Stanford Law Review

Volume 70 January 2018

ARTICLE

Surveillance Intermediaries

Alan Z. Rozenshtein*

Abstract. Apple's high-profile 2016 fight with the FBI, in which the company challenged a court order commanding it to help unlock the iPhone of one of the San Bernardino terrorists, exemplifies how central the question of regulating government surveillance has become in U.S. politics and law. But scholarly attempts to answer this question have suffered from a serious omission. Scholars have ignored how government surveillance is checked by *surveillance intermediaries*: companies like Apple, Google, and Facebook that dominate digital communications and data storage and on whose cooperation government surveillance relies. This Article fills this gap in the scholarly literature, providing the first comprehensive analysis of how surveillance intermediaries constrain the *surveillance executive*: the law enforcement and foreign-intelligence agencies that conduct surveillance. In so doing, it enhances our conceptual understanding of, and thus our ability to improve, the institutional design of government surveillance.

Surveillance intermediaries have financial and ideological incentives to resist government requests for user data. Their techniques of resistance are *proceduralism* and *litigiousness* that reject voluntary cooperation in favor of minimal compliance and aggressive litigation; *technological unilateralism*, in which companies design products and services to make surveillance harder; and *policy mobilization* that rallies legislative and public opinion against government surveillance. Surveillance intermediaries also enhance the *surveillance separation of powers*: They make the surveillance executive more subject to interbranch

* Visiting Assistant Professor of Law, University of Minnesota Law School. At the time this article was written and accepted for publication, I was serving as an attorney advisor in the Office of Law and Policy, National Security Division, U.S. Department of Justice. All statements of fact, opinion, or analysis expressed are mine alone and do not necessarily reflect the official positions or views of the Department of Justice or any other U.S. government agency. This Article has been reviewed by the Department of Justice to prevent the disclosure of classified or otherwise sensitive information. For helpful comments I thank Aditya Bamzai, Zachary Clopton, Jennifer Daskal, Stephanie Davidson, Ashley Deeks, Mieke Eoyang, Jack Goldsmith, Shane Harris, Aziz Huq, Orin Kerr, Adam Klein, Betsy Kuhn, David Kris, Joshua Matz, Jon Michaels, Hannah Neprash, David Pozen, Austin Raynor, Daphna Renan, Shalev Roisman, Paul Rosenzweig, Rachel Sachs, Margo Schlanger, Peter Swire, Matthew Waxman, Benjamin Wittes, Andrew Woods, and participants at the Technology Giants, Sovereign Power, and Surveillance conference organized by the Hoover Institution's National Security, Technology, and Law Working Group. I also thank the editors of the *Stanford Law Review* for their excellent editorial work.

constraints from Congress and the courts and to intrabranch constraints from economic and foreign relations agencies as well as from the surveillance executive's own surveillance-limiting components.

The normative implications of this descriptive account are important and crosscutting. Surveillance intermediaries can both improve and worsen the *surveillance frontier*: the set of tradeoffs between public safety, privacy, and economic growth from which we choose surveillance policy. They enhance *surveillance self-government*—the democratic supervision over surveillance policy—when they mobilize public opinion and strengthen the surveillance separation of powers. But they undermine it when their unilateral technological changes prevent the government from exercising its lawful surveillance authorities.

Table of Contents

Introduction

On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik attacked a suburban office park in San Bernardino, California.[1] Swearing allegiance to the so-called Islamic State, they murdered fourteen people and injured more than twenty before dying in a police shootout.[2] It was the deadliest act of terrorism on U.S. soil since 9/11.[3]

The Federal Bureau of Investigation (FBI) recovered Farook's iPhone but couldn't access it; the phone was locked and ran a version of iOS (Apple's operating system) that the company had recently hardened against third-party access, including access by Apple itself.[4] When the FBI served Apple with a court order to disable some of the iPhone's security features,[5] the company refused, arguing that the government lacked the necessary legal authority and that the order would harm its users' security and impose "unreasonabl[e] burden[s]" on Apple.[6] Apple CEO Tim Cook posted an open letter on his company's website, condemning the attacks but criticizing the FBI's request as "undermin[ing] the very freedoms and liberty our government is meant to protect."[7] Through months of litigation, and despite not contesting that it had the technical means to comply with the government's order, Apple refused to help unlock the iPhone.[8]

---

1. Jennifer Medina et al., *San Bernardino Suspects Left Trail of Clues, but No Clear Motive*, N.Y. TIMES (Dec. 3, 2015), https://perma.cc/KQ97-JT52.

2. *Id.*; Michael S. Schmidt & Richard Pérez-Peña, *F.B.I. Treating San Bernardino Attack as Terrorism Case*, N.Y. TIMES (Dec. 4, 2015), https://perma.cc/HH79-Z52Z.

3. That record stood for a depressingly short time. Six months later, another shooter inspired by the Islamic State attacked a gay nightclub in Orlando, Florida, killing forty-nine people. *See* Lizette Alvarez & Richard Pérez-Peña, *Orlando Gunman Attacks Gay Nightclub, Leaving 50 Dead*, N.Y. TIMES (June 12, 2016), https://perma.cc/Z79X-ZD9N.

4. *See* Memorandum of Points and Authorities at 1-4, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016), 2016 WL 680288.

5. *In re Search of an Apple iPhone*, 2016 WL 618401.

6. Apple Inc's [sic] Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 20, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. 5:16-cm-00010-SP (C.D. Cal. Feb. 25, 2016) [hereinafter Apple's Motion to Vacate].

7. *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://perma.cc/UTL9-VFLH.

8. *See* Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), https://perma.cc/89AG-2PGY; Cook, *supra* note 7. In the end, the FBI purchased a third-party tool that allowed it to access the iPhone. *See* Mark Berman & Matt Zapotosky, *The FBI Paid More Than $1 Million to Crack the San Bernardino iPhone*, WASH. POST (Apr. 21, 2016), https://perma.cc/J4WT-3QRL; *see also infra* note 164 and accompanying text.

How could a consumer electronics company beat the government in a high-profile national security investigation? And why did almost half of Americans take its side?[9] After all, this wasn't a secret investigation by a rogue agent into a minor offense. A federal judge issued a court order for the government to search an undeniably relevant piece of evidence: a phone used by a known terrorist. Imagine if a telephone company had so publicly resisted a similar request after 9/11 or at the height of the Cold War, arguing that its customers expected it to do "everything in [its] power to protect their personal information,"[10] including by keeping that information from federal agents bearing court orders. The result would likely have been congressional denunciations, consumer boycotts, and a hasty surrender.

Apple's surprise victory was striking for another reason: It flew in the face of the conventional wisdom about government surveillance in the digital age. Scholars have long worried about a handful of giant companies dominating digital communications, in part because they fear that such centralization would increase the government's ability to conduct electronic surveillance, which in turn would erode accountability and civil liberties.[11] Scholars have argued that the government can more easily control a few large companies than a sea of users and small providers[12] and that such companies have good reasons to cooperate with the government: to comply with the law,[13] feel good about helping the government fight threats to public safety and national

9. *See, e.g.*, *CBS News Poll: Americans Split on Unlocking San Bernardino Shooter's iPhone*, CBS NEWS (Mar. 18, 2016, 8:24 PM), https://perma.cc/AAU3-TAFY ("In a CBS News/New York Times poll, 50 percent of the more than 1,000 people surveyed said Apple should unlock the phone, though nearly as many, 45 percent, think it should not.").

10. *See* Cook, *supra* note 7.

11. *See, e.g.*, JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 117-18 (2008); Nancy S. Kim & D.A. Jeremy Telman, *Internet Giants as Quasi-governmental Actors and the Limits of Contractual Consent*, 80 MO. L. REV. 723, 762-63 (2015).

12. *See, e.g.*, Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2298 (2014); *see also* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 252 (2010) (noting that "[w]ith everyone in the country now connected," fewer parties "need to be persuaded to cooperate" with government surveillance); Balkin, *supra*, at 2304 ("Individuals who disseminate content that the state wants to control may be anonymous or pseudonymous, or located beyond the reach of territorial governments. Therefore states increasingly target digital infrastructure, not only because most people are speaking through it, but also because targeting infrastructure is the easiest method of control.").

13. *See* LAWRENCE LESSIG, CODE: VERSION 2.0, at 71 (2006) ("But as code writing becomes commercial—as it becomes the product of a smaller number of large companies—the government's ability to regulate it increases. The more money there is at stake, the less inclined business (and their backers) are to bear the costs of promoting an ideology."); Balkin, *supra* note 12, at 2299.

security,[14] curry favor with regulators,[15] or sell data and services to law enforcement and foreign-intelligence agencies.[16] These scholars have suggested that because so many technology companies profit from collecting user data, they naturally undervalue their users' privacy and thus too readily cooperate with government surveillance.[17] And they've lamented privacy law's impotence to check these dynamics. On the statutory side, the government skirts legal constraints through informal public-private partnerships.[18] And on the constitutional side, the third-party doctrine strips Fourth Amendment protections from the "digital dossiers" that companies create out of user data.[19]

To these scholars, the years since 9/11 have been a boom time for the "surveillance-industrial Internet complex"[20] and a dark one for privacy and civil liberties. They point to the "handshake agreements"[21] by which telecoms like AT&T and Verizon abetted the U.S. government's warrantless surveillance program, a program whose shaky legal foundations became a defining constitutional scandal of the War on Terror.[22] In the wake of the 2013 Snowden disclosures, they point to Silicon Valley allowing the government to

14. *Cf.* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 927-28 (2008).

15. *See* Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105, 143-44 (2016); Michaels, *supra* note 14, at 936-37 (discussing "regulatory corruption" (capitalization altered)).

16. *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1100 (2002).

17. *See* Michaels, *supra* note 14, at 937-38.

18. *See id.* at 932-35.

19. *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 102-10 (2011); Kim & Telman, *supra* note 11, at 763-64. The third-party doctrine, first fully articulated by the Supreme Court in *Smith v. Maryland*, holds that "a person has no legitimate expectation of privacy," and thus no Fourth Amendment rights, "in information he voluntarily turns over to third parties." 442 U.S. 735, 742-44 (1979). There are signs, however, that at least some Justices of the Court are willing to revisit the doctrine. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."); *see also* Transcript of Oral Argument, Carpenter v. United States, No. 16-402 (U.S. Nov. 29, 2017) (debating the third-party doctrine in the context of cell site location information).

20. *See* Christian Fuchs, Commentary, *Surveillance and Critical Theory*, MEDIA & COMM., Sept. 30, 2015, at 6, 7.

21. *See* Michaels, *supra* note 14, at 904.

22. *See* CHARLIE SAVAGE, POWER WARS: INSIDE OBAMA'S POST-9/11 PRESIDENCY 175-76 (2015); *see also* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://perma.cc/WU4Z-4RE6.

stockpile emails, messages, and browser records,[23] and they argue that the secrecy surrounding government surveillance leads technology companies to acquiesce to "regime[s] of automatic compliance."[24] They criticize the courts for crippling the Fourth Amendment through the third-party doctrine and miserly standing rights, thereby forcing us to accept Silicon Valley as our "corporate avatars," even though the technology industry has neither the will nor the means to effectively challenge government snooping.[25] And they worry about what's to come, sometimes in dystopian terms. For example, Bernard Harcourt rejects the distinction between government and corporate surveillance as one without a difference.[26] Instead he conjures a nightmarish vision of our new reality: a "large oligopolistic octopus"[27] that transcends the public-private divide and threatens our freedom with its "tenticular oligarchy."[28]

How do we reconcile the conventional wisdom with recent history? How do we account for Apple's victory, and should we treat it as a one-off exception or as a sign of things to come? The answer, as this Article tries to show, is that the conventional wisdom is incomplete and must adapt to a new reality. Although the digital age has broadened the horizons of government surveillance, it has also imposed constraints on account of its political economy: the technological, commercial, political, and cultural arrangement of our digital infrastructure. By entrusting our data processing and communications to a handful of giant technology companies, we've created a new generation of *surveillance intermediaries*: large, powerful companies that stand between the government and our data and, in the process, help constrain government surveillance. Far from an anomaly, the fight over the San Bernardino iPhone previews the likely new normal: a contentious relationship between the companies that manage our digital bodies and the government that protects our physical ones. Surveillance intermediaries like Apple (and Google and Facebook and Microsoft) have the incentives and means to meaningfully constrain government surveillance. They do so both by their own lights and by subjecting government surveillance to greater checks from within the government itself.

---

23. *See, e.g.*, LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 54-55 (2016).

24. Hannah Bloch-Wehba, *Process Without Procedure: National Security Letters and First Amendment Rights*, 49 SUFFOLK U. L. REV. 367, 379 (2016).

25. *See* Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441, 1444-45, 1458 (2015).

26. *See* BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 79 (2015).

27. *Id.*

28. *See id.* at 188.

Although commentators have begun to recognize that technology companies might constrain government surveillance,[29] they have not systematically investigated this possibility. As Samuel Rascoff observes in the context of foreign intelligence (though the observation applies equally to domestic law enforcement): "A critically important—and thus far, largely unheralded (at least by scholars)—feature of the new intelligence oversight ecosystem is the role of American technology and telecommunications firms."[30] By setting forth a comprehensive analysis of the incentives, activities, and effects of surveillance intermediaries, this Article tries to fill that gap.

This gap is important to fill because we can't accurately analyze government surveillance without a proper model of how surveillance intermediaries constrain, not just enable, government surveillance. We need such a model to constructively advance many of the highest-profile debates in electronic privacy and cybersecurity, including end-to-end encryption and other technical impediments to law enforcement investigations;[31] offshore data storage and cross-border data access;[32] privacy protections for the Internet of

29. *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 207-10 (2015); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 600 (2009) ("The prospect of resistance from the legal teams of third-party record holders often creates a substantial deterrence against government overreaching even when the third-party doctrine does not."); Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 662-65 (2016) (noting that technology companies have expressed opposition to certain forms of government surveillance and have even engaged in "commercial 'self-help,' employing default encryption technologies on mobile devices and explicitly marketing them as being impervious to government snooping"); Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1127 n.401 (2016) ("The implications of the Snowden disclosures for [communications and technology] companies appear significant, and these companies are coalescing into an engaged voice in the politics of surveillance.").

30. Rascoff, *supra* note 29, at 662.

31. *Compare, e.g.*, Geoffrey S. Corn, Essay, *Averting the Inherent Dangers of "Going Dark": Why Congress Must Require a Locked Front Door to Encrypted Data*, 72 WASH. & LEE L. REV. 1433, 1437 (2015) ("[T]o protect the interests of society, Congress should compel any manufacturer or distributor of communications and storage technologies that offer[s] encryption as part of any product [it] sell[s] or distribute[s] in the United States to build in a mechanism allowing for lawful government surveillance and searches of the data stored or transmitted over those devices or services."), *with, e.g.*, HAROLD ABELSON ET AL., MIT COMPUT. SCI. & ARTIFICIAL INTELLIGENCE LAB., MIT-CSAIL-TR-2015-026, KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS 1 (2015), https://perma.cc/7FFQ-BHBY ("[P]roposals [for government access to encrypted systems] are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm.").

32. *See* Jennifer Daskal, *The Un-territoriality of Data*, 125 YALE L.J. 326, 389-97 (2015); Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 739-51 (2016). For a discussion of surveillance intermediaries as stakeholders in reforming the system

footnote continued on next page

Things;[33] and the future of electronic foreign intelligence surveillance.[34] If we don't accurately trace the behavior of surveillance intermediaries, including both the positive and negative consequences of that behavior, our policy may fail to accomplish the desired results, or even backfire.

An accurate model of surveillance intermediaries can also contribute to the ongoing scholarly debate over what sort of institutional design—"not simply what the limits on communications surveillance should be, but who should set them"[35]—will best promote *surveillance governance*: the regulation and oversight of government surveillance. The "new administrativist[s]"[36]—part of the broader movement to apply institutional design principles to the criminal justice system[37]—have applied the lessons of administrative law to surveillance governance,[38] recognizing the importance of focusing on oversight of

of cross-border law enforcement data access, see Peter Swire & Justin Hemmings, *Stakeholders in Reform of the Global System for Mutual Legal Assistance* 10-13 (Ga. Tech Scheller Coll. of Bus., Working Paper No. 2015-32, 2015), https://perma.cc/P9QH-JUD5.

33. *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 808 (2016) ("[A] Fourth Amendment built on old-fashioned 'effects' can address a new world in which things are no longer just inactive, static objects, but objects that create and communicate data with other things.").

34. At the end of 2017, shortly before this Article went to print, section 702 of the Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1813 (2015)); *see also* FISA Amendments Act of 2008, Pub. L. No. 110-261, sec. 101, § 702, 122 Stat. 2436, 2438-48 (codified as amended at 50 U.S.C. § 1881a), was set to expire. *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, § 2, 126 Stat. 1631, 1631 (codified at 18 U.S.C. § 2511 (2016), 50 U.S.C. §§ 1801, 1881a-1881g). In the run-up to the reauthorization debate, commentators split over whether section 702 should be reauthorized as is or with minimal changes, *see, e.g.*, Chris Inglis & Jeff Kosseff, *In Defense of FAA Section 702: An Examination of Its Justification, Operational Employment, and Legal Underpinnings* 2 (Hoover Inst., Aegis Paper No. 1604, 2016), https://perma.cc/TPX5-EJMJ (arguing that Congress should reauthorize section 702 "without any significant changes to the statute"), or whether reauthorization instead presented a valuable opportunity for reform, *see* DONOHUE, *supra* note 23, at 136-60 (urging substantial limitations to section 702).

35. *See* Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 295 (2011).

36. Andrew Manuel Crespo, *Systemic Facts: Toward Institutional Awareness in Criminal Courts*, 129 HARV. L. REV. 2049, 2059 (2016) (capitalization altered).

37. *See, e.g.*, Rachel E. Barkow, *Institutional Design and the Policing of Prosecutors: Lessons from Administrative Law*, 61 STAN. L. REV. 869, 873 (2009) (arguing that "by heeding lessons of institutional design from administrative law, . . . federal prosecutors' offices could be designed to curb abuses of power"); *see also* Renan, *supra* note 29, at 1048 n.29 (collecting sources).

38. *See* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1872, 1893 (2015) (arguing that courts could "ensure democratic accountability of policing . . . by barring practices that were not authorized either by a legislative body in sufficiently clear terms or through administrative rulemaking"); Renan, *supra* note 29, at 1043 (arguing for the need to "integrate administrative governance with the law and theory of the Fourth Amendment"); Christopher Slobogin, *Panvasive Surveillance,*

footnote continued on next page

surveillance programs rather than individual activities.[39] Other scholars, drawing on a tradition favoring increased presidential control over the federal bureaucracy,[40] advocate a "presidential intelligence" that would give the White House more control over foreign surveillance.[41] Still others, focusing on law enforcement, urge a renewed emphasis on judicial oversight.[42] Whichever of these approaches (or combinations of approaches) is correct, we must first understand how surveillance intermediaries constrain government surveillance—both directly and by augmenting the ability of other government actors to check the executive branch's surveillance activities. Only then can we make informed choices about how best to design our institutions.

More broadly, scholars increasingly recognize that to fully understand the separation of powers we must look to factors beyond the internal structure of the government. As Rascoff notes, "The Madisonian insight that individual rights are most effectively protected when '[a]mbition . . . [is] made to counteract ambition'—a claim that is usually realized through inter- and intragovernmental checks at the federal and state levels"—can be operationalized by the private sector.[43] The private sector's capacity to shape, and even help constitute, the separation of powers is at its height in the domains of technology and communications. And as these domains become ever more central in the twenty-first century, the private sector's influence on our

Political Process Theory, and the Nondelegation Doctrine, 102 GEO. L.J. 1721, 1725 (2014) ("[A]dministrative law principles, including central features of the Administrative Procedure Act . . . , should apply to law enforcement departments, which are, after all, administrative agencies."); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 95 (2016) ("[T]he concrete rules governing panvasive techniques should be viewed through the entirely different prism of administrative law. The reason administrative law should be the primary mechanism in this setting is simple: police departments are agencies, and as such should have to abide by the same constraints that govern other agencies.").

