 626 (noting that "the Solicitor General had represented to the [Supreme] Court, believing it to be true, that the government had given notices to criminal defendants where warrantless surveillance had been the source of evidence against them," which was not true).

261. As "far back as World War II," the National Security Agency has "had classified relationships with carefully vetted U.S. companies that assist with essential foreign intelligence-gathering activities." Office of Inspector Gen., Report No. ST-09-0002, Working Draft 28 (2009) (unpublished manuscript), https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf [https://perma.cc/6VMP-LJZ8]. After the September 11 attacks, two telecommunications companies (widely believed to be Verizon and AT&T) "contacted [the] NSA and asked, 'What can we do to help?'" Declan McCullagh, *Surveillance 'Partnership' Between NSA and Telcos Points to AT&T, Verizon*, CNET (June 27, 2013, 2:40 PM), https://www.cnet.com/news/surveillance-partnership-between-nsa-and-telcos-points-to-at-t-verizon/ [https://perma.cc/979H-RPKY].

262. *See supra* Part II.A.

263. *See, e.g.*, United States v. Lavabit, LLC, 749 F.3d 276, 282–83 (4th Cir. 2014) ("[T]he Government obtained a seizure warrant from the district court under the Stored Communications Act . . . . The seizure warrant provided that Lavabit was to turn over '[a]ll information necessary to decrypt communications sent to or from [the target's] Lavabit email account . . . , including encryption keys and SSL keys.'" (third, fourth, and fifth alterations in original) (citation omitted)).

data about private people—the risks we run if we persist on the current path. Of course, these risks might not come to pass. Courts might read the government's existing authority narrowly, legislatures might deny the government any further authority, and the executive might obey those directions. That would be a good result, and there is nothing wrong with pursuing that strategy even while one understands it may fail.

But the risks of error in this situation are not symmetric. If network intermediaries continue to stockpile private data and successfully resist government demands for aid that would be socially harmful, we will enjoy modest but certain benefits: our location will be used by our devices to enhance restaurant recommendations, our in-home always-on speakers will play music at our spoken command, and our search results will be more personalized for us. But if they do not succeed in this strategy, the data will have already been collected and it will be too late to do anything about it—exposing us to stochastic and largely unbounded harms. Nassim Taleb has called this property (benefits that are "small and visible," with side effects that are "potentially severe and invisible") "fragility."[264] Ex post resistance might work, but it is a very fragile strategy.

III. REGULATING PRIVATE SURVEILLANCE

This Part grapples with the possibility that the government might get access to whatever network intermediaries can and do learn about us. Soon, if we are not there already, those intermediaries will know essentially everything. Call this the *panoptic presumption*. If it is accepted, not as a normative argument but a descriptive reality, what would follow?[265]

This Part argues that this state of affairs increases the normative desirability of regulating the information about us that can be collected and retained by network intermediaries. Market forces cannot do the job because the "market for privacy" has a number of well-understood failures—and introducing government surveillance into the mix only magnifies those failures. Instead, personal information should be treated as a potentially harmful asset, the collection and retention of which should be regulated ex ante.

---

264. NASSIM NICHOLAS TALEB, ANTIFRAGILE: THINGS THAT GAIN FROM DISORDER 9–11 (2012).

265. Because of the nature of the argument in Part II, the panoptic presumption is not meant to be taken as a literal prediction that the government will in fact acquire all of the information held by network intermediaries. Different observers might have differing assessments of how strong the presumption should be understood to be based on differing assessments of the likelihood of what this Article calls "legality risk." Whatever one's assessment in this respect, it would scale the need for the recommendations in Part III accordingly—that is, to whatever extent one believes the panoptic presumption is a descriptively accurate consequence of the new writs of assistance, it should follow that the solutions in Part III should be regarded as necessary to the same extent.

A. The Failures in the Market for Privacy

Why not just allow individual people to decide what they share with network intermediaries, and take seriously the privacy consequences of those voluntary choices?[266] After all, as Jerry Kang has noted, one might "reasonably view personal information as a valuable commodity that should be exchanged on the free market."[267] And indeed, Stephanos Bibas has argued that a "contractual approach" to data privacy is the right one, at least in some circumstances.[268]

But a purely individual-choice model will not work because genuine freedom of choice requires information and the power to choose.[269] As to the former, an enormous amount of information about people is gathered without their knowledge, much less their consent.[270] Further, people are quite poor at assessing the harms that may result from even consensual disclosure of their private data—it is hard to assess the harms it will lead to in the future, and "the trivial and incremental character of each loss . . . tends to minimize its ultimate effect."[271] This problem is especially severe when it comes to evaluating secondary and tertiary consumers of personal information.[272] As to the existence of power to choose, as Paul Schwartz has argued, surveillance itself can erode choice: "the more that is known about

266. *Cf.* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). Such a person is said to have "assumed the risk" of disclosure, at least for Fourth Amendment purposes. *Id.* at 744. This "third-party doctrine" enjoys near-universal contempt among criminal procedure scholars. *See, e.g.*, 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(c) (4th ed. 2004) (stating that this doctrine is "dead wrong"); Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1315 (1981); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 564–66 (1990).