39. *See, e.g.*, Renan, *supra* note 29, at 1042 ("While our Fourth Amendment framework is transactional, . . . surveillance is increasingly *programmatic*.").

40. *See, e.g.*, Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245, 2252 (2001) ("[I]n comparison with other forms of control, the new presidentialization of administration renders the bureaucratic sphere more transparent and responsive to the public, while also better promoting important kinds of regulatory competence and dynamism.").

41. *See* Rascoff, *supra* note 29, at 637; *id.* at 639 (offering a "qualified normative defense of the turn to the institutional presidency . . . as a source of political direction and accountability for the post-9/11 intelligence bureaucracy").

42. *See* Crespo, *supra* note 36, at 2059-65.

43. Rascoff, *supra* note 29, at 689 (alterations in original) (footnote omitted) (quoting THE FEDERALIST NO. 51, at 319 (James Madison) (Clinton Rossiter ed., 2003 prtg.)); *see also* Jon D. Michaels, *An Enduring, Evolving Separation of Powers*, 115 COLUM. L. REV. 515, 520 (2015) ("[T]oday's increasingly sharp turn to privatized government is . . . best understood through a separation-of-powers framework.").

constitutional order will only increase. This Article supplies the factual background and conceptual tools for a more accurate and nuanced account of how technology companies fit into what Aziz Huq and Jon Michaels have called the "external political surround": the "diverse external ecosystem of actors who influence how the separation of powers plays out."[44]

In this Article, I examine surveillance intermediaries and their role in government surveillance as follows. Parts I, II, and III ask the descriptive question: How do surveillance intermediaries influence when, how, and how much the government conducts electronic surveillance? Part I explains how our ballooning appetite for generating and storing digital information has made surveillance intermediaries more central than ever to government surveillance. It also describes the intermediaries' commercial and ideological incentives to resist government surveillance, especially in the wake of the Snowden disclosures.

Part II sorts surveillance intermediaries' techniques for resisting government surveillance into three categories. Intermediaries couple a *proceduralism* that rejects voluntary cooperation with government requests to an aggressive *litigiousness* against government demands for data and restrictions on publicizing those requests.[45] Intermediaries also rely on *technological unilateralism*, leveraging their size and centralized platforms to implement architectural features like end-to-end encryption and overseas data storage.[46] And through *policy mobilization*, intermediaries try to turn public opinion against government surveillance by combining old-fashioned techniques like lobbying and public relations campaigns with new strategies that rely on publishing transparency reports and other information on government surveillance.[47]

Part III explains how these techniques of resistance augment the *surveillance separation of powers*: how the *surveillance executive*[48]—the law enforcement

44. Aziz Z. Huq & Jon D. Michaels, *The Cycles of Separation-of-Powers Jurisprudence*, 126 YALE L.J. 346, 403 (2016) (capitalization altered).

45. *See infra* Part II.A.

46. *See infra* Part II.B.

47. *See infra* Part II.C.

48. I have adapted Shirin Sinnar's useful label of the "national security executive": the massive bureaucracy, spanning multiple executive agencies, that is responsible for national security. *See, e.g.*, Shirin Sinnar, *Institutionalizing Rights in the National Security Executive*, 50 HARV. C.R.-C.L. L. REV. 289, 290-91, 293 (2015). Barry Friedman and Maria Ponomarenko similarly combine law enforcement and national security institutions, drawing all "organs of government that conduct surveillance on, or utilize force against, the population of the United States" under the umbrella of "policing agencies." Friedman & Ponomarenko, *supra* note 38, at 1831 n.15. Unlike Friedman and Ponomarenko, I confine myself to electronic surveillance (rather than physical surveillance,
footnote continued on next page

and foreign-intelligence agencies like the FBI and the National Security Agency (NSA) that conduct surveillance—can be checked by other parts of the government. Surveillance intermediaries enhance *interbranch checks* by making it easier and more politically rewarding for Congress to rein in the surveillance executive and by creating justiciable cases through which the courts can oversee surveillance activities.[49] They also augment *intrabranch* and *intra-agency checks*, empowering economic and foreign relations agencies, as well as the surveillance executive's own inspectors general and privacy and civil liberties offices.[50]

Part IV addresses the normative question: In what ways is it good or bad that surveillance intermediaries have so much power over government surveillance? Here I distinguish between two stages of surveillance policymaking: first, the process of analyzing different options and identifying their costs and tradeoffs; and second, the process of choosing a particular surveillance policy from the available options. At each stage I offer a mixed verdict. At the first stage, surveillance intermediaries can help society better construct *surveillance frontiers*—menus of surveillance policy options—by adding more information and more diverse perspectives, as well as by minimizing inefficient alternatives. But they can also create negative second-order effects by forcing the government to engage in more intrusive surveillance and by making it easier for the surveillance intermediaries themselves to collect more data on their users. At the second stage, surveillance intermediaries can enhance *surveillance self-government*—democratic supervision over surveillance policy—by fortifying inter- and intrabranch checks and raising the public's awareness of government surveillance. But when the intermediaries constrain otherwise lawful government surveillance through technological unilateralism, surveillance self-government suffers. Part IV concludes by using this normative framework to offer an answer to an important emerging doctrinal question: whether the First Amendment forbids compelling surveillance intermediaries to provide technical assistance to law enforcement. (It should not.)

Before I begin, I want to flag several limitations on the scope of this Article. First, I focus on newer-generation, user-centric surveillance intermediaries—those companies that provide digital communications and data storage and processing to consumers—rather than on more traditional intermediaries like phone companies, internet service providers, and the large-scale managers of

interrogation, or enforcement) and thus use the term "surveillance executive" rather than the broader "policing agencies."

49. *See infra* Part III.A.

50. *See infra* Part III.B.

the internet backbone.[51] This is in part to keep the project at a manageable scope and in part because it is the Apples and Facebooks of the world that have been on the forefront of resisting government surveillance. Other intermediaries may yet exhibit a similar pattern of activity, but, if so, such behavior will have to be analyzed on its own terms.[52]

Second, I am *not* arguing that surveillance intermediaries have, on balance, made it harder for the government to engage in surveillance. Much government surveillance is by nature secret and thus not amenable to public discussion or analysis. And even surveillance that can be discussed more openly, such as that done for law enforcement purposes, is difficult to quantify and compare. Thus, I take no sides in the vigorous ongoing debate over whether, on balance, technological changes like widespread encryption have resulted in law enforcement "going dark," or whether the digitization of everyday life has instead led to a "golden age of surveillance."[53]

Even if surveillance intermediaries enable a net increase in government surveillance, such surveillance is subject to meaningfully stronger constraints than if surveillance intermediaries didn't resist. Their resistance introduces "friction[s]"[54] into the surveillance process; just as in the physical world, these

51. For an example of work examining the role such companies could play in reforming government surveillance, see Mieke Eoyang, *Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance* 14-17 (Hoover Inst., Aegis Paper No. 1603, 2016), https://perma.cc/Y3J7-CKBZ.

52. There are some early indications that the traditional intermediaries may also be adopting a more confrontational stance against government surveillance. For example, Verizon, which owns Yahoo, signed on to an amicus brief on behalf of leading tech companies in the pending Supreme Court case *Carpenter v. United States*, arguing that the Court should extend Fourth Amendment protections to geolocation data. *See* Brief for Technology Companies as Amici Curiae in Support of Neither Party at 8-9, 29-32, Carpenter v. United States, No. 16-402 (U.S. Aug. 14, 2017), 2017 WL 3530959. *WIRED* captured the surprising nature of Verizon's participation in its story headline. *See* Lily Hay Newman, *Verizon—Yes, Verizon—Just Stood Up for Your Privacy*, WIRED (Aug. 16, 2017, 10:00 AM), https://perma.cc/D2GF-AC4V.

53. *Compare* James B. Comey, Dir., FBI, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Remarks Before the Brookings Institution 2 (Oct. 16, 2014), https://perma.cc/8BVW-E248 ("Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so."), *with* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 420 (2012) ("Notably, law enforcement and national security agencies fear they are 'going dark' as criminals and terrorists increasingly use a bewildering variety of new communications tools. On more careful examination, however, . . . this mix of new technology is actually enabling a 'golden age of surveillance.'").

54. *See* LESSIG, *supra* note 13, at 202.

frictions push against and slow the government's motion, even if they cannot ultimately stop it or set it in reverse. And in some cases—such as the government's access to real-time data—encryption and other technological changes may very well decrease absolute levels of government surveillance. Either way, this relative if not absolute decline in surveillance is substantial, and thus the influence of surveillance intermediaries is worth the effort to describe, analyze, and judge.

I. Rise of the Surveillance Intermediaries

In today's world, government surveillance—whether targeted or programmatic, for law enforcement or foreign intelligence—relies on the cooperation of a small number of technology companies that are large, multinational, and opposed to it. This Part describes how this became the case and why these companies have the incentive, and not just the means, to resist government surveillance.

To begin, consider the three environments in which government surveillance takes place. The first is the *public environment*, as when the police tail a suspect down the street or when spy satellites take pictures from space. Here the government can directly surveil, and without needing anyone's cooperation. The second environment is the *target environment*, as when the government searches someone's person or home. Here the target can theoretically resist—for example, by running away or barricading her doors. But the government has obvious and overwhelming advantages over individual targets, whose attempts at resistance seldom meaningfully frustrate government surveillance.

Historically, most government surveillance has taken place in these two environments. But another, the *third-party environment*, has come to dominate. Here a third party collects information, usually for its own business purposes, that the government wants—for example, phone company billing records that include a cellphone subscriber's call history. Instead of seeking information from the target directly, the government seeks it from the third party, either because it's easier to get the information that way or because only the third party has the information. The third party becomes a *surveillance intermediary*: It stands between the government and the target of the surveillance.

The third-party environment has long been an important locus of government surveillance, particularly where the government has sought communications data. This is because the most important communications systems in U.S. history—from the telegraph to the telephone to the internet—have been owned and operated by the private sector.[55] In the past, these

55. *See* Eoyang, *supra* note 51, at 3.

surveillance intermediaries generally cooperated with the government, whether under formal legal regimes or informal voluntary arrangements.[56] Under the notorious Project SHAMROCK, which lasted from the end of World War II to its exposure in the mid-1970s, Western Union and other telegraph companies voluntarily provided the NSA with daily copies of most international telegraphs entering or exiting the United States.[57] More recently, major U.S. telecommunications providers like AT&T and Verizon aided the government in controversial surveillance programs set up after 9/11.[58]

While the third-party environment has always been vital to government surveillance, today its role is even more critical because of how much more information we generate. Some of this information is a digital substitute for past analog activity—emails have replaced letters, and texts and instant messaging apps increasingly displace phone calls. But we have also created new categories of information like geolocation data, which is easy to collect because of our constant use of cellphones and GPS-enabled devices. The emerging Internet of Things will generate even more data. And because cheap storage

56. Generally, but not always. An important exception was the *New York Telephone* case discussed below. *See* United States v. N.Y. Tel. Co., 434 U.S. 159 (1977); *infra* notes 135-39 and accompanying text. And at the dawn of electronic surveillance, in the landmark Fourth Amendment case *Olmstead v. United States*, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), a coalition of major telephone companies submitted an amicus brief opposing government wiretapping. *See* Brief in Support of Petitioners' Contention at 1, 8, *Olmstead*, 277 U.S. 438 (Nos. 493, 532 & 533); *see also* Orin Kerr, *Communications Network Providers Opposed Government Surveillance—in 1928*, WASH. POST: VOLOKH CONSPIRACY (July 13, 2016), https://perma.cc/9N8X-RN55. There is some evidence that at least one telecommunications provider, Qwest Communications (later acquired by CenturyLink, *see* Press Release, CenturyLink, CenturyLink and Qwest Complete Merger (Apr. 1, 2011), https://perma.cc/X6EY-EBCB) rebuffed a pre-9/11 request from the NSA to participate in the agency's surveillance activities. *See* Scott Shane, *Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11*, N.Y. TIMES (Oct. 14, 2007), https://perma.cc/ZVB4-JPE4. But overall, cooperation was the rule and conflict a rare exception.

57. *See* S. REP. NO. 94-755, bk. 3, at 765, 767-69, 771, 776 (1976). Until the NSA's formation in 1952, SHAMROCK was controlled by first the Army Signals Security Agency and then the Armed Forces Security Agency. *See id.* at 770. SHAMROCK featured prominently in the famous Church Committee report on the U.S. government's surveillance abuses, *see id.* at 765-76, and the program's exposure was part of the impetus for the intelligence reforms of the 1970s, including FISA. *See* L. Britt Snider, *Unlucky SHAMROCK: Recollections from the Church Committee's Investigation of NSA*, STUD. INTELLIGENCE, Winter 1999-2000 Unclassified Edition, at 43, 49-51; *see also* Jeremy D. Mayer, *9-11 and the Secret FISA Court: From Watchdog to Lapdog?*, 34 CASE W. RES. J. INT'L L. 249, 249 (2002).

58. *See* SAVAGE, *supra* note 22, at 183-87.

and bandwidth are readily available,[59] we find it convenient to let third-party providers hold our trails of "digital 'exhaust'"[60] in the cloud.

This mass of data tells rich stories about our lives—what we do and where, when, and with whom we do it. Hence it's a treasure trove for surveillance officials. When police make arrests, the "pocket litter" they seize often includes smartphones. When investigators work cases, they routinely apply for warrants to search email and social media accounts to get evidence of wrongdoing, intent, or co-conspirators. And when intelligence analysts seek to understand the activities of terrorists, spies, and foreign leaders, they're as likely to rely on emails and instant messages stored by the major surveillance intermediaries as they are on more traditional sources of foreign intelligence, such as human sources.

Statistics released by the major surveillance intermediaries illustrate the massive volumes at play and the speed at which they're increasing. In 2015 Google received over 24,000 requests from U.S. law enforcement for user data, a nearly threefold increase from 2010.[61] Facebook received even more requests for user data—nearly 37,000 in 2015.[62] Although the government prohibits companies from publishing similarly detailed statistics about foreign-intelligence and national security requests,[63] its own statistics disclose that in 2013, section 702 of the Foreign Intelligence Surveillance Act (FISA)[64] was used to target nearly 90,000 people or entities.[65] None of these searches was conducted unilaterally; each of them relied on a private company's

59. *See, e.g.*, Brian Barrett, *Amazon's New Unlimited Cloud Storage Is Absurdly Cheap*, WIRED (Mar. 26, 2015, 11:28 AM), https://perma.cc/2USL-RSLV.

60. MANYIKA ET AL., MCKINSEY GLOB. INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 1 (2011), https://perma.cc/4RZ3-6ABQ.

61. *See Transparency Report: Requests for User Information*, GOOGLE, https://perma.cc/64X6-4D8Z (archived Oct. 13, 2017).

62. *See Government Requests Report: United States; January 2015-June 2015*, FACEBOOK, https://perma.cc/V5TM-UUHR (archived Oct. 13, 2017); *Government Requests Report: United States; July 2015-December 2015*, FACEBOOK, https://perma.cc/6HYC-LCUS (archived Oct. 13, 2017).

63. *See* 50 U.S.C. § 1874(a) (2015).

64. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, sec. 101, § 702, 122 Stat. 2436, 2438-48 (codified as amended at 50 U.S.C. § 1881a). Under section 702, the government can collect the electronic communications of "persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). For a detailed analysis, see 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 2D ch. 17 (2012).

65. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 33 (2014), https://perma.cc/2GFL-78HM.

cooperation,[66] illustrating "the role industry almost invariably plays as technical middleman (and potential legal gatekeeper) in facilitating electronic eavesdropping."[67]

Because of network effects (digital platforms become more valuable as more people use them) and economies of scale, a few industry giants dominate among these middlemen and gatekeepers. Just three companies—Google, Microsoft, and Yahoo—control 98% of the U.S. search engine market.[68] Two video streaming services, Netflix and YouTube, consume over half of the downstream fixed access bandwidth during peak periods in North America.[69] And the average Facebook user spends close to an hour every day using Facebook services—and that's before you include Facebook-owned WhatsApp.[70] What's true of platforms applies to devices: 97% of U.S. smartphones run either Google's Android or Apple's iOS.[71] Ultimately, the biggest surveillance intermediaries dominate not just the internet but also the global economy. Five U.S. technology companies—Apple, Alphabet (Google's parent company), Microsoft, Amazon, and Facebook—routinely have the biggest market capitalizations in the world.[72]

This vast corporate power would do little to constrain government surveillance if surveillance intermediaries saw their interests as aligned with those of government spies and investigators. But they don't. Today's intermediaries have powerful incentives to resist government surveillance. In this regard the 2013 Snowden disclosures were a major inflection point. The massive leaks of classified information revealed a broad surveillance system—and, worse, implicated major Silicon Valley companies as collaborators,

66. The government has explained that "under Section 702 of FISA, the United States Government does not unilaterally obtain information from the servers of U.S. electronic communication service providers," and that "[a]ll such information is obtained with FISA court approval and with the knowledge of the service provider." Office of the Dir. of Nat'l Intelligence, *Section 702 of the Foreign Intelligence Surveillance Act*, IC ON THE RECORD, https://perma.cc/9VPS-WMPT (archived Oct. 13, 2017); *see also* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 65, at 33 (describing the process for initiating surveillance).

67. Michaels, *supra* note 14, at 911-12 (footnote omitted).

68. *See comScore Releases February 2016 U.S. Desktop Search Engine Rankings*, COMSCORE (Mar. 16, 2016), https://perma.cc/ENF9-K29V.

69. *See* Sandvine, 2016 Global Internet Phenomena: Latin America & North America 4 tbl.1 (2016), https://perma.cc/J56F-SEP6.

70. James B. Stewart, *Facebook Has 50 Minutes of Your Time Each Day. It Wants More.*, N.Y. TIMES (May 5, 2016), https://perma.cc/P8Z2-LSV7; *see* Adrian Covert, *Facebook Buys WhatsApp for $19 Billion*, CNN (Feb. 19, 2014), https://perma.cc/35HZ-ZSTD.

71. *See comScore Reports February 2016 U.S. Smartphone Subscriber Market Share*, COMSCORE (Apr. 6, 2016), https://perma.cc/EF7X-JRU3.

72. *See, e.g.*, Shira Ovide & Rani Molla, *Technology Conquers Stock Market*, BLOOMBERG GADFLY (Aug. 2, 2016, 7:30 AM EDT), https://perma.cc/2UPE-83CX.

causing blowback from domestic civil liberties groups and overseas customers.[73] Although the disclosures motivated some legislative and policy changes,[74] they didn't alter the core of U.S. surveillance. They did, however, as Julian Sanchez notes, "transform[] the incentives of the technology companies that maintain [the] architectures" that permit surveillance.[75] This, so far, has been Edward Snowden's main victory: to increase the incentives for surveillance intermediaries to resist the government.[76]

These incentives fall into two categories. The first is financial. Companies have always had the incentive to lower compliance costs by resisting government surveillance (as long as the costs of such resistance were themselves not too great).[77] But the Snowden disclosures have turned such resistance into an opportunity for product differentiation. For example, when Apple publicly touts how its business model doesn't need to access user data,[78]

73. *See* Yan Zhu, *Security Experts Call on Tech Companies to Defend Against Surveillance*, ELEC. FRONTIER FOUND. (Feb. 26, 2014), https://perma.cc/R6QL-C77J (noting that "trust in technology companies has been badly shaken" in the wake of the Snowden disclosures); *see also* Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), https://perma.cc/7MMV-K9PK. The extent of cooperation was often overstated, however, especially when the disclosures first came out. For example, early stories mistakenly reported that the NSA tapped directly into the servers of major U.S. companies like Google and Microsoft and that it did so with the companies' knowledge. *See* Ed Bott, *How Did Mainstream Media Get the NSA PRISM Story So Hopelessly Wrong?*, ZDNET (June 14, 2013, 5:09 AM PDT), https://perma.cc/4CSU-45F3.

74. The most important legislative change was the USA FREEDOM Act of 2015, which ended the NSA's collection of bulk telephony metadata. *See* Pub. L. No. 114-23, § 103, 129 Stat. 268, 272 (codified at 50 U.S.C. § 1861(b)-(c) (2015)). The most important policy change was the Obama Administration's Presidential Policy Directive 28 (PPD-28), which increased privacy protections for foreigners with respect to foreign intelligence. *See* Presidential Policy Directive/PPD-28, Directive on Signals Intelligence Agencies, 2014 DAILY COMP. PRES. DOC. NO. 00031 (Jan. 17, 2014), https://perma.cc/ZDL5-3UTP. Although the Trump Administration could revoke PPD-28, it has so far left the policy in place. *See* Cameron Kerry, *Trump Puts U.S.-EU Privacy Shield at Risk*, LAWFARE (June 12, 2017, 1:41 PM), https://perma.cc/B4VT-H8MU.

75. Julian Sanchez, Opinion, *Snowden Showed Us Just How Big the Panopticon Really Was. Now It's Up to Us*, GUARDIAN (June 5, 2014, 4:02 PM EDT), https://perma.cc/WP6P-YPYJ; *see also* SAVAGE, *supra* note 22, at 570 ("The Snowden leaks changed the behavior of communications companies. Firms began to compete, in part as a marketing move, to be seen as protecting the security of users' private messages.").

76. *See* SCHNEIER, *supra* note 29, at 207 ("So far, the most important effect of the Snowden revelations is that they have ruptured the public-private surveillance partnership . . . ."); Rascoff, *supra* note 29, at 663; Nicholas Weaver, *Band-Aids Can't Fix Bullet Holes: Silicon Valley and the NSA*, LAWFARE (Sept. 30, 2015, 3:55 PM), https://perma.cc/Z5G8-T448.

77. *See* Bellia, *supra* note 35, at 340 ("[P]roviders are likely to have an incentive to advocate limits on executive discretion in surveillance law because broader use of surveillance techniques will be costly to providers.").

78. *See Privacy*, APPLE, https://perma.cc/VG7X-YLPN (archived Nov. 16, 2017) ("Apple doesn't gather your personal information to sell to advertisers or other organizations.").

part of what it's doing is jabbing at companies like Google and Facebook, which rely on scanning user data to sell advertisements.[79]

Resisting U.S. government surveillance can also improve a company's global competitiveness—specifically, its ability to sell its products and services abroad. This is particularly important because the international market provides the bulk of sales for modern technology companies (unlike for the phone companies and retail banks that made up the earlier generation of surveillance intermediaries). For example, Facebook has over two billion active monthly users,[80] of which the vast majority are outside the United States; similarly, over half of the company's ad revenues come from abroad.[81] Given such globally distributed revenue streams, along with the ability to move their key asset—data—instantaneously around the world, today's surveillance intermediaries come as close as we've ever seen to the Platonic ideal of the multinational corporation.

Many of the surveillance intermediaries' foreign users (and their governments) suspect that the internet is a "Trojan horse for . . . surveillance by the NSA and American companies"[82] and would rather that U.S. technology companies resist—or at least not slavishly cooperate with—what they see as the out-of-control U.S. surveillance state. (It doesn't help that the government's go-to reassurance for domestic audiences is that it mostly just monitors foreigners.)[83] Because cloud services are globally integrated—everyone's information transits the same systems and is often stored in the same data centers—even strictly *domestic* surveillance by the U.S. government raises the specter, real or imagined, of *foreign* surveillance. Most foreign customers, like their domestic counterparts, are probably untroubled by this possibility—if

79. *See, e.g.*, Mark Hachman, *The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers*, PCWORLD (Oct. 1, 2015, 3:00 AM PT), https://perma.cc/6XEA-NQQX (comparing tech companies' policies regarding the use of user data to sell targeted advertisements).

80. *See Company Info*, FACEBOOK, https://perma.cc/D4W8-JSQV (archived Oct. 13, 2017).

81. *Facebook Earns 51 Percent of Ad Revenue Overseas*, CNBC (June 10, 2015, 8:06 AM ET), https://perma.cc/63C5-DLDC.

82. Cameron F. Kerry, Ctr. for Tech. Innovation at Brookings, Bridging the Internet-Cyber Gap: Digital Policy Lessons for the Next Administration 9 (2016), https://perma.cc/Z2X2-WABL.

83. For example, when news broke about the NSA's PRISM program, President Obama emphasized that the program "does not apply to U.S. citizens, and it does not apply to people living in the United States." Remarks on Health Insurance Reform and an Exchange with Reporters in San Jose, California, 2013 DAILY COMP. PRES. DOC. NO. 00397, at 5 (June 7, 2013), https://perma.cc/QCH4-YUUE. Cameron Kerry, then the Acting Secretary of Commerce, describes the message as having "wave[d] a glaring red flag outside the U.S." Kerry, *supra* note 82, at 1.

they think about it all. But for foreign companies, U.S. surveillance supplies the perfect cover behind which to lobby for old-fashioned protectionism.[84]

Economic incentives to oppose government surveillance are not merely theoretical: Consider the decision of the Court of Justice of the European Union in the *Schrems* case, which, in the wake of the Snowden disclosures, invalidated a safe harbor agreement between the European Union and the United States that permitted U.S. companies to repatriate European data.[85] *Schrems* threatened a market in transatlantic data flows worth many billions of dollars a year.[86] More generally, estimates made after the Snowden leaks predicted losses of tens or hundreds of billions of dollars for U.S. companies in the form of canceled or forgone global cloud service contracts.[87] Silicon Valley blames Washington for putting it in this predicament, and it is not in a forgiving mood.[88]

The financial incentives to resist government surveillance are matched by ideological ones. One cause of friction is cultural incompatibility—what Amy Zegart has called the "suit-hoodie divide" between technology companies and the government.[89] But the differences run deeper. Many of those who work for surveillance intermediaries, along with the industry's associated academics and researchers, subscribe to what some sociologists have called the "Californian Ideology": a worldview that is simultaneously countercultural in lifestyle, laissez-faire in economics, and libertarian in politics.[90] As reporter Cade Metz describes, for instance, "In Silicon Valley, strong encryption isn't really up for debate. Among tech's most powerful leaders, it's orthodoxy."[91] This is not only because it is seen as technically superior to other ways of increasing security. As computer scientist Phillip Rogaway, one of the most eloquent exponents of cryptography's political implications, has argued, encryption also helps

84. *See* Adam I. Klein, *Decryption Mandates and Global Internet Freedom: Toward a Pragmatic Approach* 4-5 (Hoover Inst., Aegis Paper No. 1608, 2016), https://perma.cc/LFD7-T5ZW.

85. *See* Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶¶ 1-2, 7, 106 (Oct. 6, 2015), https://perma.cc/898N-MW7E.

86. Natalia Drozdiak & Sam Schechner, *EU Court Says Data-Transfer Pact with U.S. Violates Privacy*, WALL ST. J. (Oct. 6, 2015, 1:42 PM ET), https://perma.cc/2GPU-YGQK.

87. *See* Miller, *supra* note 73.

88. *See* Weaver, *supra* note 76.

89. Amy Zegart, *Policymakers Are from Mars, Tech Company Engineers Are from Venus*, LAWFARE (June 6, 2016, 9:54 AM), https://perma.cc/8WV6-4U3R.

90. *See* Richard Barbrook & Andy Cameron, *The Californian Ideology*, 6 SCI. AS CULTURE 44, 44-45 (1996); *see also* Peter Swire, The Declining Half-Life of Secrets and the Future of Signals Intelligence 4 (2015), https://perma.cc/RX32-MR5R ("[M]uch of the information technology talent has anti-secret and libertarian inclinations.").

91. *See* Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED (Apr. 5, 2016, 11:00 AM), https://perma.cc/QRN9-5MRD.

prevent a "dystopian world of pervasive surveillance," with all the attendant social and political evils.[92]

Certainly not all engineers working in Silicon Valley have such strong ideological views. But managers and corporate leaders may still have an incentive to align corporate policy with the Californian Ideology for recruiting and morale purposes. And more generally, it only takes a few true believers to effectively thwart government surveillance. For example, at the time it rolled out end-to-end encryption, WhatsApp had only about fifty engineers, and only fifteen of those were needed to enable encrypted messaging for a billion people.[93] Technology's enormous returns to scale empower those with more radical views—those who most strongly favor encryption or oppose surveillance. For instance, Moxie Marlinspike, who developed the secure-communication service Signal and helped WhatsApp encrypt its system,[94] has defended encryption as enabling lawbreaking to spur social change.[95] Marlinspike's views are only a sharply drawn version of a sentiment pervading Silicon Valley: that by reintroducing fully private conversations, end-to-end encryption properly restores law enforcement surveillance to pre-digital-age levels.[96]

Although Silicon Valley has strong incentives to resist government surveillance, it's important not to overstate the point. First, not all actions by surveillance intermediaries that make surveillance more difficult are necessarily motivated by a desire to thwart U.S. government surveillance. Given the amount and sensitivity of data stored on devices and online services, companies have a natural desire to make their products as secure as possible for their users; the same security that protects against cybercriminals and malicious hackers naturally impedes governments as well. In addition, because surveillance intermediaries have global user bases, many of their users are located in repressive regimes. Companies may feel a particular responsibility to ensure the security of those users against repression by their governments and so may build their systems accordingly.[97]

92. *See* Phillip Rogaway, The Moral Character of Cryptographic Work 25, 29-30, 44-46 (2015), https://perma.cc/LPZ7-7GDE.

93. *See* Metz, *supra* note 91.

94. *See* Andy Greenberg, *Meet Moxie Marlinspike, the Anarchist Bringing Encryption to All of Us*, WIRED (July 31, 2016, 6:45 AM), https://perma.cc/DKH6-97K8.

95. *See We Should All Have Something to Hide*, MOXIE MARLINSPIKE (June 12, 2013), https://perma.cc/ZQX7-XQ54.

96. *See* Metz, *supra* note 91.

97. It's worth noting, though, that some leading surveillance intermediaries have still been willing to make compromises when doing business in countries that have repressive regimes but where the companies have large user bases. For example, both Facebook and Apple have either made or at least considered making concessions to the Chinese government. *See, e.g.*, Mike Isaac, *Facebook Said to Create Censorship Tool to Get Back Into*

footnote continued on next page

Second, surveillance intermediaries frequently cooperate with government surveillance. In addition to complying with unexceptional government orders for data, there are other areas in which surveillance intermediaries support—or at least grudgingly tolerate—government surveillance. For example, technology companies cooperate with the government to remove terrorist propaganda,[98] internet service providers comply with their legal obligations to report child pornography,[99] and the government and the private sector work together to detect and disrupt cyberattacks.[100] Surveillance intermediaries and other technology companies also sometimes enable the government's surveillance capabilities, whether by serving as "fourth-party" data brokers that purchase, package, and resell user data,[101] or by providing infrastructure and technology.[102] For instance, Amazon has contracted with the Central Intelligence Agency (CIA) to provide cloud computing for U.S. intelligence agencies,[103] and companies like Cellebrite provide tools that help federal, state, and local law enforcement agencies access locked smartphones.[104]

China, N.Y. TIMES (Nov. 22, 2016), https://perma.cc/3WUW-7GS8 (noting that in exploring ways to reenter the Chinese market, Facebook has created as-yet undeployed software "to suppress posts from appearing in people's news feeds in specific geographic areas"); Paul Mozur, *Apple Removes Apps from China Store That Help Internet Users Evade Censorship*, N.Y. TIMES (July 29, 2017), https://perma.cc/82DM-NJUN.

98. *See, e.g.*, Mike Isaac, *Twitter Steps Up Efforts to Thwart Terrorists' Tweets*, N.Y. TIMES (Feb. 5, 2016), https://perma.cc/457L-GQAX.

99. *See, e.g.*, Susan Klein & Crystal Flinn, *Social Media Compliance Programs and the War Against Terrorism*, 8 HARV. NAT'L SECURITY J. 53, 79 (2017) ("[M]any email providers, cloud companies, and other online service providers have decided that it is in the best interests of their users and their companies to keep their services free of illegal content. Consequently, such companies often use automated tools developed by the [National Center for Missing and Exploited Children] or developed internally to check all of their private e-mails for pornographic pictures and videos involving children." (footnote omitted)); *see also* 18 U.S.C. § 2258A (2016) (setting forth reporting requirements for electronic communication service providers).

100. For example, the Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, div. N, tit. I, 129 Stat. 2242, 2936-56 (codified at 6 U.S.C. §§ 1501-1510 (2016)), encourages public-private sharing of cyberthreat information. *See* Kristin N. Johnson, Essay, *Managing Cyber Risks*, 50 GA. L. REV. 547, 578-80 (2016).

101. *See* Michaels, *supra* note 14, at 917-19 (describing "fourth parties" as companies that "collect information from a range of private (third-party) sources"); *see also* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 167 (2012); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 31 (2015).

102. *See* SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX 121-22 (2014).

103. *See* Frank Konkel, *The Details About the CIA's Deal with Amazon*, ATLANTIC (July 17, 2014), https://perma.cc/5MEV-RK86.

104. *See* Nick Taborek, *You're Under Arrest! Hand Over That iPhone*, BLOOMBERG BUSINESSWEEK (Mar. 29, 2012, 4:55 PM PDT), https://perma.cc/YG6W-ZTKJ.

Some scholars worry that such relationships, along with the revenues that come from traditional government information technology contracts (like Google's public sector cloud storage business), prevent companies from standing up to government surveillance.[105]

Finally, it's also possible that the motivation for surveillance intermediaries to resist government surveillance is largely driven by the contingent political climate of the last few years: the Obama Administration's close and friendly relationship with Silicon Valley;[106] the aftershocks of the Snowden disclosures;[107] and the continuing absence of large-scale, 9/11-style terrorist attacks. If this is true, intermediary resistance might merely be "grounded in a particular political moment" and would thus ebb if the political or security context changed.[108] The pendulum may well swing back.[109]

But then again, it might not. Never in the history of electronic surveillance have technology companies so aggressively stood up to the government. Nor have they ever relied so heavily on a foreign user base or exhibited such an intense libertarian aversion to government invasions of privacy. Charting the push and pull between these factors and the changing political and social context is an empirical question that cannot be answered by theoretical analysis. But the age in which technology companies would salute smartly to

105. *See* Cover, *supra* note 25, at 1473-75; *see also* Balkin, *supra* note 12, at 2332 ("The recipients of many, if not most, national security letters are large businesses. They may have little reason to challenge NSLs and gag orders, first, because they want smooth relations with the government . . . ."). Scott Malcomson, for instance, implies that Amazon's cloud service contract explains its conspicuous absence from a May 2015 letter signed by Apple, Facebook, Google, and other companies urging President Obama to oppose legislation mandating encryption "back doors" for law enforcement. *See* SCOTT MALCOMSON, SPLINTERNET: HOW GEOPOLITICS AND COMMERCE ARE FRAGMENTING THE WORLD WIDE WEB 161-62, 167-68 (2016).

106. *See* Jenna Wortham, *Obama Brought Silicon Valley to Washington*, N.Y. TIMES (Oct. 25, 2016), https://perma.cc/H2V8-F6F6.

107. *See supra* notes 73-76 and accompanying text.

108. Renan, *supra* note 29, at 1116; *see* SCHNEIER, *supra* note 29, at 209-10; Cover, *supra* note 25, at 1484.

109. Early signs don't point toward a rapprochement between Silicon Valley and the Trump White House; nearly a hundred technology companies, including many of the major surveillance intermediaries, filed an amicus brief in the Ninth Circuit opposing the Trump Administration's first executive order banning immigration from seven predominantly Muslim countries. *See* Brief of Technology Companies and Other Businesses as Amici Curiae in Support of Appellees at 1-3, Washington v. Trump, 847 F.3d 1151 (9th Cir. 2017) (No. 17-35105), 2017 WL 626517; *id.* app. A (listing the signatory amici); *see also* Andrew Keane Woods, *Draining the Valley Instead of the Swamp*, LAWFARE (Feb. 6, 2017, 5:03 PM), https://perma.cc/EM4Q-VWKK ("[T]he brief is notable in that it was filed at all. American tech firms have been in a delicate balancing act, attempting to assuage their customers' concerns on the one hand without going so far as to 'poke the bear' on the other; the brief is a sign that the balance has tilted.").

government surveillance orders is over. Companies like Apple and Facebook really did warrant-proof some of their products by encrypting them, in the teeth of intense public opposition by federal, state, and local law enforcement agencies—and, as Part II below will show, this is far from all they did. It is, as they say, hard to make predictions, especially about the future. But even if surveillance intermediaries come to moderate their opposition, it's a fair bet that their cooperation will be grudging, their resistance meaningful, and thus their power worth studying.

II. Techniques of Resistance

Part I told the story of how the major surveillance intermediaries have risen to prominence and why they're incentivized to resist government surveillance. But does any of this matter? Do even technological goliaths stand a chance against the power of the sovereign state, especially when it is discharging its ultimate responsibilities: public safety and national security? After all, how many divisions has Facebook got?[110] The answers to these questions are: Yes, it matters; yes, they stand a chance; and, between them, they have quite a few divisions. Their *techniques of resistance* fall into three categories: first, *proceduralism* and *litigiousness*; second, *technological unilateralism*; and third, *policy mobilization*.[111] These techniques reinforce each other and benefit from surveillance intermediaries' size and multinational reach.

A. Proceduralism and Litigiousness

The law is a powerful tool with which to resist government surveillance; the first step to using it is to bring that surveillance into the legal process. Unlike their forerunners, who often cooperated with informal, noncompulso-

110. On being warned to heed the Vatican's concerns about the treatment of Catholics in the Soviet Union, Stalin reportedly sniffed, "The Pope! How many divisions has *he* got?" *See* WINSTON S. CHURCHILL, THE SECOND WORLD WAR: THE GATHERING STORM 135 (1948).

111. My taxonomy of law, technology, and society follows in the tradition of Lawrence Lessig's New Chicago School, which identified four modalities for regulating behavior—law, social norms, market forces, and "architecture," *see* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662-63 (1998)—and which Lessig used to build his influential account of how behavior is regulated on the internet, s*ee* LESSIG, *supra* note 13, at 121-25. Ryan Calo has applied a similar approach to analyze how individuals can avoid government surveillance. *See* Ryan Calo, Essay, *Can Americans Resist Surveillance?*, 83 U. CHI. L. REV. 23, 23-24 (2016). And security researcher Bruce Schneier has argued that corporations can fight government surveillance through "transparency, technology, litigation, and lobbying." SCHNEIER, *supra* note 29, at 207. Like Schneier, I focus on private sector actors and so do not include the market as a separate element, treating it instead as the background against which surveillance intermediaries wield their techniques of resistance.

ry government requests,[112] today's surveillance intermediaries generally won't hand over data unless the government compels its production through formal legal channels.[113] For example, Google advertises that "[t]he government needs legal process—such as a subpoena, court order or search warrant—to force Google to disclose user information."[114] These kinds of promises have been widely adopted,[115] with the hope of convincing users that their services won't hand over their personal data until the government has jumped through the appropriate procedural hoops.[116]

Unsurprisingly, the government finds it harder to conduct surveillance when surveillance intermediaries rebuff informal requests. As Michaels has explained, "A legalistic, transactional relationship with a corporation, in which the firm cooperates only to the extent a court order or subpoena specifies, is likely to inhibit the type of open-ended, fast-moving collaboration that the intelligence agencies prefer."[117] Forcing the government to use formal legal process adds friction to what might otherwise be a smooth relationship of informal collaboration.