267. Kang, *supra* note 13, at 1246. Kang is ultimately skeptical of this model, but he takes it seriously on its own economic-efficiency terms. *Id.* at 1246–48.

268. *See generally* Steven A. Bibas, Note, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591 (1994). Kang also surveys some of the other literature making this point. *See* Kang, *supra* note 13, at 1247 n.234 (citing Scott Shorr, Note, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756, 1818–46 (1995); Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM, Sept. 1996, at 92).

269. Cohen, *supra* note 71, at 1396 (noting that free choice requires "accurate information about choices and their consequences" as well as "enough power—in terms of wealth, numbers, or control over resources—to have choices").

270. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON 33 (2004); Kang, *supra* note 13, at 1199 ("The very technology that makes cyberspace possible also makes detailed, cumulative, *invisible* observation of our selves possible." (emphasis added)).

271. Cohen, *supra* note 71, at 1398; *see also* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COMM. 395, 492 (1996) ("[A]s long as in each individual transaction the cost of not providing the information is disproportionate to the loss (which is a function of the cumulation of the transactions, not any single transaction), a property rights approach appears unlikely to have much real influence on database creation.").

272. Cohen, *supra* note 71, at 1396–97.

an individual, the easier it is to force his obedience."[273] And even fully informed and autonomous individuals have less power over the collection of information about them than they think.[274] Companies are generally free, under American law, to collect information about people with whom they have no contractual relationship, and use it for their own purposes.[275]

That is the standard answer—but the argument in Part II suggests a further one. Even if individuals can master the privacy consequences of surrendering their private information to companies, there are unique challenges to the "consent" model when that private disclosure may result in government surveillance. Government surveillance is often conducted in secret and outside the ordinary court system;[276] even when it is done as part of criminal law enforcement, the user may have no way to know that his or her information is being demanded or that it has been turned over. Indeed, the user may not even have standing to object to the third party's disclosure of his or her information to the government.[277] How is a person supposed to meaningfully "consent" to a regime like that? If we must "consent" to the possibility of secret government surveillance to use any network service, then that consent in and of itself creates the harms described in Part I: an uncertainty about whether we are ever being watched, and the accompanying self-censorship and lack of breathing space for ordinary human flourishing.

For related reasons, it is not feasible to expect ordinary market competition to solve the problems identified in Parts I and II. To be sure, conscientious network service providers could voluntarily choose to learn less about their users.[278] Some companies do choose to gather as little user data as they can,

---

273. Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995); *see also* Kang, *supra* note 13, at 1216.

274. In 2009, for example, the Office of the Privacy Commissioner of Canada released a formal report about complaints that Facebook had violated Canada's data-privacy laws. *See generally* ELIZABETH DENHAM, REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) AGAINST FACEBOOK INC. UNDER THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (2009), https://www.priv.gc.ca/media/1033/2009_008_0716_e.pdf [https://perma.cc/X4HN-R8FC]. A substantial portion of those complaints were about the collection of information from non-Facebook users. *Id.* at 70–77.

275. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 7 (2013). For example, users cannot "untag" themselves from photos unless they join Facebook. DENHAM, *supra* note 274, at 70. Facebook, for its part, regards the only issue as one of copyright and stated to investigators that "the reproduction rights for a photograph or video generally belong to the person who took it," and the "responsibility for obtaining the consent of non-users rests not with Facebook, but rather with the users who upload non-users' personal information." *Id.* at 72.

276. Glenn Greenwald, Opinion, *FISA Court Oversight: A Look Inside a Secret and Empty Process*, GUARDIAN (June 18, 2013, 7:36 PM), https://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy [https://perma.cc/E87B-HRFF].

277. One district court has accepted this conclusion in the WikiLeaks case involving Twitter user information. *See In re* United States, 830 F. Supp. 2d 114, 129, 138 (E.D. Va. 2011); *In re* § 2703(d) Order, 787 F. Supp. 2d 430, 436 (E.D. Va. 2011); *see also supra* notes 113–16 and accompanying text.

278. This is part of what Maciej Ceglowski—an entrepreneur and frequent speaker on technology policy—has advocated for. Maciej Ceglowski, *Haunted by Data*, IDLE WORDS,

or at least less than their competitors do.[279] But there are serious limits to this good-intentions model of network-intermediary behavior. For one thing, network service providers must build their products in compliance with applicable law, which may restrict their design decisions. Rozenshtein argues that it may be necessary to "demand technological impact assessments before a technology company develops a product or service that disrupts a key government function like effective surveillance."[280] Whatever the merits of such proposals or their feasibility, it would be necessary for network service providers of any meaningful size to obey them if they were implemented.[281]

More to the point, many network intermediaries have built their businesses on collecting private user data. Knowing things about people is valuable, at least potentially. It is of no use to tell a digital-advertising network that it should learn less about the people who see its ads: that information is their asset. So for as long as collecting such user data remains legal and valuable, companies that decline to do so will operate at a relative competitive disadvantage to those that do not.[282]

B. Information as a Toxic Asset

A better solution is to recognize that personal information, for all its value to the companies that gather it, also has harmful side effects. It is, as Schneier puts it, a potentially "toxic asset."[283] The question is what to do about it. The

---

http://idlewords.com/talks/haunted_by_data.htm [https://perma.cc/XR9S-43Y7] (last visited Apr. 13, 2018). "If you can get away with it," he argues, "don't collect it," and "if you have to collect it, don't store it!" ("You can get a lot of mileage out of ephemeral data.") And if you "have to store it, don't keep it," at least not "forever." *Id.*

279. At present, the most prominent example is Apple, which often boasts about how little information it collects about its customers. *See, e.g.*, Matthew Panzarino, *Apple's Tim Cook Delivers Blistering Speech on Encryption, Privacy*, TECHCRUNCH (June 2, 2015), https://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/ [https://perma.cc/WD9M-UMB2] (noting Apple CEO Tim Cook's assertion in a speech that while "some of the most prominent and successful companies have built their businesses by lulling their customers into complacency about their personal information" while "gobbling up everything they can learn about you and trying to monetize it," he was of the view that this was "wrong").

280. Rozenshtein, *supra* note 13, at 182.

281. By way of analogy, before the relaxation of export controls on cryptography in the United States, commercial software providers almost universally obeyed such controls. *See* Swire & Ahmad, *supra* note 122, at 437–39 (detailing the history of the "crypto wars" and export controls). Interestingly, however, even during this period, free software that implemented strong encryption was "widely available on the Internet." *Id.* at 439 & n.48 (discussing PGP—short for "Pretty Good Privacy").

282. For this reason, Apple's privacy stance has been criticized by market analysts who would like to see the company collect far more information about its users than it currently does. *See, e.g.*, Eric Jackson, *Apple Has to Get over Its Privacy Hang-Ups and Launch Better Services*, CNBC (June 28, 2017, 2:14 PM), http://www.cnbc.com/2017/06/28/apple-has-to-get-over-its-privacy-hang-ups-commentary.html [https://perma.cc/8X9P-8T42].

283. *See also* Bruce Schneier, *Data Is a Toxic Asset, so Why Not Throw It out?*, CNN (Mar. 1, 2016, 12:12 PM), http://edition.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html [https://perma.cc/44LE-5BME] ("Data is a toxic asset. We need to start thinking about it as such, and treat it as we would any other source of toxicity. To do anything else is to risk our security and privacy."). I am not the first to employ an

widespread collection of private data, which in turn enables government surveillance, is not something individual people can easily avoid. It is also caused by the instrumentally rational decisions of businesses. Yet it threatens serious social harm. That is a classic sort of market failure—an environmental externality. In his classic article "The Tragedy of the Commons," Garrett Hardin analogized the problem of pollution to the decisions facing self-interested herdsmen grazing their flock on an open pasture.[284] Just as each herdsman asks only about "the utility *to me* of adding one more animal to my herd,"[285] so too must each network intermediary only ask about the value to themselves of collecting, storing, and retaining the marginal bit of user data. Just as a rational herdsman will therefore tend to "add another animal to his herd" ("[a]nd another; and another"),[286] so too will intermediaries tend to stockpile data that may be of commercial use to them. The grazing of animals, to be clear, is socially useful, just as collecting information is—but grazing also produces social harm, just as the collection of information does. The problem is that the herdsman does not bear that harm personally, just as network intermediaries are not the ones who are principally harmed by the enhanced potential for surveillance. In the face of these mismatched incentives, we must, as Hardin advocates, avoid the looming tragedy by legislating not prohibition but "temperance."[287]

This Part lays out a framework for what temperance might look like. In the context of environmental law, Lewis Kornhauser and Richard Revesz have argued that a regulatory regime for toxic materials must decide both the "volume of hazardous wastes" that will be produced and when (and how) to "dispose of the wastes."[288] Similarly, here, an ex ante regulatory regime for network intermediaries must decide both what intermediaries may learn about us and how long they may retain that knowledge. This Part argues that such a framework solves, as a side effect, data breaches by both private parties and foreign governments—problems that on some accounts are even

---

environmental analogy for data collection in a general sense, but the existing scholarly literature has not developed the concept in detail, and has not focused on the problem of surveillance. Dennis Hirsch has argued in favor of "emissions fees" for commercial email to fight the environmental problem of spam but does not discuss the problem of surveillance. Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 40–41 (2006). Ira Rubenstein (citing Hirsch at points) uses the concept to explore the subject of "privacy self-regulation," but again does not discuss surveillance. *See generally* Ira S. Rubenstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S 355 (2010). This gap in the literature is due to a failure to account for the argument developed in Part II: if no firm line can be drawn between industry and government data collection in the long run, then a primary harm of industrial data collection will continue to be that it enables government surveillance.

284. Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243, 1244 (1968) (explaining that such arrangements "may work reasonably satisfactorily for centuries" but eventually "comes the day of reckoning," when "the inherent logic of the commons remorselessly generates tragedy").