This procedural friction comes from two sources. First, anything more powerful than a subpoena generally requires court approval. Second, production orders for more sensitive categories of data require correspondingly higher levels of predication. The government can get basic subscriber information—the name and IP addresses associated with a particular Gmail

112. *See supra* notes 55-58 and accompanying text.

113. The main exception is when a company discloses data under a provision of the Stored Communications Act (SCA) that permits the voluntary disclosure of communications content "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." 18 U.S.C. § 2702(b)(8) (2016); *see* Stored Communications Act, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860-68 (1986) (codified as amended at 18 U.S.C. §§ 2701-2712); *see also, e.g.*, *Transparency Report Help Center: Legal Process for User Data Requests FAQs*, GOOGLE, https://perma.cc/3YM4-TSSK (archived Oct. 16, 2017) ("Sometimes we voluntarily disclose user information to government agencies when we believe that doing so is necessary to prevent death or serious physical harm to someone. The law allows us to make these exceptions, such as in cases involving kidnapping or bomb threats. Emergency requests must contain a description of the emergency and an explanation of how the information requested might prevent the harm. Any information we provide in response to the request is limited to what we believe would help prevent the harm.").

114. *Transparency Report Help Center*, *supra* note 113.

115. *See, e.g.*, *Information for Law Enforcement Authorities*, FACEBOOK, https://perma.cc/PNH9-GXLS (archived Oct. 16, 2017) (noting the various forms of legal process without which Facebook will not disclose data to the government).

116. *See* Konstantinos Stylianou et al., *Protecting User Privacy in the Cloud: An Analysis of Terms of Service*, EUR. J.L. & TECH. 15-16 (2015), https://perma.cc/42DP-XUPF.

117. Michaels, *supra* note 14, at 923.

account, for instance—merely by issuing a grand jury subpoena,[118] which it can do as long as the subpoena is neither "unreasonable [n]or oppressive."[119] If the government wants Google to disclose email headers (the time, date, and to and from addresses of the emails stored on the account), it needs to "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the . . . records . . . are relevant and material to an ongoing criminal investigation."[120] If it wants the contents of emails on the account, it will generally need a search warrant and thus will have to establish probable cause that the emails constitute "(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; [or] (3) property designed for use, intended for use, or used in committing a crime."[121] And if the government wants the ultimate in surveillance—real-time monitoring—it needs to satisfy the even higher requirements set forth in the Wiretap Act.[122]

Further, where the law is ambiguous as to what level of process is required, surveillance intermediaries often err on the side of demanding the higher level of process. For example, after the Sixth Circuit held that the government needs a warrant to compel the production of email content,[123] surveillance intermediaries treated the decision as binding nationwide.[124] The government has not sought to challenge that practice.[125]

Demanding legal process is only the first step. Surveillance intermediaries regularly push back against surveillance orders, providing the minimum

118. *See* 18 U.S.C. § 2703(c)(2).

119. *See* FED. R. CRIM. P. 17(c)(2).

120. *See* 18 U.S.C. § 2703(c)(1), (d).

121. FED. R. CRIM. P. 41(c); *see also* 18 U.S.C. § 2703(a)-(b).

122. The Wiretap Act was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968. *See* Pub. L. No. 90-351, tit. III, 82 Stat. 197, 212-25 (codified as amended at 18 U.S.C. §§ 2510-2522). Congress later amended the Wiretap Act to include electronic communications. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. I, 100 Stat. 1848, 1848-59 (codified as amended at 18 U.S.C. §§ 2510-2522). The requirements for real-time monitoring include that the crime under investigation be a federal felony, *see* 18 U.S.C. § 2516(3), or a state crime falling within the list in § 2516(2) and that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," *id.* § 2518(3).

123. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

124. *See* Brendan Sasso, *Facebook, Email Providers Say They Require Warrants for Private Data Seizures*, HILL (Jan. 25, 2013, 10:40 PM EST), https://perma.cc/N4DH-MV3C.

125. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 222 n.1 (2d Cir. 2016) (Lynch, J., concurring in the judgment) ("In the wake of *Warshak*, it has apparently been the policy of the Department of Justice since 2013 always to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process."), *cert. granted*, No. 17-2, 2017 WL 2869958 (U.S. Oct. 16, 2017).

amount of responsive data and rejecting orders they believe to be overly broad or otherwise legally deficient. For example, Yahoo reassures users that it "carefully review[s] Government Data Requests for legal sufficiency and interpret[s] them narrowly in an effort to produce the least amount of data necessary to comply with the request."[126] Similarly, Twitter notes that it "may not comply with requests for a variety of reasons" and that it "may seek to narrow requests that are overly broad."[127] Twitter remained true to its word when it challenged a Department of Homeland Security (DHS) administrative summons for user information behind the @ALT_USCIS Twitter account, which was set up after President Trump's inauguration to criticize the DHS's immigration policies.[128] In the face of Twitter's resistance, the DHS withdrew its request for the information.[129]

To be sure, companies typically comply with surveillance orders, resisting only the handful they believe to be defective (which is as it should be, given that the vast majority of orders are uncontroversial). But as a result of their scrutiny even in a minority of cases, government investigators issue fewer and more limited orders than they otherwise would, aware that their orders will be scoured for defects—real or imagined—and eager to avoid delays and fights with corporate counsel. This reality belies the common assumption that the government always gets its way and that surveillance intermediaries operate under a "regime of automatic compliance."[130]

When there are disputes, surveillance intermediaries and the government often work things out. The government can provide additional legal or factual support or, if necessary, can narrow or even withdraw a request. But when the two sides reach an impasse, intermediaries are increasingly unwilling to roll over: They fight the government in court, and they often win.

The highest-profile challenges have come from Apple contesting court orders to unlock iPhones. These orders were issued under the All Writs Act,[131] which authorizes federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[132] The Act, originally enacted as part of the Judiciary Act of 1789,

126. *Transparency Report: Frequently Asked Questions*, YAHOO, https://perma.cc/G7MV-BUCR (archived Oct. 13, 2017).

127. *Transparency Report: Information Requests*, TWITTER, https://perma.cc/K3RC-ZQ9E (archived Oct. 21, 2017).

128. *See* Jordan Brunner, *Twitter Drops Complaint Against DHS*, LAWFARE (Apr. 7, 2017, 3:38 PM), https://perma.cc/F3MU-LYFB.

129. *See id.*

130. *See* Bloch-Wehba, *supra* note 24, at 379.

131. *See* Judiciary Act of 1789, ch. 20, § 14, 1 Stat. 73, 81-82 (codified as amended at 28 U.S.C. § 1651 (2016)).

132. 28 U.S.C. § 1651(a).

grants courts "a residual source of authority to issue writs that are not otherwise covered by statute."[133] In other words, the Act fills gaps where Congress has been silent—where it has neither granted nor withheld a power that a court might need to effectuate its judgments.[134] Courts routinely invoke the All Writs Act in criminal cases to require third parties to help the government, and the Act has proven particularly important to facilitate electronic investigations, where relevant data is often held by surveillance intermediaries.

The leading authority on how the All Writs Act applies to electronic investigations is *United States v. New York Telephone Co.*, decided in 1977.[135] In *New York Telephone*, the Supreme Court held that under the Act, a court could force a telephone company to help the government install a pen register, a device that records dialed numbers.[136] In so doing, the Court developed a multifactor test to determine whether the All Writs Act permits a court to order a third party to help the government in an investigation.[137] Unfortunately, the test, which is still used today, is "frustratingly murky"[138] and hard to apply. It includes such vague factors as whether the "third party [is] so far removed from the underlying controversy that its assistance could not be permissibly compelled" and whether the assistance would be "offensive to it."[139] *New York Telephone* is overdue for a revamp, and its patchy guidance has left the courts, the government, and the private sector alike uncertain as to its scope in the digital age.

Apple first challenged a proposed All Writs Act order in a drug trafficking investigation in Brooklyn.[140] Having recovered a locked iPhone running Apple's iOS 7, the government applied for an All Writs Act order requiring Apple to extract the iPhone's unencrypted data.[141] But the magistrate judge, skeptical that the Act allowed him to issue the requested order, declined to issue it, instead inviting Apple to comment on "whether the assistance the

133. *See* Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

134. *Cf. id.* ("Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling.").

135. 434 U.S. 159 (1977).

136. *Id.* at 172, 176-78.

137. *See id.* at 174-78; *see also In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 351 (E.D.N.Y. 2016) (summarizing the *New York Telephone* factors).

138. *See* Orin Kerr, *Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case: Part 2, the All Writs Act*, WASH. POST: VOLOKH CONSPIRACY (Feb. 19, 2016), https://perma.cc/X9QZ-CXZU.

139. *See N.Y. Tel.*, 434 U.S. at 174.

140. *See In re Apple*, 149 F. Supp. 3d at 344-45, 347.

141. *See id.* at 345-46.

government seeks is technically feasible and, if so, whether compliance with the proposed order would be unduly burdensome."[142]

Apple accepted the invitation.[143] The proposed order had been drafted based on Apple's own guidance[144]—a prime example of a surveillance intermediary first demanding and then resisting compulsory process—and Apple admitted that it could carry out the order with minimal effort, as it had done at least seventy times before.[145] Nevertheless, Apple argued that the order was invalid. The company based its argument on the Communications Assistance for Law Enforcement Act (CALEA) of 1994,[146] which requires telecommunications carriers to maintain the capability to comply with certain types of law enforcement surveillance.[147] Both Apple and the government agreed that CALEA did not apply to iPhone unlocking, but they drew different conclusions from this statutory omission: The government argued that this was the kind of gap that the All Writs Act was meant to fill, while Apple argued that CALEA's silence on the issue evinced congressional intent to limit the scope of government-assistance orders and thus preempted the government's All Writs Act gambit.[148] Apple also argued that the proposed order would be impermissibly burdensome—in particular, complying with the order "could threaten the trust between Apple and its customers and substantially tarnish the Apple brand."[149] The magistrate judge ultimately held that the All Writs Act did not give courts the authority to issue an unlocking order,[150] and the government withdrew its request two months later, after a third party provided the device's passcode.[151]

Despite attracting mainstream attention,[152] the Brooklyn case was merely a sparring session compared to the brawl over the San Bernardino iPhone. That

142. *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, No. 1:15-mc-01902-JO, 2015 WL 5920207, at *1, *7 (E.D.N.Y. Oct. 9, 2015).

143. *See In re Apple*, 149 F. Supp. 3d at 347.

144. *See id.* at 346.

145. *See id.*

146. Pub. L. No. 103-414, tit. I, 108 Stat. 4279, 4279-89 (1994) (codified as amended at 47 U.S.C. §§ 1001-1010 (2015)).

147. *See* 47 U.S.C. § 1002.

148. *See In re Apple*, 149 F. Supp. 3d at 355-57.

149. *Id.* at 368-69 (quoting Apple Inc.'s Response to Court's October 9, 2015 Memorandum and Order at 4, *In re Apple*, 149 F. Supp. 3d 341 (No. 1:15-mc-01902-JO)).

150. *Id.* at 376.

151. Ellen Nakashima, *Once Again, the Government Finds a Way to Crack an iPhone Without Apple's Help*, WASH. POST (Apr. 23, 2016), https://perma.cc/5LAR-QUT9.

152. *See, e.g.*, Katie Benner & Joseph Goldstein, *Apple Wins Ruling in New York iPhone Hacking Order*, N.Y. TIMES (Feb. 29, 2016), https://perma.cc/AJ6Z-Q34G; Nicole Hong,

footnote continued on next page

iPhone ran a newer version of iOS than did the Brooklyn phone.[153] Apple had designed the newer version to prevent anyone, including Apple itself, from extracting data if the iPhone was locked.[154] But Apple did not dispute that it could still modify that specific iPhone's operating system to make it easier for the FBI to unlock the phone.[155] On the government's request, a magistrate judge in the Central District of California issued an All Writs Act order to Apple to write and install this tweaked version of iOS.[156]

Apple refused.[157] Its statutory argument was that the All Writs Act didn't authorize the court to order Apple to write the requested code.[158] As a general matter, Congress hadn't mandated such cooperation in CALEA, a decision that Apple argued was intentional and thus preempted using the All Writs Act in this case.[159] More specifically, under *New York Telephone*, the order was impermissible: Apple was unconnected to the San Bernardino attack, the government had failed to establish that it needed Apple's help to unlock the phone, and the order was too burdensome, both in terms of the resources required to comply and the security risks that Apple alleged would result.[160] Apple also made two broader constitutional arguments: The First Amendment protected it from writing what it considered objectionable computer code, and writing the code would be so burdensome that it would violate Apple's Fifth Amendment right to substantive due process.[161]

Judge Questions Legal Authority to Force Apple to Unlock iPhones, WALL ST. J. (Oct. 26, 2015, 4:11 PM ET), https://perma.cc/7SFR-M8P8.

153. *See* Memorandum of Points and Authorities, *supra* note 4, at 4 (noting that the iPhone was running iOS 9).

154. *See* Apple's Motion to Vacate, *supra* note 6, at 6.

155. Specifically, the FBI wanted Apple to write a custom version of iOS that would only be loaded on the San Bernardino iPhone and that would disable three security features that were preventing the FBI from brute-force guessing the lock code: (1) an auto-erase feature that investigators thought might have been turned on and that would have deleted the phone's contents after ten incorrect passcode attempts; (2) a requirement that passcodes be entered manually rather than electronically; and (3) a delay between passcode attempts. *See* Memorandum of Points and Authorities, *supra* note 4, at 3, 7-9.

156. *See In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016).

157. *See* Apple's Motion to Vacate, *supra* note 6, at 20.

158. *See id.* at 15-16.

159. *See id.* at 16-19.

160. *See id.* at 20-30.

161. *See id.* at 32-34.

The public reaction to the San Bernardino case was thunderous.[162] The litigation attracted over a dozen amicus briefs—an unheard-of number for a motions dispute before a magistrate judge—from technology companies, civil society groups, and law professors, as well as letters from notable figures such as the UN's special rapporteur for freedom of opinion and expression.[163] The litigation received more legal and public attention than is accorded many prominent Supreme Court cases.

The case was mooted when the FBI unlocked the phone without Apple's help (it reportedly bought a third-party unlocking tool for over a million dollars).[164] But the underlying issue hasn't gone away. The locking mechanisms on electronic devices—not just smartphones, but also laptops and tablets—increasingly impede law enforcement investigations, and not just at the federal level. For example, like many state and local law enforcement agencies, the Manhattan District Attorney's office has hundreds of inaccessible iOS devices that are hobbling investigations of drug trafficking, computer hacking, and violent crime.[165] And states, counties, and cities are even less able than is the FBI to spend a million dollars or invest hundreds or thousands of hours of technical expertise every time they come across a locked device.

Taking a broader view, the iPhone cases exemplify how difficult it's going to be (and already often is) for the government to force surveillance intermediaries to provide the "technical assistance" required of them under the government's law enforcement and foreign-intelligence authorities.[166] Courts have only begun to interpret the scope of such provisions,[167] and substantial

162. *See, e.g.*, Erich Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), https://perma.cc/4F2C-U4AU.

163. For a full list of the amicus filings and letters supporting Apple, see Press Release, Apple Inc., Amicus Briefs in Support of Apple (Mar. 2, 2016), https://perma.cc/4H9E-EJH2.

164. *See* Berman & Zapotosky, *supra* note 8.

165. N.Y. CTY. DIST. ATTORNEY'S OFFICE, REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY: AN UPDATE TO THE NOVEMBER 2015 REPORT 8-11 (2016), https://perma.cc/XC9U-7545.

166. On the law enforcement side, both the Wiretap Act and the statute governing pen registers and trap-and-trace devices permit courts to require third-party communications providers to render "technical assistance" to effectuate a wiretap or a pen register or trap-and-trace device. *See* 18 U.S.C. § 2518(4) (2016) (wiretaps); *id.* § 3124(a) (pen registers); *id.* § 3124(b) (trap-and-trace devices); *see also supra* note 122. On the foreign-intelligence side, several of FISA's provisions also compel "technical assistance." *See* 50 U.S.C. §§ 1802(a)(4)(A), 1805(c)(2)(B), 1842(d)(2)(B)(i), 1861(c)(2)(F)(vi) (2015); *see also id.* §§ 1881a(h)(1)(A), 1881b(c)(5)(B) ("information, facilities, or assistance").

167. The major case so far has come out of the Ninth Circuit, which held that the Wiretap Act's technical assistance requirement—which requires providers to render "technical assistance necessary to accomplish the interception . . . with a minimum of interference with the services" being monitored, 18 U.S.C. § 2518(4), "at least precludes total incapacitation of a service while interception is in progress," Company v. United States

footnote continued on next page

interpretive questions remain. For example, as David Kris, former Assistant Attorney General for National Security and a leading authority on foreign-intelligence law, asks: What counts as "technical assistance"?[168] "[I]s it 'technical assistance' for a provider to push down to a user's phone, with or perhaps without the user's knowledge, a software patch or program that facilitates surveillance (e.g., by covertly disabling encryption)?"[169] And "[d]oes the answer change if the software (code) is written by the government rather than the provider itself?"[170] For surveillance intermediaries, the vagueness of "technical assistance" is likely to be favorable terrain from which to mount legal challenges against government surveillance.

Potentially even more important than the iPhone cases, which were about data stored on devices, are disputes over the government's access to data in the cloud: the massive distributed network of servers that we use to store much of our data. The leading case is what has come to be known as *Microsoft Ireland*.[171] As part of a drug trafficking investigation, the government served Microsoft with a warrant under section 2703 of the Stored Communications Act (SCA),[172] which authorizes the government to compel communications service providers to produce user data.[173] The warrant ordered Microsoft to turn over data it was storing abroad in an Irish data center.[174] The Second Circuit agreed with Microsoft that in light of the presumption against extraterritoriality, the Act did not authorize the government to compel the production of foreign-stored data.[175] In October 2017 the Supreme Court granted certiorari to review the Second Circuit's decision;[176] as of this Article's publication the Court has yet to issue its decision.

(*In re* Application of the U.S. for an Order Authorizing Roving Interception of Oral Commc'ns), 349 F.3d 1132, 1145 (9th Cir. 2003).

168. David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, 8 J. NAT'L SECURITY L. & POL'Y 377, 408 (2016).

169. *Id.*

170. *Id.*

171. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016), *cert. granted*, No. 17-2, 2017 WL 2869958 (U.S. Oct. 16, 2017).

172. *See id.* at 200; *see also* Stored Communications Act, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860-68 (1986) (codified as amended at 18 U.S.C. §§ 2701-2712).

173. *See* 18 U.S.C. § 2703.

174. *Microsoft Ireland*, 829 F.3d at 200.

175. *Id.* at 201. The Supreme Court recently rearticulated the presumption against extraterritoriality: "Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." RJR Nabisco, Inc. v. Eur. Cmty., 136 S. Ct. 2090, 2100 (2016) (citing Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010)).