285. *Id.*

286. *Id.*

287. *Id.* at 1245–46.

288. Lewis A. Kornhauser & Richard L. Revesz, *Regulation of Hazardous Wastes*, *in* 3 NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 238, 238–39 (Peter Newman ed., 1998).

more serious than surveillance. In part for that reason, this framework may be more politically feasible than direct regulation of the government's authority to command information and aid; at a minimum, it faces a different set of political challenges, such that it may prove to be a more realistic solution.

1. Regulating the Collection and Storage of Information

Conceptually, for any information that is conceivably collected about people, the law must answer two related questions: When is it legal to gather that information? And once it is gathered, how long may it be retained? Under American law at present, the answer to those questions (with very minor exceptions) is that anything may be gathered by anyone and kept forever. This Part argues that this response is implausibly extreme, and that our present laissez-faire approach is, in fact, the root cause of the surveillance problem this Article describes. Rules about collection and retention should vary according to the type of data at issue and the intermediary that proposes to gather it.

Before beginning this discussion in earnest, two notes on terminology. When I describe the collection of data, I mean data that is acquired by the network intermediary "in the clear"—that is, in a form that can be understood and used by the network intermediary itself. This is in contrast to an intermediary that collects information only in an encrypted form, such that its contents remain accessible to the user, or others on the user's demand, but not to the network intermediary itself. In the latter circumstance, the network intermediary does not actually have access to information in a form that is of concern. Moreover, when I speak of disposing of or destroying data, I am aware that depending on how that disposal is accomplished, forensic techniques may be available that can still recover it.[289] My intent is to bracket that issue, and assume that to the extent law requires data to be disposed of, it is done in a manner that makes it nonrecoverable for practical purposes.

The United States currently has no general regulatory framework for the gathering of personal information about users of networked services and devices. There are no rules that "collectively address the acquisition, storage, transmission, use and disclosure of personal information within the business community."[290] Not even informal "standards" really exist to limit the

289. See, for example, *Commonwealth v. Copenhefer*, 587 A.2d 1353 (Pa. 1991), in which the police recovered a draft ransom note from the defendant's home computer after he attempted to delete it. For further discussion, see Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503, 516 (2001) (discussing *Copenhefer*). Depending on the resources one is willing to invest in the problem, some truly exotic techniques are available, including the use of magnetic force microscopes and Bayesian statistical approaches, although the efficacy of these techniques is (at present) limited. *See generally* Craig Wright, Dave Kleiman & Shyaam Sundhar, *Overwriting Hard Drive Data: The Great Wiping Controversy*, *in* INFORMATION SYSTEMS SECURITY: 4TH INTERNATIONAL CONFERENCE, HYDERABAD, INDIA, DECEMBER 16–20, 2008 PROCEEDINGS 243–57 (R. Sekar & Arun K. Pujari eds., 2008).

290. Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 208 (1992).

"collection and utilization of personal data in cyberspace."[291] The Wiretap Act specifically permits an "officer, employee, or agent of a provider of wire or electronic communication service" to intercept and use communications of its users in the ordinary course of providing services.[292] Moreover, as Patricia Bellia has observed, American law says "little" about data retention, and much of what it does say "provides incentives for indefinite data retention."[293]

There are a few scattered exceptions. The rule implementing the Children's Online Privacy Protection Act, for example, restricts the collection of photographs of children under thirteen.[294] The Video Privacy Protection Act requires destruction of personally identifiable information "as soon as practicable, but no later than one year from the date the information is no longer necessary."[295] Similarly, the Cable Communications Policy Act of 1984 provides that cable operators "shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected."[296] But as Bellia observes, even these isolated and "sector-specific exceptions" are weak: they require "destruction of data only when the data is no longer 'necessary,' and they leave the question of necessity entirely within the data collector's discretion."[297]

As to some classes of data, the optimal solution might be to simply forbid intermediaries (or at least some intermediaries) from collecting it. This might be especially appropriate for what Paul Ohm calls "sensitive information."[298] The European Union's Data Processing Directive, for example, has a distinctive set of rules for how information about "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . data concerning health or sex life" is collected.[299] This sort of information is generally singled out for protection because of its unique ability to harm people when it falls into the wrong hands.[300] At least under some circumstances, the government might be the wrong hands—a potential "adversary," to use Ohm's term.[301] For example, in December 2016, many engineers working at technology firms signed a pledge saying

291. Schwartz, *supra* note 13, at 1611. This regulatory vacuum is no accident but the result of a "multi-year effort" by American companies to convince the government that "we don't need regulations on data collection." SCHNEIER, *supra* note 13, at 197. The potential political economy problems that industry might pose are addressed at greater length *infra*. *See infra* Part III.B.2.

292. 18 U.S.C. § 2511(2)(a) (2012).

293. Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 138 (2008).

294. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2018). Section 1303 of the Act prohibits collecting "personal information from a child" except in accordance with its procedures, which generally require parental consent. 15 U.S.C. § 6502(a)–(b) (2012).