176. United States v. Microsoft Corp., No. 17-2, 2017 WL 2869958 (Oct. 16, 2017).

Although *Microsoft Ireland* has attracted less attention than the iPhone All Writs Act cases, it could prove an even greater check on government surveillance. As Orin Kerr explains, companies have already begun to treat it as binding nationwide precedent, both because communications over the internet "nearly always cross state lines, so it's hard to have different rules for different circuits," and because adopting the case as controlling law "put[s] the burden on the government if it wants to challenge the providers' policies."[177] If the Supreme Court affirms the Second Circuit (and if Congress does not amend the SCA to explicitly make it apply extraterritorially), *Microsoft Ireland* could hobble the government's ability to gather electronic evidence in foreign investigations.[178] It could even hamper purely domestic investigations because it would apply to the foreign-stored data of *domestic* users;[179] indeed, Microsoft admitted during the litigation that it stored data based largely on where the relevant user self-reported his location.[180]

In some cases, the government may still be able to get the data through a mutual legal assistance treaty (MLAT), which allows the United States to ask for a foreign government's help with gathering evidence that's in the other government's territory.[181] The United States has MLATs with dozens of countries,[182] including Ireland,[183] and so could theoretically have asked the Irish for the evidence at issue in *Microsoft Ireland*. But as Jennifer Daskal notes, MLATs are "slow and clumsy," and the United States has them with only about half of the world's countries.[184] And in some cases, a surveillance intermediary's data storage architecture can make it impossible for any country's process to apply. For example, although Google stores some of its users' email abroad,

177. *See* Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, WASH POST: VOLOKH CONSPIRACY (Nov. 29, 2016), https://perma.cc/7Z5C-JBBG.

178. *See* Letter from Peter J. Kadzik, Assistant Attorney Gen., U.S. Dep't of Justice, to Joseph R. Biden, President, U.S. Senate 2-3 (July 15, 2016), https://perma.cc/6RWY-2RTF.

179. *See* Jennifer Daskal, *Three Key Takeaways: The 2d Circuit Ruling in the Microsoft Warrant Case*, JUST SECURITY (July 14, 2016, 6:28 PM), https://perma.cc/2KFC-9S2C ("[*Microsoft Ireland*] means that US law enforcement can no longer compel, via a lawfully obtained warrant, a US-based provider to turn over the emails of a US citizen being investigated in connection with a New York City murder if his or her data happens to be stored on a server outside the United States territory. Rather, it must make a diplomatic request for the data in whatever place the data happens to be stored. And then wait—perhaps months or longer—for a response.").

180. *See Microsoft Ireland*, 829 F.3d at 230 (Lynch, J., concurring in the judgment).

181. *See* Woods, *supra* note 32, at 748-49.

182. 2 BUREAU FOR INT'L NARCOTICS & LAW ENF'T AFFAIRS, U.S. DEP'T OF STATE, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT 20 (2016), https://perma.cc/2TWX-SPZE.

183. Treaty on Mutual Legal Assistance in Criminal Matters, Ir.-U.S., Jan. 18, 2001, T.I.A.S. No. 13,137.

184. Daskal, *supra* note 32, at 393-94.

only Google's U.S.-based employees can access it.[185] Under *Microsoft Ireland* the United States couldn't force Google to turn over foreign-stored emails, but nor could it use an MLAT with the foreign country in which the data is stored because the foreign country might lack jurisdiction over Google's U.S. employees.[186] For such data, this arrangement creates a warrant black hole.[187]

Although companies usually litigate on their own behalf (as in the cases described above), they can sometimes also challenge government surveillance on behalf of their users. Yahoo set an important early precedent when, in 2007, it challenged a foreign intelligence surveillance order issued under FISA.[188] Yahoo's main argument was that the order violated its users' Fourth Amendment rights.[189] Although the FISA appeals court rejected Yahoo's challenge, it affirmed that Yahoo had standing to raise the Fourth Amendment rights of its users.[190]

The Yahoo case is important because individuals themselves will often lack standing to challenge a surveillance program. In *Clapper v. Amnesty International USA*, the Supreme Court held that plaintiffs could not establish standing to challenge a surveillance program absent concrete knowledge that they were targets of the surveillance.[191] *Clapper* invoked the corporate standing that the FISA appeals court granted Yahoo to defend against the charge that its parsimonious approach to individual standing "insulate[d] [section 702] from judicial review."[192] And although the Yahoo case relied in part on specific language in FISA,[193] the decision could become an important general precedent in future surveillance cases if courts take a broad reading of its permissive approach to vindicating third-party rights.

185. *See* Kerr, *supra* note 177.

186. *See id.*

187. *See id.*

188. *See In re* Directives to Yahoo! Inc., No. 08-01, 2008 WL 10632524, at *2 (Foreign Intelligence Surveillance Ct. of Review Aug. 22, 2008). The officially reported version of the case redacted Yahoo's identity. *See In re* Directives [Redacted Text], 551 F.3d 1004 (Foreign Intelligence Surveillance Ct. of Review 2008). In 2014 the government released, on the intelligence community's official Tumblr account, a less-redacted version of the opinion identifying Yahoo. *See* Office of the Dir. of Nat'l Intelligence, *Statement by the Office of the Director of National Intelligence and the U.S. Department of Justice on the Declassification of Documents Related to the Protect America Act Litigation*, IC ON THE RECORD (Sept. 11, 2014, 6:31 PM), https://perma.cc/D9K4-7JGU.

189. *See In re Directives to Yahoo!*, 2008 WL 10632524, at *3-4.

190. *See id.* at *3-4, *13.

191. *See* 133 S. Ct. 1138, 1148, 1155 (2013).

192. *Id.* at 1154.

193. *See In re Directives to Yahoo!*, 2008 WL 10632524, at *3.

Finally, in addition to challenging surveillance orders directly, surveillance intermediaries also fight for the right to publicize information about those orders. For example, Twitter has (unsuccessfully) sued the government for the right to publicize the number of national security requests it receives.[194] And Microsoft has argued that the SCA's nondisclosure provision—under which the government can block companies from telling their users that the government has demanded their data—violates its own and its users' constitutional rights.[195]

Although the scorecard has been uneven, litigation successes like the Brooklyn All Writs Act case and *Microsoft Ireland* demonstrate that challenging the government in court can be a powerful way for surveillance intermediaries to resist government surveillance. But there are also indirect benefits to litigating against the government, even when companies lose. First, litigation signals a surveillance intermediary's commitment to user privacy. For example, every year the Electronic Frontier Foundation (EFF) issues an influential "Who Has Your Back?" scorecard of technology companies' willingness to fight government surveillance requests; for years this scorecard awarded points to companies merely for litigating against the government, whether or not the company won.[196] Second, litigation creates focal points around which public pressure can coalesce. One example is Microsoft's brief in the *Microsoft Ireland* litigation, which opened with a dramatic thought experiment about a German warrant for the letters of a *New York Times*

194. *See* Twitter, Inc. v. Holder, 183 F. Supp. 3d 1007, 1009, 1014 (N.D. Cal. 2016). Twitter argued that government restrictions on publishing aggregate data violated the First Amendment. *Id.* at 1009. Because such data is classified, the district court rejected Twitter's argument, holding that "[t]he First Amendment does not permit a person subject to secrecy obligations to disclose classified national security information." *Id.* at 1014. The district court nevertheless gave Twitter leave to amend its complaint to challenge the underlying classification decision. *Id.*

195. *See* Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 895-97 (W.D. Wash. 2017); *see also* 18 U.S.C. §§ 2703, 2705(b) (2016). In the wake of that lawsuit, the Department of Justice adopted a policy ending the routine use of nondisclosure orders when issuing SCA orders. The new policy led Microsoft to drop the lawsuit. *See* Ellen Nakashima, *Justice Department Moves to End Routine Gag Orders on Tech Firms*, WASH. POST (Oct. 24, 2017), https://perma.cc/4YHN-HYZ6.

196. *See* NATE CARDOZO ET AL., ELEC. FRONTIER FOUND., WHO HAS YOUR BACK?: PROTECTING YOUR DATA FROM GOVERNMENT REQUESTS 16 (2014), https://perma.cc/S57C-AL3Y; NATE CARDOZO ET AL., ELEC. FRONTIER FOUND., WHO HAS YOUR BACK?: WHICH COMPANIES HELP PROTECT YOUR DATA FROM THE GOVERNMENT? 13-14 (2013), https://perma.cc/UEA3-4UT3; MARCIA HOFMANN ET AL., ELEC. FRONTIER FOUND., 2012: WHEN THE GOVERNMENT COMES KNOCKING, WHO HAS YOUR BACK? 10 (2012), https://perma.cc/677T-KJEJ.

reporter;[197] this portion of the brief was clearly written with a public audience in mind, and the media covered it accordingly.[198] Another example is the iPhone unlocking cases, which have spurred public awareness of encryption more effectively than could ever have been accomplished by a public relations campaign.

Although any surveillance intermediary can litigate a government order, the biggest companies are best positioned to fight it out. Unlike small companies, they have the money for protracted litigation. And as repeat players, they have a key advantage over one-shot litigants: They have the luxury of choosing the best vehicle for a legal argument. For example, Apple could wait to challenge an All Writs Act iPhone unlocking order until the magistrate judge in Brooklyn invited it to do so. Finally, the size and multinational reach of the biggest surveillance intermediaries give them an additional argument in litigation: that they would incur such reputational and market costs from complying with U.S. government surveillance that such orders would be unreasonably burdensome.[199]

B. Technological Unilateralism

Legal resistance is a useful tool, but it's no panacea. Its flaw is that it requires someone else (the courts) to agree that the resistance is appropriate. Companies can avoid this problem of third-party reliance by embracing *technological unilateralism*: making technological changes to their systems irrespective of (if not intentionally adverse to) the government's preferences.

Contrary to a common misperception,[200] U.S. law does not force communications companies generally to design their systems to enable government surveillance. CALEA, which requires companies to comply with law enforcement requests, applies only to a narrow category of mostly traditional

197. *See* Brief for Appellant at 1, Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016) (No. 14-2985), 2014 WL 7004807.

198. *See, e.g.*, Dominic Rushe, *Privacy Is Not Dead: Microsoft Lawyer Prepares to Take on US Government*, GUARDIAN (Dec. 14, 2014, 11:05 EST), https://perma.cc/2WET-CMTR (describing the thought experiment).

199. The magistrate judge in the Brooklyn All Writs Act case embraced this argument. *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 369-71 (E.D.N.Y. 2016). As Kris notes, Apple's reputational argument in the case, if "[t]aken to its logical conclusion, . . . might mean that a provider could create its own undue burden by strongly and publicly opposing assistance with governmental surveillance." Kris, *supra* note 168, at 408.

200. *See, e.g.*, Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 7-8, 8 n.33 (2008) (citing CALEA for the proposition that "the government now requires that new communications technologies be designed with back ends that facilitate government surveillance").

telecommunications companies and excludes services like email, messaging, or video calling[201]—a major part of modern communications. CALEA also allows companies to implement end-to-end encryption into their services.[202]

The internet—its physical infrastructure and the software and hardware that run on top of it—is controlled by private companies, who can do almost anything they want with it. And one consequence of the architectural choices they've made is what the FBI and other federal, state, and local law enforcement agencies refer to as the "going dark" problem: the inability of law enforcement to access communications for technical reasons, even when they have the lawful authority (such as a warrant or other legal process) to do so.[203]

Of all the technological changes frustrating surveillance efforts, encryption has attracted the most attention. For two parties to encrypt a communication session, they must first agree on a shared key, often called the session key.[204] The sender uses the session key to encrypt the communication, and the recipient uses the same key to decrypt it.[205] The process of agreeing on a session key without a malicious third party gaining access to it—commonly known as the problem of key exchange—generally requires complex protocols.[206] For this reason, encrypted-communications platforms

201. *See* 47 U.S.C. § 1002(a) (2015) (limiting the capability requirements to "telecommunications carrier[s]"); *id.* § 1001(8) (defining "telecommunications carrier" to exclude "persons or entities insofar as they are engaged in providing information services"); *id.* § 1001(6) (defining "information services" to include "electronic messaging services").

202. *See id.* § 1002(b)(3) ("A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier *and the carrier possesses the information necessary to decrypt the communication.*" (emphasis added)).

203. *See* Comey, *supra* note 53, at 2 (capitalization altered). As noted above, I am not arguing that law enforcement's *overall* position with respect to technology is that of going dark. *See supra* note 53 and accompanying text. Rather, my point is that with respect to the particular technological developments discussed here, law enforcement has experienced a meaningful decrease in its ability to access communications and personal data.

204. *See, e.g.*, KEITH M. MARTIN, EVERYDAY CRYPTOGRAPHY: FUNDAMENTAL PRINCIPLES & APPLICATIONS 392 (2d ed. 2017).

205. Such encryption algorithms are called symmetric ciphers because the same key is used for encryption and decryption. Symmetric ciphers perform the vast bulk of encryption. *See id.* at 24-25, 392-93. The leading standard high-performance symmetric cipher, the Advanced Encryption Standard, *see id.* at 139, is used, for example, to encrypt iPhones. *See* Apple, iOS Security: iOS 10, at 7, 10 (2017), https://perma.cc/XMQ6-E9LL.

206. *See* MARTIN, *supra* note 204, at 25-27. Key exchange in Transport Layer Security, the current standard for secure web browsing, uses public-key cryptography (often Rivest-Shamir-Adleman, or RSA) for the exchange of session keys and digital certificates for authentication. *See* ILYA GRIGORIK, HIGH-PERFORMANCE BROWSER NETWORKING 53 (2d release 2014).

automatically handle key exchange behind the scenes.[207] Some go further and actually keep a copy of the keys (or some other method to decrypt the communications).[208] In such cases three entities (at least) can decrypt the communication: the sender, the recipient, and the third party that handled the key exchange.

Companies have good reasons to maintain third-party access to their customers' data.[209] Silicon Valley's dominant business model relies on selling user data. It is by now well understood that nothing on the internet is truly "free"; as Apple's Tim Cook has explained, "[W]hen an online service is free, you're not the customer. You're the product."[210] Thus, services like those provided by Google and Facebook have generally made money by scanning user communications to generate targeted ads.[211]

Third-party access can also make for better products, enabling companies to let users recover lost passwords or search their hosted data. Third-party access can also increase system security. For example, like many webmail providers, Google scans incoming email messages for malware.[212] Were Google unable to access user emails (whether by decrypting them or storing them in unencrypted form), it would find it harder to perform this important,

207. *See, e.g.*, WhatsApp, WhatsApp Encryption Overview 4 (2017) (describing WhatsApp's key exchange protocol), https://perma.cc/X7G7-9F76.

208. *See, e.g.*, Kurt Wagner, *Is Your Messaging App Encrypted?*, RECODE (Dec. 21, 2015, 4:30 AM EST), https://perma.cc/5YF7-6SK2 (noting that Google keeps encryption keys for messages sent via its Hangouts service and that Snapchat does the same for its platform).

209. Some commentators have cited the business advantages of third-party access as evidence of a natural ceiling for end-to-end encryption. *See* The Berkman Ctr. for Internet & Soc'y at Harvard Univ., Don't Panic.: Making Progress on the "Going Dark" Debate 10-12 (2016), https://perma.cc/3756-ATNK. Even if this is the case, it will still, as the intelligence community has pointed out, leave many avenues for malicious actors to take advantage of those encrypted services that do not allow third-party access. *See* Letter from Deirdre M. Walsh, Dir. of Legislative Affairs, Office of the Dir. of Nat'l Intelligence, to Senator Ron Wyden 1-2 (May 5, 2016), https://perma.cc/379S-KGMR.

210. TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS 335 (2016) (quoting an open letter from Tim Cook previously published on Apple's website).

211. *See supra* note 79 and accompanying text. Notably, Google has announced that it will no longer scan the contents of user emails to serve targeted advertisements. *See* Daisuke Wakabayashi, *Google Will No Longer Scan Gmail for Ad Targeting*, N.Y. TIMES (June 23, 2017), https://perma.cc/HV5N-2P95. Whether other electronic communications services follow suit remains to be seen.

212. Google, Privacy Policy 2 (2017), https://perma.cc/H9GV-AWY7 ("Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.").

security-enhancing service. These examples show why the standard framing of encryption as a "privacy vs. security" issue is incorrect. Just as some privacy-security tradeoffs are better framed as "privacy-privacy tradeoffs,"[213] the debate over encryption might be better conceptualized as a *security-security tradeoff*.

The alternative to letting third parties decrypt communications is known as *end-to-end encryption*: Only the sender and the recipient (the "ends" of the communication) can decrypt the message.[214] The third party handles secure key exchange but doesn't keep a copy of the decryption keys.[215] This model is used by end-to-end encrypted "data in motion" services—like Apple's iMessage, Facebook's WhatsApp, and services like Signal and Telegram that emphasize privacy as their number-one feature.[216] "Data at rest" storage can also be end-to-end encrypted. Here, the user is first the sender (when she encrypts the data) and later the recipient (when she decrypts and accesses it). If only the user who created a device's passcode can unlock the device and decrypt its stored data, the device is end-to-end encrypted—as, for example, are the latest Apple iPhones.[217]

Companies use end-to-end encryption for several reasons. First, the consensus in the academic and commercial information-security communities is that an end-to-end encrypted system is, all else being equal, more secure than a system in which a third party has access to the underlying data—whether by having access to the cryptographic keys (an arrangement known as "key

213. *See* David E. Pozen, Essay, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 221-22 (2016); *see also, e.g.*, BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES; CONFRONTING A NEW AGE OF THREAT 123-48 (2015).

214. *See* The Berkman Ctr. for Internet & Soc'y at Harvard Univ., *supra* note 209, at 4. This should not be confused with another use of the term "end-to-end encryption," which refers to a system that ensures that the communication is encrypted along the entire communication path from sender to recipient. *See, e.g.*, Joris V.J. van Hoboken & Ira S. Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 ME. L. REV. 487, 516 (2014); The Chertoff Grp., The Ground Truth About Encryption and the Consequences of Extraordinary Access 5 (2016), https://perma.cc/Q3LT-2N8N. Such encryption, which could more accurately be called full-transit encryption, is unrelated to end-to-end encryption as that term is commonly used. For instance, a Gmail message could be encrypted through the entire communication from one Gmail user to another, and thus enjoy full-transit encryption, while not being end-to-end encrypted because Google could decrypt the message.

215. *See* The Berkman Ctr. for Internet & Soc'y at Harvard Univ., *supra* note 209, at 4.

216. *See End-to-End Encryption*, WHATSAPP, https://perma.cc/2QAT-JACC (archived Nov. 17, 2017); *Our Approach to Privacy*, APPLE, https://perma.cc/UX3T-EX8N (archived Nov. 16, 2017); SIGNAL, https://perma.cc/34V9-BF7F (archived Nov. 17, 2017); *Telegram FAQ*, TELEGRAM, https://perma.cc/DXP9-8JJ8 (archived Nov. 17, 2017).

217. *See* Apple, *supra* note 205, at 7, 10-18.

escrow") or by some other method.[218] This is in large part because third-party-access systems are far more complicated to implement and thus run afoul of the information security axiom that "complexity is the enemy of security."[219]

Second, companies can use end-to-end encryption to signal privacy bona fides and thus gain market share. The traditional way for a company to convince users that it cares about their privacy is through a terms-of-service agreement that restricts how it can use their data. Terms of service, however, are a weak form of self-restraint because companies can alter them, including by reversing previous commitments not to access certain data. Deploying end-to-end encryption is a more credible form of self-binding; it guarantees on the basis of mathematics—not just law or commercial practice—that the company will never access its users' encrypted data. End-to-end encryption thus effectively signals that a company takes user privacy seriously. So it's not surprising to see a company like Apple, which relies less on monetizing data than competitors like Google or Facebook, proudly declaring: "We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business."[220] Apple's Tim Cook has been particularly critical of "some of the most prominent and successful companies" for "buil[ding] their businesses by lulling their customers into complacency about their personal information."[221] As Tim Wu has noted, it doesn't "take an MBA to notice that Apple's defense of individual privacy [is] also an assault on the principal revenue scheme of its competitors."[222]

Third, end-to-end encryption gives companies something akin to an impossibility defense when responding to government orders for data, at least when the data has already been end-to-end encrypted. The difference between the two iPhone All Writs Act cases offers a useful illustration. The data the FBI sought on the Brooklyn iPhone was not end-to-end encrypted.[223] Thus, Apple could easily have complied with an All Writs Act order (as it had done many times before[224]). By contrast, the data the FBI sought from the San Bernardino

218. *See, e.g.*, ABELSON ET AL., *supra* note 31, at 18-20; The Chertoff Grp., *supra* note 214, at 5-6.