295. 18 U.S.C. § 2710(e) (2012).

296. 47 U.S.C. § 551(e) (2012).

297. Bellia, *supra* note 293, at 151–52.

298. *See generally* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2015).

299. Council Directive 95/46, art. 8, 1995 O.J. (L 281) 31, 40 (EC).

300. Ohm, *supra* note 298, at 1161 ("Information is deemed sensitive if adversaries (to use the computer scientific term) can use it to cause harm to data subjects or related people.").

301. *Id.*

that they would "refuse to participate in the creation of databases of identifying information for the United States government to target individuals based on race, religion, or national origin."[302] Those engineers also pledged to advocate within their organizations "to minimize the collection and retention of data that would facilitate ethnic or religious targeting[,] to scale back existing datasets with unnecessary racial, ethnic, and national origin data[, and] to responsibly destroy high-risk datasets and backups."[303] Gathering this sort of information, they feared, might facilitate impermissible targeting of vulnerable populations by a hostile government that came wielding the new writs of assistance.[304]

The law should restrict the collection of less-sensitive information, like location data, to certain sorts of network service providers. A mobile phone service must collect location information because the customer has to communicate with radio towers to use the service, and which ones the customer uses will necessarily reveal the user's location.[305] More simply, a service designed to offer driving directions has to know where you are for it to do its job. But in other instances, location information is gathered simply to target advertisements,[306] or sell it to someone else, as was the case with a third-party flashlight app that gathered users' location information when used.[307] While restricting the collection of semisensitive information still provides the government with some targets to collect it from, it would at least reduce the scale of the problem.

The law must also provide an answer to *how long* information we give to intermediaries may be retained. Other than "indefinitely," there are two kinds of answers to that question, both of which might be appropriate for some types of data. One answer is "until a user asks that it be removed." Evocatively, this concept is sometimes called the "right to be forgotten."[308] Such "rights" depend on user initiative: that is, you've got to ask.[309] There have been legitimate concerns raised about this "right" under American law,

---

302. Matt Day, *Amazon, Microsoft Workers Sign 'Never Again' Pledge to Oppose Trump's Call for Muslim Registry*, SEATTLE TIMES (Dec. 15, 2016, 3:45 PM), https://www.seattletimes.com/business/microsoft/never-again-pledge-draws-tech-workers-who-vow-not-to-help-build-possible-registry/ [https://perma.cc/6KF3-CA5S].

303. *Our Pledge*, NEVERAGAIN.TECH, http://neveragain.tech [https://perma.cc/KB2C-FDJP] (last visited Apr. 13, 2018).

304. *See id.*

305. *See* Samuel, *supra* note 10, at 1327–28 (describing how this aspect of cellular phone service can be used to infer someone's location).

306. *See* Gordon C. Bruner II & Anand Kumar, *Attitude Toward Location-Based Advertising*, J. INTERACTIVE ADVERT., July 2013, at 3–5.

307. Robert McMillan, *The Hidden Privacy Threat of . . . Flashlight Apps?*, WIRED (Oct. 20, 2014, 6:30 AM), https://www.wired.com/2014/10/iphone-apps/ [https://perma.cc/2CP9-73PF]. Another flashlight app, "Brightest Flashlight Free," was fined by the FTC for deceiving its users about how their location information would be used. Press Release, FTC, Android Flashlight App Developer Settles FTC Charges It Deceived Customers (Dec. 5, 2013), https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived [https://perma.cc/KN5W-YGEX].

308. *See generally* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN (2016).

309. *Id.* at 27–54 (detailing a large number of requests to Google to remove information about private people).

especially to the extent it has been applied to limit the dissemination of public records.[310] But the new writs of assistance suggest that at least a modest on-demand disposal regime is necessary as a safety valve, in the event of expanded government surveillance authority. When Congress or the courts make new information available to the government, they generally do so retroactively—that is, the government gets access to information that already exists, not just information that is created or collected after that moment.[311] Information must therefore be shared with network service providers without knowing, in advance, what the government's ability to get it will be. When the government acquires new authority to get information or assistance from network service providers, it should be possible to remove the information we have stored about us if that new authority changes the calculus of what we are willing to share. Imagine being a member of a minority religion and witnessing the election of a hostile government in your home country. Imagine further that the new hostile government successfully persuaded the legislature or the courts to empower it to get assistance from social networks like Facebook in identifying members of your sect for what it claimed were "national security reasons." In this situation, you would want to have a right to insist that Facebook delete your religious affiliation from its records. This right to insist that networks delete the information that might identify you would be consistent with what you would have shared in the first place had you known what was going to happen.

The problem with on-demand disposal is that it replicates many of the market failures that prompt the need for regulation in the first place. People do not always know who has collected information about them, especially when the collection has been done indirectly (by purchasing or otherwise acquiring it from the entities that directly observed and collected the information), and so people will not always know who to ask for deletion. Therefore, the law can and should require the *automatic* disposal of private information by network intermediaries in more circumstances than it does now by requiring the disposal of some information after a *time certain*, rather than upon user demand. The justification for such a system is conceptually similar to the one for statutes of limitation and repose: the peace that comes from knowing, after a certain period, that the events of the past will not come

310. *See, e.g.*, Martin v. Hearst, 777 F.3d 546, 551 (2d Cir. 2015) (concluding that a Connecticut statute "does not render historically accurate news accounts of an arrest tortious merely because the defendant is later deemed as a matter of legal fiction never to have been arrested"); Alison Frankel, *No 'Right to Be Forgotten' Even If Record Is Expunged: 2nd Circuit*, REUTERS (Jan. 28, 2015), http://blogs.reuters.com/alison-frankel/2015/01/28/no-right-to-be-forgotten-even-if-record-is-expunged-2nd-circuit/ [https://perma.cc/7AMT-LFAB].

311. For example, in 2001, Congress expanded the FBI's authority to issue NSLs in the USA PATRIOT Act, such that the FBI could issue them in "circumstances roughly comparable to those in which a federal prosecutor could obtain a grand jury subpoena." Nieland, *supra* note 106, at 1202; *see also* Doe v. Ashcroft, 334 F. Supp. 2d 471, 482–84 (S.D.N.Y. 2004) (noting the attempt to "harmonize" NSL practice with prosecutors' power using grand jury subpoenas). But nothing in the legislation restricted this new pseudosubpoena power to obtaining information that was given to network service providers *after* the effective date of the Act.

to radically disturb your present circumstances.[312] By analogy, a person should know that after a certain amount of time has passed, the government cannot drudge up certain types of old information about them. Consider location information: an automatic disposal rule for location information would permit a person to be sure after (say) ninety days that his or her visit to an abortion clinic, labor union hall, or temple would no longer be retained. However, automatic disposal cannot and should not be universal—sometimes indefinite storage is precisely what we want, as is the case with many users wanting their emails or photos retained indefinitely in the cloud by their provider so they do not have to personally attend to backing them up locally. In that circumstance, storing the information indefinitely but using a collection restriction, such as keeping the information in an encrypted format, is a superior solution.

Decisions about the generation and disposal of information interact because, as Michael Froomkin has observed, the way in which the law regulates data retention will also affect incentives for data collection.[313] To the extent that information is more useful or valuable when it can be retained for longer, permitting its indefinite retention will tend to encourage more collection at the front end. By contrast, if information must generally be deleted after a short time or after certain conditions are met, thereby rendering it less valuable, less of it may be collected in the first place. For this and other reasons, determining and implementing details of a framework like this one would no doubt be complex. Whatever body is charged with doing so (a new expert agency, for example) would need to make determinations about what types of information were sensitive and should be regulated, what types of intermediaries should be permitted to collect what sort of information, and what time limits make sense for the retention of that which would be gathered. While this Article does not propose to resolve every detail with this framework, if accepted, it would at least supply the right questions. *What* should network intermediaries be able to learn about us? *Which* intermediaries? And for *how long*? At the moment, we are not asking those questions at all—and so we are having the answers implicitly supplied by the commercial logic of businesses especially the advertising-technology industry. It may be that our present regulatory vacuum on these questions is socially optimal, although I doubt it. But even a conscious decision to leave things as they are would be superior to the present state of affairs.

2. Considerations of Political Economy

One possible objection to the above might go: If the government wants this information, what incentive would it have to adopt the sorts of regulations this Article describes? If my descriptive claims about the

312. *See* Holmes, *supra* note 163, at 477 ("A thing which you have enjoyed and used as your own for a long time, whether property or an opinion, takes root in your being and cannot be torn away without your resenting the act and trying to defend yourself, however you came by it. The law can ask no better justification than the deepest instincts of man.").

313. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1542–43 (2000) ("Rules about data retention and use will shape what is collected and how it is done.").

government's likely motivations and behavior in Part II are correct, what chance does this proposal have? Eric Posner and Adrian Vermeule call this problem the "inside/outside fallacy."[314] This problem occurs, they argue, when "the analyst is combining ideal with nonideal theory in an incoherent way, positing nonideal motivations for purposes of diagnosis and then positing idealized motivations for purposes of prescription."[315] In the welfare-economics literature, this is known as the "determinacy paradox"[316]—an analyst must account not only for "what solution a benevolent social planner would desire to institute,"[317] but also for "who will have the incentives to supply that solution, *given* the analyst's diagnosis of the problem."[318]

Upon closer examination, however, regulating network intermediaries actually enjoys certain advantages on this dimension over the "collect and resist" strategy described skeptically in Part II. Whenever the first order cause of the harm is the government, proposals for reform typically must grapple with the inside/outside fallacy. The usual way in which this is done is by positing the hypothetical presence of different motivations for the judiciary or legislatures than for the executive, and arguing for constraining the problematic behaviors via legislation or court action.[319] That is internally coherent, but, as I argue in Part II, when it comes to this particular issue, judges and legislatures are typically part of the problem, and at any rate may be limited in their ability to practically constrain the executive. So if the actors in the U.S. legal system as a whole are systemically favorable to government demands for information and aid, any workable solution must come with an explanation for how it can overcome that systemic characteristic, rather than simply wishing it did not exist. Regulation of data collection and retention enjoys a few advantages along this dimension, at least when compared to attempts to regulate the government's authority to demand assistance.