219. *Cf., e.g.*, Ronald L. Rivest, *On the Notion of "Software Independence" in Voting Systems*, 366 PHIL. TRANSACTIONS ROYAL SOC'Y A 3759, 3760 (2008) ("It is a common maxim that complexity is the enemy of security and accuracy, thus it is very difficult to evaluate a complex system.").

220. *See* Cook, *supra* note 7.

221. *See* Andrew Griffin, *Apple Boss Tim Cook Slams Google and Facebook for Selling Users' Data*, INDEPENDENT (June 3, 2015, 3:12 PM BST), https://perma.cc/6MSX-BQ7U (quoting a speech by Tim Cook).

222. WU, *supra* note 210, at 336.

223. *See* Apple Inc.'s Response to Court's October 9, 2015 Memorandum and Order, *supra* note 149, at 3.

224. *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 346 (E.D.N.Y. 2016).

iPhone was end-to-end encrypted.[225] This meant that Apple could not have complied with an order for data even if it had wanted to. The best it could have done was build a custom operating system that, by disabling certain other security features, would have made it easier for the FBI to access the data in decrypted form—but even then with no guarantee of success.[226] Thus, broadly deploying end-to-end encryption gives companies litigation advantages.

End-to-end encryption, however, is not the only technical change that can frustrate government surveillance.[227] Companies are increasingly adopting *forward secrecy*, a system of secure key exchange such that if a particular key exchange is compromised, only the corresponding, and not any previous, session key is exposed (and thus only that communication session, and not any previous session, can be decrypted).[228] Outside of encryption, companies may choose not to store content or metadata that law enforcement seeks.[229] Or they may simply fail to create the capabilities or invest the resources necessary to respond to surveillance orders quickly or at all, a serious problem for surveillance requests seeking real-time data.[230] Finally, companies may simply

225. *See* Apple's Motion to Vacate, *supra* note 6, at 5-6.

226. *See id.* at 12-13.

227. *See Encryption Technology and Potential U.S. Policy Responses: Hearing Before the Subcomm. on Info. Tech. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 5 (2017) (statement of Amy S. Hess, Exec. Assistant Dir., FBI) ("[W]e obtain the proper legal authority to intercept and access communications and information, but we increasingly lack the technical ability to do so. This problem, which we refer to as 'going dark,' is broader and more extensive than just encryption . . . ."); The Berkman Ctr. for Internet & Soc'y at Harvard Univ., *supra* note 209, at 4 ("[T]he going dark problem encompasses a range of architectural changes that impede government access . . . .").

228. *See* COLIN BOYD & ANISH MATHURIA, PROTOCOLS FOR AUTHENTICATION AND KEY ESTABLISHMENT 50 (2003); *see also, e.g.*, @j4cob, *Forward Secrecy at Twitter*, TWITTER (Nov. 22, 2013), https://perma.cc/A6D4-HU7R (noting Twitter's adoption of forward secrecy); Glenn Fleishman, *WhatsApp Outpaces iMessage on Verification and Forward Secrecy*, MACWORLD (Apr. 11, 2016, 4:45 AM PT), https://perma.cc/7K9U-BSBG (noting WhatsApp's adoption of forward secrecy).

229. This problem led the European Union in 2006 to adopt the Data Retention Directive, which required electronic communications providers to preserve traffic data for emails and phone calls. *See* Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 CHI. J. INT'L L. 233, 238 (2007). The Directive was invalidated in 2014 by the European Court of Justice, *see* Joined Cases C-293/12 & C-594/12, Dig. Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res., ECLI:EU:C:2014:238, ¶¶ 1, 71 (Apr. 8, 2014), https://perma.cc/SHY6-CZFG, but many European countries still have the domestic data-retention laws that were passed as part of the Directive's first round of national implementation. *See* Privacy Int'l, National Data Retention Laws Since the CJEU's *Tele-2/Watson* Judgment: A Concerning State of Play for the Right to Privacy in Europe 12 (2017), https://perma.cc/ZY8E-4V7Z.

230. *See* Comey, *supra* note 53, at 2-3 ("[A]n order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some can't comply, because they have not developed interception capabilities. Other providers want to provide assistance, but

footnote continued on next page

refuse to allow the government access to their platforms. Facebook, Instagram, and Twitter have all cut off data access to developers that share information with law enforcement for surveillance purposes.[231]

Another approach is to make architectural changes that take advantage of legal, rather than technological, impediments to surveillance. For example, if a company chooses not to store any data, the government will have to resort to real-time wiretaps, which carry higher procedural requirements.[232] Another example is encryption itself; one scholarly debate asks whether merely encrypting a communication is enough to raise a reasonable expectation of privacy in it, thus triggering Fourth Amendment protections.[233]

For law enforcement, the most pressing such example is the *Microsoft Ireland* decision discussed in Part II.A above. Microsoft's decision to store user data in Ireland forced the United States to litigate a tricky legal issue regarding the jurisdictional reach of the SCA, the main statute governing law enforcement access to stored electronic data.[234] As Zachary Clopton notes, "[E]ven though the physical locations of data may be certain, those locations may be completely disconnected from any relevant interest of the technology's users or regulators"—here, the United States's interest in accessing data pursuant to a lawful criminal investigation—and "[t]echnology may also allow regulated entities to cheaply evade territorial rules."[235] Indeed, companies

they have to build interception capabilities, and that takes time and money."); Sally Q. Yates, Acting Deputy Attorney Gen., U.S. Dep't of Justice, Remarks at the Association of State Criminal Investigative Agencies Spring Conference (May 4, 2015), https://perma.cc/NC9N-VEJH (highlighting the situation where "the company that developed the service did not include in its design the capability to comply with the court order").

231. *See* Elizabeth Dwoskin, *Facebook Says Police Can't Use Its Data for "Surveillance,"* WASH. POST (Mar. 13, 2017), https://perma.cc/HZ4D-NB47.

232. *Cf.* Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 356 (2011) (noting that in the context of services like Facebook that do store data, "investigators could circumvent the high procedural hurdles presented by the Wiretap Act by simply waiting long enough to avoid the contemporaneity requirement and then retrieving the same information").

233. *Compare id.* at 371-72 ("[A] company with resources like Facebook could encrypt data and make privacy expectations higher than any other form of communication."), *with* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503, 505 (2001) ("[E]ncryption cannot create Fourth Amendment protections because the Fourth Amendment regulates government *access* to communications, not the *cognitive understanding* of communications already obtained.").

234. *See supra* notes 171-80 and accompanying text.

235. Zachary D. Clopton, Essay, *Territoriality, Technology, and National Security*, 83 U. CHI. L. REV. 45, 49 (2016). The reverse is also a problem: When companies store data in the United States, they prevent other countries from easily accessing it. This is because domestically stored data is subject to the restrictions of the Wiretap Act, the SCA, and

footnote continued on next page

routinely leave the decision where to store data to users, allowing them to forum shop with the ease of a drop-down menu.[236]

Microsoft Ireland illustrates another architectural technique, one that raises the political costs of government surveillance. Even if the executive branch wins the fight over the extraterritorial application of the SCA—whether by prevailing at the Supreme Court in *Microsoft Ireland* or convincing Congress to amend the law—Microsoft, by storing relevant data in Ireland, will have made it harder for the government to conduct surveillance. This is because the government pays a diplomatic cost whenever it demands data that is located in—and thus implicates the sovereignty of—a foreign state. This was on display in Ireland's amicus brief in the litigation, which (politely) suggested that a U.S. court order for Microsoft to produce data stored in Ireland could be an "infringement[] by [an]other state[] of its sovereign rights with respect to its jurisdiction over its territory."[237] Because many other surveillance intermediaries are building data centers in Europe,[238] these diplomatic costs will likely rise across the board.

---

the statute governing pen registers and trap-and-trace devices, all of which limit the ability of communications providers to share user data with third parties, including in response to lawful foreign process. 18 U.S.C. § 2511(1)(c) (2016) (Wiretap Act); *id.* § 2702(a)(2) (SCA); *id.* § 3121(a) (pen registers and trap-and-trace devices). To resolve this problem, the United States has negotiated a potential agreement with the United Kingdom that would, in concert with changes to U.S. law, let the United Kingdom serve process directly on U.S. companies. *See* Jennifer Daskal & Andrew Keane Woods, *Congress Should Embrace the DOJ's Cross-Border Data Fix*, LAWFARE (Aug. 1, 2016, 8:52 AM), https://perma.cc/K585-Y7LC (noting that the "agreement would permit UK law enforcement to make direct requests to US-based providers"); Letter from Peter J. Kadzik to Joseph R. Biden, *supra* note 178, at 1.

236. *See, e.g.*, Aaron Levie, *Introducing Box Zones: Building a Global Cloud*, BOX BLOGS (Apr. 11, 2016), https://perma.cc/JAW4-KA64 ("Box Zones enables businesses around the globe to adopt Box as their modern content management platform, while letting them store their data in the region of their choice . . . .").

237. Brief of Amicus Curiae Ireland at 1, Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016) (No. 14-2985); *see also* Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament at 8, *Microsoft Ireland*, 829 F.3d 197 (No. 14-2985), 2014 WL 7277561 ("European citizens are highly sensitive to the differences between European and U.S. standards on data protection. Such concerns are frequently raised in relation to the regulation of cross-border data flows and the mass-processing of data by U.S. technology companies. The successful execution of the warrant at issue in this case would extend the scope of this anxiety to a sizeable majority of the data held in the world's datacenters outside the U.S. (most of which are controlled by U.S. corporations) and would thus undermine the protections of the EU data protection regime, even for data belonging to an EU citizen and stored in an EU country.").

238. *See* Mark Scott, *U.S. Tech Giants Are Investing Billions to Keep Data in Europe*, N.Y. TIMES (Oct. 3, 2016), https://perma.cc/C868-X8LB.

Similarly, surveillance intermediaries can raise the political costs of government surveillance when they leave the government no choice but to use more controversial methods. For example, several of the security researchers who authored a prominent critique of government data-access mandates for encrypted systems[239] had previously argued that the government should instead "exploit the rich supply of security vulnerabilities already existing in virtually every operating system and application to obtain access to communications of the targets of wiretap orders."[240] But when the government exploits vulnerabilities and hacks endpoint devices, it risks controversy and backlash, especially if the government doesn't also tell companies about their products' bugs.[241]

To summarize, surveillance intermediaries can use technical changes to their system architectures to frustrate government surveillance in three ways: by increasing surveillance's technical, legal, and political costs. And although any surveillance intermediary can frustrate government surveillance in these ways, the largest companies have three advantages.

First, the largest companies have the resources to make secure products better and, in particular, more user-friendly. It's important to recognize that the technology for encrypting communications has been available for decades. Pretty Good Privacy (PGP), one of the first widely available programs for email encryption, was released in 1991.[242] More recently, the Tor Project lets anyone

239. *See* ABELSON ET AL., *supra* note 31, at 1.

240. Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 5 (2014).

241. In the wake of the 2014 discovery of the Heartbleed bug and amid broad suspicion that the NSA knew about this major vulnerability in the widely used OpenSSL standard for encrypted web traffic, the head of the National Security Council's cybersecurity directorate described the government's "disciplined, rigorous and high-level decision-making process for vulnerability disclosure." Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, WHITE HOUSE (Apr. 28, 2014, 3:00 PM ET), https://perma.cc/PNN8-J4JC. Through the Freedom of Information Act, the EFF acquired the document outlining the process for disclosing vulnerabilities in "commercial information technology or industrial control products or systems (to include both hardware or software)." Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process 1 (n.d.), https://perma.cc/N3PX-5DZ7; *see* EFF v. NSA, ODNI—*Vulnerabilities FOIA*, ELEC. FRONTIER FOUND., https://perma.cc/S6BH-RWVP (archived Nov. 8, 2017) (describing the EFF's efforts to obtain the process document). In November 2017, the government released updated information about the disclosure process. *See* Rob Joyce, *Improving and Making the Vulnerability Equities Process Transparent Is the Right Thing to Do*, WHITE HOUSE (Nov. 15, 2017, 9:11 AM ET), https://perma.cc/CXU3-QJ72.

242. D. Atkins et al., PGP Message Exchange Formats 2 (1996), https://perma.cc/GM4M-68CD.

browse the web anonymously merely by downloading a free web browser.[243] Yet regular internet users don't use PGP and Tor because both systems are difficult to use.[244] This may reflect the fact that open-source projects frequently lack the resources and organization to make their products sufficiently user-friendly for widespread adoption.[245] By contrast, companies like Apple or WhatsApp have the money and talent to build end-to-end encryption into their services so seamlessly that users communicate securely without even realizing it.

Second, multinational companies have both the global infrastructure and plausible business reasons to store data overseas, where it may be more difficult—for technological, legal, or political reasons—for the government to access. For example, Microsoft's worldwide network of data centers makes it very easy for it to offshore data that it would otherwise store domestically. Microsoft's size and multinational user base give it credible justifications to store the data abroad—justifications that have nothing to do with U.S. surveillance. Foreign customers may prefer that their data be physically located in their own countries. And Microsoft's network may run more efficiently if it can store data physically near the data's user, or even dynamically shift data around the network depending on network congestion.

Third, large companies can push out architectural changes to large numbers of users around the world. For example, when WhatsApp implemented end-to-end encryption, over a billion people, both in the United States and abroad, suddenly gained a strong defense against government surveillance.[246] For the same amount of technological work, large companies can make surveillance much more difficult than can services with small user bases. This is particularly true because companies tend to enable end-to-end encryption by default and the vast majority of users never bother to change those (or any other) default settings.[247]

---

243. *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1087 (2017).

244. *See, e.g.*, Alma Whitten & J.D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE 669, 670 (Lorrie Faith Cranor & Simson Garfinkel eds., 2005) (concluding that PGP "is not usable enough to provide effective security for most computer users"). Tor is easier to use than PGP, but its quirks can still trip up casual users. *See* Jeremy Clark et al., *Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability*, *in* PROCEEDINGS OF THE THIRD SYMPOSIUM ON USABLE PRIVACY AND SECURITY 41, 41, 51 (2007). And of course, the dark web is its own kind of wilderness.

245. *See* David M. Nichols & Michael B. Twidale, *The Usability of Open Source Software*, FIRST MONDAY (Jan. 6, 2003), https://perma.cc/Q29G-Q9GS ("Open source projects lack the resources to undertake high quality usability work.").

246. *See* Metz, *supra* note 91.

247. *See* Charles Arthur, *Why the Default Settings on Your Device Should Be Right First Time*, GUARDIAN (Dec. 1, 2013, 3:00 EST), https://perma.cc/A5KC-HV6N.

Critically, these changes quickly become facts on the ground. As historians and social theorists of technology have long recognized, technology is highly path dependent.[248] It is thus often expensive to undo earlier architectural decisions.[249] And because the government is slow to regulate technology,[250] technology companies can deploy services to a vast number of consumers years before the government can catch up. Combined with the endowment effect—the psychological tendency to value something more when you possess it[251]—this means that consumers will perceive a government rollback of encryption or some other security feature as a greater burden than they would if the government had prevented the spread of the technology in the first place.[252]

C. Policy Mobilization

As we've seen, surveillance intermediaries can use legal and technological resistance to challenge the government's implementation of existing surveillance policy. But in the long run, the most effective (although harder) approach is to change the policy itself.

Surveillance intermediaries have the clout to shape surveillance policy in part because they enjoy high status with both officials and the general public. Apple, Amazon, Alphabet (Google), Facebook, and Microsoft are all in the top ten of *Fortune*'s list of the "world's most admired companies."[253] At least in the Obama Administration, senior government officials, from the President on down, routinely pilgrimaged to Silicon Valley to parley with tech industry leaders.[254] More generally, Silicon Valley is like the factories of the post-World War II industrial boom or the railroads in their late nineteenth century golden

248. *See* LANGDON WINNER, THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY 2-29 (1986).

249. *See* COHEN, *supra* note 101, at 181; The Chertoff Grp., *supra* note 214, at 6.

250. *See* Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES L. 369, 396-97 (2016).

251. *See generally* Russell Korobkin, *The Endowment Effect and Legal Analysis*, 97 NW. U. L. REV. 1227, 1228-29, 1250 (2003) (describing the endowment effect).

252. *See* Julian Sanchez, *Feinstein-Burr 2.0: The Crypto Backdoor Bill Lives On*, JUST SECURITY (Sept. 9, 2016, 2:06 PM), https://perma.cc/XM3F-JJ9Q. This is the flip side to an argument made by Peter Swire and Kenesa Ahmad: that law enforcement's panic over end-to-end encryption is not because of any danger of actually "going dark" but rather because agencies are overreacting to the loss of a current surveillance capability while ignoring their net gain from technology. *See* Swire & Ahmad, *supra* note 53, at 463-73.

253. *World's Most Admired Companies*, FORTUNE, https://perma.cc/YJ42-6XXZ (archived Oct. 14, 2017) (capitalization altered).

254. *See, e.g.*, Doug Gross, *Photo Shows Obama at Dinner with Steve Jobs, Mark Zuckerberg*, CNN (Feb. 18, 2011, 1:45 PM EST), https://perma.cc/E9UC-PX3N; Ellen Nakashima, *Obama's Top National Security Officials to Meet with Silicon Valley CEOs*, WASH. POST (Jan. 7, 2016), https://perma.cc/3NZF-JDW2.

age: an industry that dominates economically—and, critically, *culturally*—and one that is perceived as a key engine of economic growth. When Silicon Valley speaks, the country listens, attentively and enthusiastically. Despite a recent growing concern over technology giants' outsize role in politics and the economy,[255] the technology industry, unlike many others, has successfully marketed itself as a culturally and politically progressive force. Google's famous "Don't Be Evil" commandment is emblematic of this carefully crafted self-presentation.[256] When Goldman Sachs or Monsanto urges us to support something, that's enough to cause many of us to oppose it; when Apple's CEO denounces a technical assistance order, many of the same corporate skeptics quickly fall in line.

Despite being by far the largest collectors of our personal information, technology companies have effectively portrayed themselves as champions of user privacy in the face of government surveillance. And although their multinational business interests sometimes lead them to make compromises to do business in repressive countries,[257] these compromises also give them a powerful rhetorical argument against acceding to U.S. surveillance demands: If Apple helps the FBI circumvent iPhone encryption, it will be that much harder to resist when China or Russia makes the same demand.[258] Technology

255. *See, e.g.*, Ben Jacobs, *DC Eyes Tighter Regulations on Facebook and Google as Concern Grows*, GUARDIAN (Sept. 17, 2017, 7:34 AM EDT), https://perma.cc/4N4T-QJ86 ("[T]he growing influence of major tech companies has become a topic of bipartisan concern in Washington DC, and voices on Capitol Hill are getting louder about the need for more oversight of the digital giants' growing role in American politics."); Ben Smith, *There's Blood in the Water in Silicon Valley*, BUZZFEED NEWS (Sept. 12, 2017, 12:37 PM), https://perma.cc/BBT3-FC8S (describing a "palpable, and perhaps permanent, turn against the tech industry" as a "major trend in American politics" and discussing in particular the left's concern over "consolidated corporate power" in that industry).

256. *See Google Code of Conduct*, ALPHABET (Aug. 7, 2017) https://perma.cc/7AZL-B3QZ (capitalization altered).

257. *See supra* note 97.