First, treating surveillance as a harm created by the stockpiling of information and then proposing to regulate the stockpile mitigates other

---

314. Eric A. Posner & Adrian Vermeule, *Inside or Outside the System?*, 80 U. CHI. L. REV. 1743, 1745–47 (2013).

315. *Id.* at 1744.

316. *See* Jagdish N. Bhagwati, Richard A. Brecher & T.N. Srinivasan, *DUP Activities and Economic Theory*, *in* NEOCLASSICAL POLITICAL ECONOMY: THE ANALYSIS OF RENT-SEEKING AND DUP ACTIVITIES 17 (David C. Colander ed., 1984).

317. Posner & Vermeule, *supra* note 314, at 1746.

318. *Id.* at 1747; *see also* James E. Fleming, *Toward a More Democratic Congress?*, 89 B.U. L. REV. 629, 639–40 (2009) (negatively assessing proposals for congressional improvement that require legislative approval); Mark Tushnet, *Some Skepticism About Normative Constitutional Advice*, 49 WM. & MARY L. REV. 1473, 1474 (2008) (arguing that advice about constitutional design must account for the "political considerations" of the relevant actors).

319. *See, e.g.*, Bellia, *supra* note 293, at 167. Professor Bellia notes that "there are strong arguments for favoring stable application of certain key constitutional and quasi-constitutional baselines in surveillance law" and suggests ways that "we might translate those baselines for a world of increasingly perfect memory." *Id.* She posits a doctrinal, court-based solution to the problem she identifies.

harms created by that stockpiling.[320] One of those harms is theft: if network intermediaries stored less private information, they would be less likely to have it stolen, either by insiders or outside hackers.[321] As Bruce Schneier observed, data theft is a serious problem: "Every week, thieves break into networks and steal data about people, often tens of millions at a time."[322] Such thefts can be used to commit identity fraud.[323] The data may also be used to commit blackmail—consider the 2015 theft of identifying information from Ashley Madison, a website designed to help married people have affairs.[324] Beyond private thefts, network intermediaries with large stockpiles of information are also an attractive target for foreign adversaries. In March 2016, John Podesta—then the chairman of Hillary Clinton's presidential campaign—had his email compromised in a data breach that was linked to the Russian government.[325] Those emails, going back years, were subsequently published during the waning days of a presidential election in ways that deeply troubled U.S. intelligence services.[326] Regulations that would reduce these problems in addition to reducing the government's own

320. The dynamic is similar, at a high level of generality, to James Tobin's proposal for a tax on cross-border currency transactions. *See generally* James Tobin, *A Proposal for International Monetary Reform*, 4 E. ECON. J. 153 (1978). Tobin's aim was to cushion exchange rate fluctuations by imposing very small taxes on exchanges of one currency to another, which had the side effect of generating revenue for the government. *Id.* at 155. That side effect has, consequently, often served as the *principal* justification for "Tobin taxes" of various sorts. *See, e.g.*, Kelsey Snell, *Sanders Goes Robin Hood with Plan to Make Wall Street Pay for College*, WASH. POST (Jan. 26, 2016), https://www.washingtonpost.com/news/powerpost/wp/2016/01/26/sanders-goes-robin-hood-with-plan-to-make-wall-street-pay-for-college [https://perma.cc/4BWS-UHCD] (noting Bernie Sanders's proposal of a "tax on speculation" to help eliminate tuition at public colleges and universities).

321. As Ed Felten observed, there is no technical difference between a court order to turn over data and an "inside attack" of a malicious kind:

> From a purely technological standpoint, these two scenarios are exactly the same: an employee copies user data and gives it to an outside party. Only two things are different: the employee's motivation, and the destination of the data after it leaves the company. Neither of these differences is visible to the company's technology—it can't read the employee's mind to learn the motivation, and it can't tell where the data will go once it has been extracted from the company's system. Technical measures that prevent one access scenario will unavoidably prevent the other one.

Ed Felten, *A Court Order Is an Insider Attack*, FREEDOM TO TINKER (Oct. 15, 2013), https://freedom-to-tinker.com/2013/10/15/a-court-order-is-an-insider-attack/ [https://perma.cc/E8PY-TY6P].

322. Schneier, *supra* note 283.

323. *Id.*

324. *See* Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ [https://perma.cc/5B6D-REU9] (discussing hackers' release of Ashley Madison customer information online in an attempt to blackmail the website's owner to take down the site as well as a similar sister site).

325. Lorenzo Franceschi-Bicchierai, *How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts*, MOTHERBOARD (Oct. 20, 2016, 9:30 AM), https://motherboard.vice.com/en_us/article/mg7xjb/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts [https://perma.cc/4EC6-AX9L].

326. Greg Miller & Adam Entous, *Declassified Report Says Putin "Ordered" Effort to Undermine Faith in U.S. Election and Help Trump*, WASH. POST (Jan. 6, 2017), https://www.washingtonpost.com/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html [https://perma.cc/3Z9S-PRJT].

capacity for surveillance might be politically viable in a way that a proposal that only reduced the government's powers would not.[327]

In addition, network service providers often operate in more than one jurisdiction and so are subject to regulation by multiple governments, some of which might have different views on surveillance policy, which might be able to change an intermediary's behavior worldwide. Facebook reports that it had over two billion monthly active users at the end of 2017,[328] meaning not just the majority but the vast majority of its users were outside the United States.[329] And the European Union's new General Data Protection Regulation contains requirements consistent with much of what this Article suggests above,[330] including on-demand deletion and limitations on data collection.[331] The Regulation will require affected companies—everyone doing business in the EU—to update the user interface of their software to offer the required options to EU users, respond to personal data-export and data-deletion requests, develop audit and compliance reporting tools, and so on.[332] Once that work is done, the costs of offering it to Americans is significantly decreased, and companies may find it impossible as a practical matter not to do so. Facebook's implementation of "hard delete on user accounts," the ability of users to delete their account permanently, was similarly done to comply with EU rules.[333] But because of Facebook's internal data architecture, it was necessary to make the feature available to all users.[334]

The major political economy downside to a proposed regulation on industry is the industry. As noted above,[335] there is a reason U.S. law treats this industry the way it does: it is a major force in American politics, and distinctively so, because the major network intermediaries are American companies. The same could be said of every industry that has ever been regulated,[336] so this objection is not necessarily fatal. But it is a drawback to

327. Moreover, ex ante regulation of network intermediaries takes place outside the exigencies that might be generated by a given moment—the Apple-FBI dispute, for example, had to be litigated in the immediate wake of a terrible, violent attack. *See supra* notes 44–46, 89–92 and accompanying text.

328. *Company Info*, FACEBOOK NEWSROOM, https://newsroom.fb.com/company-info/ [https://perma.cc/9293-B54D] (last visited Apr. 13, 2018).

329. *U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/popclock/ [https://perma.cc/7AMN-B5DB] (last visited Apr. 13, 2018) (noting that the population of the United States is just over 327 million).

330. *See supra* Part III.B.1.

331. *See GDPR Key Changes*, EUGDPR.ORG, http://www.eugdpr.org/key-changes.html [https://perma.cc/9S45-LZ3S] (last visited Apr. 13, 2018).

332. *See* Dean Alvarez, *The Impact of GDPR Outside the EU*, IT SECURITY GURU (Jan. 30, 2017), http://www.itsecurityguru.org/2017/01/30/impact-gdpr-outside-eu/ [https://perma.cc/L64D-KQHW].

333. *Notes from an Emergency*, IDLE WORDS, http://idlewords.com/talks/notes_from_an_emergency.htm [https://perma.cc/F8F8-P5WE] (last visited Apr. 13, 2018).

334. *See id.* ("That feature was added with a lot of grumbling, but because of the way Facebook organizes its data, they had to make it work the same for all users. So a European regulation led to a victory for privacy worldwide.").

335. *See supra* notes 85–88 and accompanying text.

336. For example, Rozenshtein, in the service of a different point, optimistically notes that "[a] century ago our society was one of railroads," that network service providers might be

the framework worth taking seriously: in addition to solving more problems, the proposal would also have more opponents, and perhaps not in a way that would provide a net advantage. But to the extent one is skeptical about the feasibility of directly regulating the government's powers to demand assistance, the mix of affected interests is at least different from what this Article proposes, which might make its viability a hypothesis worth disproving.

CONCLUSION

We tend to think of surveillance as a problem created by the government, and thus one to be solved by further regulation of the government itself. This Article argues for a different view. We are experiencing a surveillance problem that is, in fact, downstream from a more general problem: too much data is being collected about us by private companies and retained for too long. That enables too much surveillance, yes—but nothing about the government has changed. The government wants to solve crimes, gather intelligence, and learn whatever it can in service of what it perceives to be its legitimate ends. Our law is structured to accommodate that goal, and it is hard to imagine that it would not be. What has changed is that there are now private entities that collectively aim to know every detail of our lives, from cradle to grave. They have the technology to gather it, they have the space to store it, and they have built businesses on getting it.

The general dynamic goes well beyond surveillance. The rise of a new class of incredibly powerful firms that dominate an important sector of the modern economy, and the ways in which they interact with the government and the public sphere, raises difficult questions about the structure of society in the future. For better or worse, we are used to Leviathan—our law and our norms have grown up understanding the awesome power of the state. What we have not yet come to grips with is the new power of these network intermediaries and what we are to do about them. The first step, this Article argues, is to decide what we will let them know and remember about us. But that will not be the last.

---

thought of as "the railroad companies of the twenty-first century," and that, in the end, "[t]he railroads ultimately lost their independence." Rozenshtein, *supra* note 13, at 188.