258. The argument, though rhetorically powerful, is dubious. Russia and China are powerful sovereigns, and there's no reason to think they're waiting for permission from the United States to force technology companies to comply with their surveillance regimes. Even Western European countries, commonly thought to have privacy standards higher than those enforced in the United States, are much further along in the process of legislating limits on encryption and other tools that can thwart lawful government surveillance. *See, e.g.*, Kieren McCarthy, *UK's New Snoopers' Charter Just Passed an Encryption Backdoor Law by the Backdoor*, REGISTER (Nov. 30, 2016, 7:04 AM), https://perma.cc/YE74-25PJ; *see also* Alexandra Beech et al., *Facebook, Google Obliged to Decrypt Online Messages to Help Government Fight Terrorism*, ABC NEWS (Austl.) (July 13, 2017, 10:36 PM), https://perma.cc/2GTY-YPJ4. Far from leading the global discussion over government access to data held by third parties, the United States is pulling up the rear, most likely because other countries—not having massive technology sectors that are politically, culturally, and economically dominant—have more policy freedom to regulate technology.

companies thus cast themselves as protectors of civil liberties both at home and abroad.

Surveillance intermediaries can also mobilize public resistance against surveillance by spotlighting it. At the retail level, they do this by automatically providing notice to users of government requests for data (unless such notice is barred by law).[259] Automatic notice has become a standard expectation of civil society groups; for example, it is one of the criteria on the EFF's annual scorecard.[260] ISO/IEC 27018, an important recent international standard for cloud service providers that has been adopted by companies like Microsoft and Dropbox,[261] also requires automatic user notice.[262]

At the wholesale level, surveillance intermediaries have a number of ways of informing the public about government surveillance. Many companies publish detailed law enforcement guides,[263] which serve a dual role. They tell law enforcement how and what kind of data requests to make, which in turn helps the companies effectively manage requests not only from the various parts of the federal government but also from the thousands of state, local, and foreign law enforcement authorities that similarly need data from surveillance intermediaries. But equally importantly, law enforcement guides give the public information about what sort of surveillance demands companies will accede to (and thus, by implication, what sorts of surveillance demands the government is making).

Transparency reports, by which companies publish granular data on government surveillance orders, are another important tool. These reports, which have become industry standard, were the source of the statistics cited above on government requests—for example, that in 2015 Facebook received almost 37,000 requests for user data.[264] Although the government is required by law to annually report wiretap activity,[265] no such requirement exists for

259. *See, e.g.*, Apple Inc., Legal Process Guidelines: Government & Law Enforcement Within the United States 6 (n.d.), https://perma.cc/WH82-3PMB; *Information for Law Enforcement Authorities*, *supra* note 115; *Transparency Report: Yahoo! Inc. Law Enforcement Response Guidelines*, YAHOO!, https://perma.cc/34JH-PCAM (archived Oct. 14, 2017).

260. *See* NATE CARDOZO ET AL., ELEC. FRONTIER FOUND., WHO HAS YOUR BACK?: 2017, at 6, 10 (2017), https://perma.cc/LWD6-KHYP.

261. Tolga Erbay, *Dropbox for Business Achieves ISO 27018 Certification, an Emerging International Cloud Standard for Privacy and Data Protection*, DROPBOX BUS. (May 18, 2015), https://perma.cc/3PXT-SZVA; *Microsoft Adopts First International Cloud Privacy Standard*, MICROSOFT ON THE ISSUES (Feb. 16, 2015), https://perma.cc/TD6R-XYPS.

262. Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *Information Technology—Security Techniques—Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors*, ISO/IEC 27018, § A.5.1 (Jan. 8, 2014).

263. *See supra* note 259.

264. *See supra* note 62 and accompanying text.

265. *See* 18 U.S.C. § 2519 (2016).

stored-data requests under the SCA, which make up the bulk of government surveillance.[266] In the absence of transparency reports, detailed surveillance statistics would require time-consuming, costly, and potentially unsuccessful requests and litigation under the Freedom of Information Act (FOIA).[267]

Transparency reports have effectively disclosed information on law enforcement investigations, the type of surveillance about which companies are permitted to make the most detailed disclosures. But they've also shed light on the government's use of legal process in national security investigations. For example, the FBI and other investigative agencies can issue national security letters (NSLs) for the production of certain kinds of documents and records.[268] NSLs are a type of administrative subpoena with an important twist: The government can impose nondisclosure orders—commonly (and disparagingly) referred to outside the government as "gag orders"[269]—on NSL recipients, prohibiting those recipients from disclosing the details of any NSLs they've received or even that they've received any.[270] The USA FREEDOM Act of 2015,[271] passed at the urging of technology companies,[272] permits surveillance intermediaries to report on the number of NSLs they receive in bands of 0-499 or 0-999, though these bands, because they start at zero, don't necessarily reveal whether a company has received an NSL or not.[273] The USA FREEDOM Act also made it easier for surveillance intermediaries to publicize more data about NSLs by directing the Attorney General to adopt procedures to require "the review at appropriate intervals" of NSL nondisclosure orders to "assess whether the facts supporting nondisclosure continue to exist" and to terminate the orders "if the facts no longer support nondisclosure."[274] To get around

266. In 2015, Congress imposed various public reporting requirements for FISA orders. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 602(a), 129 Stat. 268, 292-95 (codified at 50 U.S.C. § 1873 (2015)).

267. Pub. L. No. 89-487, 80 Stat. 250 (1966) (codified as amended at 5 U.S.C. § 552 (2016)); *see* Bellia, *supra* note 35, at 342.

268. For useful background on NSLs, see 1 KRIS & WILSON, *supra* note 64, §§ 20:1-:11; Bloch-Wehba, *supra* note 24, at 369-81.

269. *See, e.g.*, Press Release, Elec. Frontier Found., EFF Sues DOJ for Records on Procedures for Ending NSL Gag Orders (June 7, 2017), https://perma.cc/8FXW-4LJR.

270. *See* 1 KRIS & WILSON, *supra* note 64, § 20:10.

271. Pub. L. No. 114-23, 129 Stat. 268 (codified in scattered sections of the U.S. Code).

272. *See* Press Release, Info. Tech. Indus. Council, Tech Encourages Congress to Act Swiftly on Bipartisan Surveillance Reform Legislation (Apr. 29, 2015), https://perma.cc/QC7H-AGMT; *see also* Andrea Peterson, *The Real Winners in the Fight over Government Surveillance*, WASH. POST (June 3, 2015), https://perma.cc/7JYG-YBZF ("The Internet industry's support for surveillance reform was critical . . . ." (quoting Kevin Bankston, Executive Director of New America's Open Technology Institute)).

273. *See* 50 U.S.C. § 1874 (2015).

274. *See* § 502(f), 129 Stat. at 288, *reprinted in* 12 U.S.C. § 3414 app. at 1506 (2016).

nondisclosure orders, companies have also used "warrant canaries": A company that hasn't received an NSL puts a sign to that effect on its website and then silently removes it when it receives a first NSL.[275] Although warrant canaries aren't particularly informative—they don't distinguish between receiving one NSL and receiving 1000—they've proved effective in attracting media attention.[276]

By notifying users of surveillance requests, publishing law enforcement guides, releasing transparency reports, and setting up warrant canaries, surveillance intermediaries make it easier for the public, often through civil society groups, to learn about and, by extension, oppose government surveillance. Consider the EFF: Its ability, through its scorecards and other reporting and advocacy, to comprehensively paint a picture of government surveillance heavily relies on the small number of market-leading services that receive the lion's share of government requests and are willing to publicize as much information as they are legally allowed to (and to challenge laws that restrict the publication of surveillance statistics).

Finally, surveillance intermediaries augment their soft power through more traditional sources of influence in the policymaking process. Traditional lobbying plays a large and underappreciated role. Google spent nearly $5 million lobbying in the second quarter of 2015, making it the third-largest corporate lobbyist; Facebook, Amazon, and Apple were close behind.[277] Beyond pushing federal legislation like the USA FREEDOM Act—which in addition to increasing surveillance transparency also ended the NSA's controversial collection of bulk telephony metadata[278]—surveillance intermediaries can also shape policy on the state level. For example, Apple, Facebook, Google, and others supported the passage of California's Electronic Communications Privacy Act (commonly known as CalECPA), which goes beyond federal data protection law in requiring warrants to compel the

275. *See* Bloch-Wehba, *supra* note 24, at 380. There is some question over whether warrant canaries violate NSL nondisclosure prohibitions. *See, e.g.*, *id.* at 380-81 ("The canary remedy is also legally questionable; in a discussion on the site, the Reddit CEO commented, 'Even with the canaries, we're treading a fine line . . . . I've been advised not to say anything one way or the other.' (quoting Kim Zetter, *Reddit Hints—Without Saying Anything—That It Got a National Security Letter*, WIRED (Mar. 31, 2016, 8:56 PM), https://perma.cc/AX8L-XVUL)).

276. *See, e.g.*, Zetter, *supra* note 275. There even used to be a website devoted to tracking warrant canaries across the internet. *See* Cooper Quintin, *Canary Watch—One Year Later*, ELECTRONIC FRONTIER FOUND. (May 25, 2016), https://perma.cc/8RU7-VYYY.

277. *See* Issie Lapowsky, *What Tech Companies Are Spending Millions Lobbying For*, WIRED (July 23, 2015, 7:00 AM), https://perma.cc/YQ6D-J9FL.

278. *See supra* note 74.

production of metadata or stored content.[279] Lastly, top executives from the leading surveillance intermediaries frequently serve stints in the government, bringing Silicon Valley's perspective on privacy and technology issues to the Washington policy apparatus.[280]

At its core, changing policy requires changing politics: mobilizing interest groups and public opinion to shape and constrain government action. Compared to legal or technical resistance, policy mobilization operates more indirectly, takes longer to come to fruition, and requires more effort. But in the long run this form of constraint on government action is the most durable and sustainable. This is especially true when, as with surveillance, the government activity involves the defense of the nation and thus is at its most powerful in times of emergency.[281]

III. Surveillance Separation of Powers

Part II described the three ways surveillance intermediaries resist government surveillance. First, they resist procedurally—demanding that the government formally order them to disclose data—and litigiously—suing over those orders on behalf of themselves and their users. Second, they resist (whether intentionally or not) by unilaterally changing their technology, implementing features like end-to-end encryption and overseas data storage that increase surveillance's technical, legal, and political costs. And third, they resist by shaping policy, raising public opposition to surveillance, lobbying and serving in the government, and increasing awareness of government surveillance through user notifications, transparency reports, law enforcement guidelines, and warrant canaries.

This Part describes how intermediaries' techniques of resistance constrain government surveillance in another way, by strengthening the *surveillance separation of powers*: the formal and informal rules, practices, and norms that determine how the government conducts and regulates surveillance.[282] By unpacking "the government" into its constituent parts, we can see how

279. Ch. 651, 2015 Cal. Stat. 5110 (codified as amended at CAL. PENAL CODE §§ 1546, 1546.1 to .4 (West 2017)); *see* Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015, 9:58 PM), https://perma.cc/3YG9-3JDZ.

280. *See, e.g.*, Cecilia Kang & Juliet Eilperin, *Why Silicon Valley Is the New Revolving Door for Obama Staffers*, WASH. POST (Feb. 28, 2015), https://perma.cc/KLS5-SVWU. This was certainly true in the Obama Administration; whether the practice will continue in the Trump Administration remains to be seen.

281. *See* ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC 4-5 (2010).

282. In this Part, I limit my discussion to the federal system, though similar dynamics likely exist at the state level.

surveillance intermediaries empower (or disempower) different government actors and allow the *surveillance executive*—those parts of the executive branch that conduct surveillance—to be better constrained at the *interbranch* level (by Congress and the courts), at the *intrabranch* level (by other executive branch agencies), and at the *intra-agency* level (by oversight and surveillance-checking bodies within the surveillance executive itself).

A. Interbranch Checks

In the classic account, the separation of powers happens between the three branches of government: the legislature, the executive, and the judiciary. The Framers designed the Constitution around this triangular relationship, trying to give each branch "the necessary constitutional means and personal motives to resist encroachments of the others."[283] The framers of modern surveillance law similarly relied on the notion of interbranch checking, counting on Congress and the courts to check the President. For example, in enacting FISA, Congress put limits, enforceable by courts, on the executive branch's domestic foreign-intelligence gathering.

More and more, however, scholars doubt that Congress and the courts have the necessary means and motives to police government surveillance. For example, Huq worries that "Congress is unlikely to be a constant Fourth Amendment ally in new technological fields,"[284] and he's similarly skeptical about the judiciary.[285] He thus pessimistically concludes that these "institutional officeholders[]" on whom our constitutional order relies for the defense of Fourth Amendment values have "weak incentives regarding rights-related ends."[286]

Executive branch veterans with personal experience working under the yoke of congressional and judicial oversight might take issue with Huq's characterization of Congress and the courts as ineffectual. But Huq is correct, at least to a first approximation, that "the Fourth Amendment and the separation of powers rise (and fall) together."[287] In this Subpart, I argue that when surveillance intermediaries resist government surveillance, they strengthen the interbranch separation of powers, amplifying the ability of Congress and the courts to regulate the surveillance executive.

---

283. *See* THE FEDERALIST NO. 51, at 321-22 (James Madison) (Clinton Rossiter ed., 1961).

284. Aziz Z. Huq, Essay, *How the Fourth Amendment and the Separation of Powers Rise (and Fall) Together*, 83 U. CHI. L. REV. 139, 161 (2016).

285. *See id.* at 161-63.

286. *Id.* at 163.

287. *Id.* at 139 (capitalization altered).

1. Congress

Congress has a difficult time overseeing surveillance because oversight requires time, money, knowledge, and power—all things Congress often lacks or is unwilling to devote. As public choice theory explains, a legislator's main incentive is to get reelected.[288] Sweating the arcana of surveillance law doesn't earn many votes, even for a member of the intelligence committees; it's hard to take credit for oversight that's largely done in secret and has few pork-barrel possibilities.[289] Congress underinvests the necessary money, expertise, and attention, and thus struggles to oversee intelligence activities, set priorities, improve programs, and inform the public.[290]

By increasing the electoral payoff of surveillance oversight, surveillance intermediaries can incentivize Congress to be more gimlet-eyed. Like any powerful interest group, technology companies exert influence over the legislative process.[291] They hold most sway over legislators in whose districts they operate, but they can donate money to (and thus influence) everyone. Surveillance intermediaries can also make surveillance more salient to the (voting) public. For example, by publicly opposing the San Bernardino iPhone unlocking order, Apple made overseeing the FBI worth more of Congress's time.

Just as surveillance intermediaries increase the benefits Congress gets from overseeing surveillance, they also decrease the costs Congress incurs for conducting such oversight. Congress, as a bicameral, decentralized, and partisan body, struggles to oversee the faster and more unified surveillance executive. This comparative institutional disadvantage compounds when Congress tries to act through "police patrols": direct congressional oversight like hearings and investigations.[292] Congress can mitigate some of these problems by availing itself of "fire alarms," piggybacking on the monitoring efforts of others, often outside the government.[293] Congress frequently creates fire alarms intentionally, as when it mandates that agencies hold public

288. *See* DANIEL A. FARBER & PHILIP P. FRICKEY, LAW AND PUBLIC CHOICE: A CRITICAL INTRODUCTION 22 (1991).

289. *See* Samuel J. Rascoff, *The President as Intelligence Overseer*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 235, 251 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016).

290. *See* Amy B. Zegart, *The Domestic Politics of Irrational Intelligence Oversight*, 126 POL. SCI. Q. 1, 25 (2011).

291. *See supra* notes 277-80 and accompanying text.

292. *See* Mathew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms*, 28 AM. J. POL. SCI. 165, 166 (1984).

293. *See id.* Ashley Deeks has recently applied the fire alarm model to congressional oversight of foreign intelligence. *See* Ashley Deeks, Essay, *Checks and Balances from Abroad*, 83 U. CHI. L. REV. 65, 82-84 (2016).

hearings before taking action or that they disclose information to the public. (The Administrative Procedure Act and FOIA are thus classic examples of fire alarm statutes.)[294] But Congress need not create a fire alarm to benefit from it. Existing fire alarms, like a surveillance target's right to challenge the surveillance in court, can be just as helpful.

Surveillance intermediaries can thus ring the fire alarm by directly resisting government surveillance. Particularly in the context of foreign intelligence, Congress has explicitly delegated its oversight responsibilities by creating causes of action for companies to challenge orders under FISA[295] and the USA PATRIOT Act.[296] Congress went even further in the USA FREEDOM Act; by prohibiting the NSA from requesting bulk telephony metadata records and forcing it to request metadata from telephone companies on an individual basis,[297] Congress made it easier for companies to monitor and challenge telephony-metadata surveillance.

Another fire alarm function performed by surveillance intermediaries is generating information about surveillance. This is important because Congress can't oversee government surveillance it doesn't know about.[298] Knowledge gaps arise for several reasons. First, the executive branch is not required to disclose (either to Congress or to the public) detailed information on all its surveillance activities. For example, although law enforcement agencies have to publish statistics on their real-time monitoring under the Wiretap Act,[299] they do not have to publish similar information about data collection under the SCA.

---

294. *See* 5 U.S.C. §§ 552-553 (2016).

295. 50 U.S.C. § 1881a(h)(4)(A), (C) (2015).

296. *Id.* § 1861(f)(2)(A)(i); *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S. Code). The statutes governing law enforcement surveillance also permit company challenges, though they are phrased in narrower terms. The Wiretap Act allows challenges for technical inability, 18 U.S.C. § 2518(12) (2016) ("A provider of wire or electronic communications service . . . may move the court to modify or quash [an interception] order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion."), and the SCA allows a challenge if "the information or records requested are unusually voluminous in nature or compliance with [the] order otherwise would cause an undue burden" on the company, *id.* § 2703(d).

297. 50 U.S.C. § 1861(b), (c)(3) prohibits bulk collection, while § 1861(c)(2)(F) sets out provider responsibilities to comply with an order for telephony metadata. *See also* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 269-70 (2017) (describing this feature of the USA FREEDOM Act as an example of "information siloing").

298. *Cf.* David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 300-01 (2010).

299. *See* 18 U.S.C. § 2519.

Second, even where congressional reporting requirements exist, as with foreign intelligence,[300] information may not disseminate effectively through Congress. One reason is that not enough congressional staffers have the security clearances necessary to access (and thus advise their bosses on) classified executive branch surveillance reports.[301] Another is that the intelligence oversight committees jealously guard information.[302] These internal blockages mean that Congress as a whole may have little understanding of executive branch surveillance even when the executive branch has fully briefed its congressional overseers. Though mundane, such organizational pathologies can cause serious problems. For example, although the executive branch repeatedly briefed the relevant committees on the bulk telephony metadata program operated under section 215 of the USA PATRIOT Act (and indeed offered a briefing to every member of Congress),[303] that information never reached many of the congressional rank and file.[304] This lack of full congressional involvement was a major source of the outcry both in and out of Congress when the program became public.[305]

When surveillance intermediaries publicize the surveillance executive's activities, whether by issuing transparency reports or by increasing the salience of government surveillance through litigation and public activities, they activate handy information-creation fire alarms. Instead of Congress having to collect and analyze raw data on surveillance activities—data the

300. *See, e.g.*, 50 U.S.C. § 3091(a)(1) ("The President shall ensure that the congressional intelligence committees are kept fully and currently informed of the intelligence activities of the United States . . . ."); *see also id.* § 1885c(a) (requiring the Attorney General to "fully inform" the congressional intelligence and judiciary committees regarding section 702 activity at least every six months). By executive order, foreign-intelligence gathering that is not regulated by FISA is subject to the same congressional notification requirements. *See* Exec. Order No. 12,333, § 3.1, 3 C.F.R. 200 (1982), *reprinted as amended in* 50 U.S.C. § 3001 app. at 469 (2015).

301. *See* Zegart, *supra* note 290, at 17, 19.

302. *See, e.g.*, *id.* at 19 ("Senate rules designate intelligence committee information 'committee sensitive,' which prohibits committee staff from sharing information with Senators' personal staff even if they hold the appropriate security clearances.").

303. *See* David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SECURITY L. & POL'Y 209, 261-73 (2014); *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287-88 (codified as amended at 50 U.S.C. §§ 1861-1862).

304. *See* SAVAGE, *supra* note 22, at 221-23.

305. *See id.* A former chief counsel of the House Permanent Select Committee on Intelligence observed that after the section 215 program was disclosed, "[m]any Members of Congress were concerned about being 'out of the loop' with respect to the details of the program." *See* Christopher A. Donesa, *Is "Secret Law" Really Either?: Congressional Intent, Legislative Process, and Section 215 of the USA PATRIOT Act*, 3 NAT'L SECURITY L.J. 101, 101, 115-16 (2014).

technology giants, because of their intermediary status, are in a unique position to acquire—Congress benefits from the information the companies create. The transparency reports and litigation companies produce are the domestic analog to the fire alarm function that foreign cybersecurity firms perform when they detect, investigate, and publicize what would otherwise be highly classified and not widely distributed information on electronic foreign-intelligence gathering by the United States and its allies.[306] This information, notes Ashley Deeks, "allow[s] all members of Congress to better understand cyberthreats generally and (possible) US capabilities in particular."[307] More generally, the effect of lowering Congress's information-gathering costs has been to apply what Patricia Bellia has called FISA's "information structure"—the "institutional mechanisms designed to generate the information necessary" for Congress to evaluate electronic foreign-intelligence gathering[308]—to other contexts, especially law enforcement access to stored data, thus broadly expanding Congress's oversight capabilities.

2. Courts

Because technology companies are increasingly demanding court orders rather than voluntarily complying with government requests, the government must put more and more of its surveillance activity before the courts. Where this leads to adversarial litigation, courts benefit from the increased information that results from the litigants' clash of views. But even if, as is true of the vast majority of surveillance court orders, the proceedings are ex parte,[309] the requirement that the government make its case to an independent tribunal itself has an important disciplining effect. Although the government generally prevails, its winning record does not mean that the courts function as a "rubber stamp" (as is sometimes argued with regard to the government's high success rate before the Foreign Intelligence Surveillance Court (FISC))[310] and fail to constrain government behavior.[311] According to Geoffrey Stone, a member of the Obama-era President's Review Group on Intelligence and

306. *See* Deeks, *supra* note 293, at 83.

307. *Id.* U.S. firms similarly investigate foreign cyber activity. *See, e.g.*, MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2 (n.d.), https://perma.cc/GFR6-KCWX.

308. *See* Bellia, *supra* note 35, at 342.

309. *See, e.g.*, Conor Clarke, Essay, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?: Ex Parte Proceedings and the FISC Win Rate*, 66 STAN. L. REV. ONLINE 125, 127 (2014).

310. *See, e.g.*, Elkin-Koren & Haber, *supra* note 15, at 148.

311. For recent arguments that the FISC's high approval rates do not support the "rubber stamp" thesis, see Emily Berman, *The Two Faces of the Foreign Intelligence Surveillance Court*, 91 IND. L.J. 1191, 1229-30 (2016); and Clarke, *supra* note 309, at 126.

Communications Technologies, it's more likely that FISC judges "take their responsibilities seriously" and "that officials in the Department of Justice take equally seriously their responsibility to put forth requests for approval only when they are confident that the requests are justified."[312] And Daniel Solove notes that "far from demonstrating that the warrant system isn't working well, the high rate of warrants granted shows that law-enforcement officials most often refrain from making spurious search requests to courts."[313]

This dynamic comes from two features of the relationship between government lawyers and the courts. First, the repeat nature of the interactions makes generating trust and credibility important; if the surveillance executive tries to pull a fast one in one instance, it knows to expect punishment from a skeptical court the next time it seeks authorization.[314] Second, because the courts generally consider surveillance applications ex parte, they depend on the government for accurate information; this further raises the reputational stakes and sensitizes the courts as well as the executive branch to the executive's obligations of candor.[315] In this way, even ex parte review disciplines government surveillance, limiting it substantially from what it would be if it occurred solely on the executive's authority.

Once the ex parte setting has given way to adversarial litigation, the willingness of surveillance intermediaries to challenge government surveillance increases the courts' power relative to the political branches with regard to government surveillance and foreign intelligence, for two reasons.

First, surveillance intermediaries challenge government surveillance in situations where the target of the surveillance would lack the incentive to do so. Specifically, the SCA, unlike the Wiretap Act,[316] lacks a statutory suppression remedy. Thus, defendants lack any incentive to challenge nonconstitutional violations of the statute—for example, that the government action exceeded statutory authorization—because a successful challenge would not prevent the prosecution from using the incriminating evidence.[317] By contrast, surveillance intermediaries have an incentive to challenge SCA orders they believe to be statutorily defective so as to avoid having to turn user

312. *See* Geoffrey R. Stone, *Reflections on the FISA Court*, HUFFPOST (updated Sept. 4, 2013), https://perma.cc/F2ZE-GJPB.

313. SOLOVE, *supra* note 19, at 130.

314. *See id.*

315. For a discussion and detailed case study from two former NSA lawyers of the searching nature of judicial oversight of government foreign intelligence surveillance, see John DeLong & Susan Hennessey, *Understanding Footnote 14: NSA Lawyering, Oversight, and Compliance*, LAWFARE (Oct. 7, 2016, 7:44 AM), https://perma.cc/F4WY-GB4J.

316. *See* 18 U.S.C. § 2518(10)(a) (2016).

317. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 806-07 (2003).

data over to the government. Such challenges bring courts to bear on government surveillance under the SCA.

Second, surveillance intermediaries can get around some of the vexing standing problems that have often prevented courts from reviewing foreign intelligence surveillance. In *Clapper*, the Supreme Court held that a group of attorneys, activists, and media organizations lacked standing to challenge section 702 surveillance because they could not establish that their claimed injury—that the government would collect their communications under the program—was "certainly impending."[318] The Court rejected the argument that the chilling effect of possibly having one's communications collected created a sufficient First Amendment injury to establish standing.[319] By requiring plaintiffs to have clear evidence they are being surveilled—a fact that, because of the secret nature of the surveillance, is difficult to establish—*Clapper* has made it hard for individuals to challenge broad surveillance programs.[320]

Clapper is only partially a case about individuals' rights to challenge surveillance programs. It is equally about the power of courts to sit in judgment over decisions made by the political branches regarding government surveillance. The Supreme Court describes standing as "built on a single basic idea—the idea of separation of powers."[321] Although scholars question whether the doctrine lives up to its billing,[322] it remains the case that standing is a prerequisite for a federal court to rule on congressional or executive activity and therefore to exercise its ability to check that activity (even if it ultimately approves it). By getting federal courts out of the business of overseeing secret

318. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1142-43, 1145 (2013).

319. *See id.* at 1152.

320. *See* Jeffrey L. Vagle, Essay, Laird v. Tatum *and Article III Standing in Surveillance Cases*, 18 U. PA. J. CONST. L. 1055, 1055 (2016) ("Plaintiffs seeking to challenge government surveillance programs have faced long odds in federal courts, due mainly to a line of Supreme Court cases that have set a very high bar to Article III standing in these cases."); Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 551, 567 (2014) (noting "the exceptionally high bar *Clapper* imposes before plaintiffs will be able to challenge secret government surveillance programs going forward").

321. Allen v. Wright, 468 U.S. 737, 752 (1984); *see also, e.g.*, *Clapper*, 133 S. Ct. at 1146 ("The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches."); Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 881 (1983) (arguing that "the judicial doctrine of standing is a crucial and inseparable element" of the separation of powers).

322. *See, e.g.*, Heather Elliott, *The Functions of Standing*, 61 STAN. L. REV. 459, 463 (2008) ("[S]tanding is ill-suited to most of the functions it is asked to serve . . . .").

surveillance via litigation, the Supreme Court largely left the issue to the political branches.[323]

Surveillance intermediaries are not afflicted by the standing problems that plague individual plaintiffs. Because surveillance intermediaries are intimately familiar with the details of the surveillance programs with which they are required to cooperate, they avoid the knowledge problems that doom other plaintiffs. Intermediaries can aggressively defend their own rights (and occasionally the rights of their users), thereby forcing courts to engage with surveillance programs they might otherwise have been able or obligated to avoid.

Although there are other ways for individuals to overcome standing problems,[324] surveillance intermediaries have several advantages over criminal defendants or public interest litigants when it comes to using the courts to check the executive branch. Rather than having to wait for an outside event to establish standing—such as a criminal indictment or a disclosure providing public information on the scope of a particular program—surveillance intermediaries know whenever a program is used. This also gives surveillance intermediaries the flexibility to choose the best litigating posture, something that can be a particular problem for criminal defendants, who, as is generally recognized, can make unattractive litigants and whose bad facts can make bad law (from the perspective of those opposing government surveillance). Finally, surveillance intermediaries, especially the largest ones, have the resources to litigate frequently and to the bitter end.

323. *Cf.* United States v. Richardson, 418 U.S. 166, 176, 179 (1974) ("In a very real sense, the absence of any particular individual or class to litigate [constitutional claims seeking detailed information on CIA expenditures] gives support to the argument that the subject matter is committed to the surveillance of Congress, and ultimately to the political process. Any other conclusion would mean that the Founding Fathers intended to set up something in the nature of an Athenian democracy or a New England town meeting to oversee the conduct of the National Government by means of lawsuits in federal courts.").

324. Sometimes the law requires notice, as when the government uses FISA-derived evidence against a criminal defendant. *See* 50 U.S.C. § 1806(d) (2015). Thus, two criminal cases have presented vehicles for merits litigation upholding section 702's constitutionality. *See* United States v. Mohamud, 843 F.3d 420, 431, 438-44 (9th Cir. 2016), *petition for cert. filed*, No. 17-5126 (U.S. June 14, 2017); United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500, at *2, *14 (E.D.N.Y. Mar. 8, 2016). The district court's opinion in *Hasbajrami* provided reasoning for its February 20, 2015 ruling denying the defendant's suppression motion. *See* 2016 WL 1029500, at *2. Hasbajrami has challenged that ruling as part of his appeal of his conviction, but that appeal is still pending. *See* United States v. Hasbajrami, No. 15-2684 (2d Cir. Aug. 21, 2015).

B. Intrabranch and Intra-agency Checks

As we've seen, surveillance intermediaries can help Congress and the courts check the surveillance executive. But to fully analyze how intermediaries augment the surveillance separation of powers, we have to go beyond just *inter*branch effects. Over the past two decades, the quest for new ways to check executive power has sent scholars hunting within the executive branch itself.[325] Charting how power is diffused throughout the executive branch, and recognizing that the "unitary executive" is not a descriptive truth but at most a doctrinal ideal, these scholars have demonstrated that the "internal separation of powers" within the executive branch is an important guarantor of the Founders' commitment to constrained government—indeed, as important as or perhaps even more so than the classic interbranch separation of powers.[326] Thus, to complete the analysis, we have to zoom in and identify the actors and institutions within the executive branch that, empowered by surveillance intermediaries, have the means and motives to constrain the surveillance executive.

As we look through the microscope, the first intrabranch level we observe is that of the interagency: the executive and independent agencies that, by themselves or under the coordinating authority of the White House, set government policy. We can sort agencies based on their main policy responsibilities and institutional interests, known in the jargon as their "equities."[327] Because the interagency policy process is consensus driven, the question of who gets to sit at the policymaking table is critical. Such questions are resolved in the first instance by matching the policy issues under discussion with the relevant equities of the various agencies. For example, a discussion about cyberwar might include representatives from the military, the diplomatic corps, and the law enforcement and intelligence communities, but probably not from the Department of Housing and Urban Development, no matter how strongly its secretary might feel about the matter.

The more credibly an agency can argue that an issue implicates its equities, the more likely it will be included in—and thus able to influence—the policymaking process on that issue.[328] That the agencies within the

325. *See, e.g.*, Neal Kumar Katyal, Essay, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2316-18 (2006).

326. *See id.* (capitalization altered); M. Elizabeth Magill, *Beyond Powers and Branches in Separation of Powers Law*, 150 U. PA. L. REV. 603, 643-46 (2001); Jon D. Michaels, *An Enduring, Evolving Separation of Powers*, 115 COLUM. L. REV. 515, 529-69 (2015).

327. *See* Cass R. Sunstein, *The Most Knowledgeable Branch*, 164 U. PA. L. REV. 1607, 1622 (2016).

328. For background on national security interagency policymaking and the role of agency equities, see ALAN G. WHITTAKER ET AL., THE NATIONAL SECURITY POLICY PROCESS: THE NATIONAL SECURITY COUNCIL AND INTERAGENCY SYSTEM (2011), https://perma.cc/APP7-XPDM.

surveillance executive have equities in surveillance policy is accepted as a matter of course. The intelligence community collects, analyzes, and disseminates foreign intelligence,[329] and federal law enforcement agencies conduct domestic surveillance, helping the Department of Justice prevent and prosecute crime. It's thus unsurprising that the agencies that make up the surveillance executive have historically taken the lead in developing and implementing surveillance policy.

Outside the surveillance executive, other agencies may perceive their equities as benefiting from less surveillance. The Commerce Department and the Office of the United States Trade Representative work to ensure the global competitiveness of U.S. companies; they might prefer that technology companies not be perceived by customers outside the United States as helping the government collect foreign intelligence. The Federal Trade Commission aims to improve the cybersecurity of consumer devices, including by encouraging encryption,[330] and so might oppose attempts by law enforcement to circumvent end-to-end encryption. The State Department works to advance "Internet freedom" like the right of people around the world to "express [themselves] . . . free from undue interference or censorship,"[331] including by funding Tor,[332] the anonymous-communications network that helps protect political dissidents from persecution (but unfortunately also facilitates trade in drugs and child pornography).[333] And various oversight and advisory bodies

329. "The U.S. Intelligence Community is a coalition of 17 agencies and organizations . . . within the Executive Branch . . . [that] work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities." *What We Do*, OFF. DIRECTOR NAT'L INTELLIGENCE, https://perma.cc/Q93F-PKRN (archived Oct. 22, 2017). It consists of Air Force Intelligence, Army Intelligence, the CIA, Coast Guard Intelligence, the Defense Intelligence Agency, the Department of Energy's Office of Intelligence and Counterintelligence, the DHS's Office of Intelligence and Analysis, the Department of State's Bureau of Intelligence and Research, the Department of the Treasury's Office of Intelligence and Analysis, the Drug Enforcement Administration, the FBI, Marine Corps Intelligence, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the NSA, Navy Intelligence, and the Office of the Director of National Intelligence. *See Members of the IC*, OFF. DIRECTOR NAT'L INTELLIGENCE, https://perma.cc/3QZ4-VR4J (archived Oct. 22, 2017).

330. *See, e.g.*, FTC, Careful Connections: Building Security in the Internet of Things 3 (2015), https://perma.cc/CX5D-LAHH.

331. U.S. Dep't of State, Department of State International Cyberspace Policy Strategy 7 (2016), https://perma.cc/EQY9-HRQW.

332. *See Tor: Sponsors*, TOR, https://perma.cc/CC9S-WM6P (archived Oct. 14, 2017) (listing the State Department's Bureau of Democracy, Human Rights, and Labor as a supporter of Tor from 2013 to 2018).

333. *See* Daniel Moore & Thomas Rid, *Cryptopolitik and the Darknet*, SURVIVAL, Feb.-Mar. 2016, at 7, 17 (noting Tor's use in facilitating political activity); *id.* at 21 (reporting the results of an analysis "suggest[ing] that the most common uses for websites on Tor

footnote continued on next page

like the standing Privacy and Civil Liberties Oversight Board (and, during the Obama Administration, the aforementioned President's Review Group on Intelligence and Communications Technologies) work to make privacy interests a central concern of surveillance policymaking.

For bureaucratic and other reasons, "hard" issues like public safety and national security often dominate policymaking, with "softer" economic and privacy concerns getting second billing.[334] When technology companies noisily and publicly resist government surveillance, they highlight equities that agencies outside the surveillance executive have in the surveillance executive's law enforcement and foreign-intelligence activities.[335] By making the costs of surveillance more salient, surveillance intermediaries strengthen the policymaking position of such outside agencies, whose equities frequently overlap with those of the resisting companies: for example, competing for foreign business, resisting authoritarian regimes, and safeguarding consumer privacy and digital security.[336] The aggregate effect has been to change the default that determines which agencies can participate in surveillance policymaking—for example, moving from economic-agencies-out to economic-agencies-in.[337]

Specific techniques of resistance also create new opportunities for the outside agencies to assert their equities. When surveillance intermediaries publish statistics about government data requests, they can't but make foreigners more worried that the U.S. government is reading their Gmails and watching their FaceTime calls. This blowback makes it easier for economic and diplomatic agencies to involve themselves in surveillance policymaking, invoking their responsibility over foreign trade. When Microsoft stores user data in Ireland, it puts a foreign policy overlay on what used to be purely domestic law enforcement investigations, thus triggering foreign policy equities.[338] And when companies (whether intentionally or not) incentivize law enforcement hacking to circumvent end-to-end encryption, they empower agencies that work to improve consumer cybersecurity.

The increased diversity of agencies involved in surveillance policymaking is analogous to what Jody Freeman and Jim Rossi have called "shared

---

hidden services are criminal, including drugs, illicit finance and pornography involving violence, children and animals").

334. *See* Kerry, *supra* note 82, at 11.

335. For a firsthand account of how the Commerce Department came to play an important role in surveillance and foreign-intelligence policy, see *id.* at 1-6.

336. *See id.* at 11-15.

337. *See id.* at 11.

338. *See* Daskal, *supra* note 32, at 390-91.

regulatory space" in administrative law,[339] except that the mandate for agencies to collaborate comes not from Congress but instead from executive branch norms of interagency coordination. To be sure, the outside agencies don't always win the day. But even when they lose, the "profound coordination challenges"[340] that arise when authority is fragmented among multiple agencies make it harder for the surveillance executive to implement its desired (and generally pro-surveillance) policy. This policymaking drag makes it harder for the government to keep from falling behind on the treadmill of technological change. The increasing gap between the government's needs and its capabilities redounds to the benefit of the surveillance intermediaries, who might "prefer fragmentation to coordination, to the extent that it allows firms to play one agency against another in an effort to weaken regulation overall, or to forum shop among regulators,"[341] especially "where agencies simply refuse to coordinate for one reason or another, whether because of substantive disagreements, personality clashes, or cultural conflicts."[342]

The best illustration of how shared regulatory space can lead to surveillance policy paralysis is the widely reported debate within the Obama Administration over encryption.[343] The FBI forcefully advocated for law enforcement access to encrypted information; other agencies emphasized competing interests like secure communications for overseas political dissidents, global sales for U.S. technology companies, and protection of consumer data from hackers.[344] The result was administrative gridlock, with President Obama urging a compromise solution but declining to propose legislation that might implement such a solution.[345] It may be years before law enforcement wins the argument inside the executive branch (if it ever does), by which point end-to-end encryption will be that much harder to roll back.

Although the executive interagency served as the backdrop for the above analysis, the analysis applies equally when we zoom in one more level. Once we have "cracked open the black box of agencies"[346] and examined how power is

339. *See* Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space*, 125 HARV. L. REV. 1131, 1135-36 (2012).

340. *Id.* at 1135.

341. *Id.* at 1183.

342. *Id.* at 1186-87.

343. *See, e.g.*, Sara Sorcher & Joshua Eaton, *What the US Government Really Thinks About Encryption*, CHRISTIAN SCI. MONITOR (May 25, 2016), https://perma.cc/4UD4-LLHW.

344. *See* Michael D. Shear & David E. Sanger, *Competing Interests on Encryption Divide Top Obama Officials*, N.Y. TIMES (Mar. 5, 2016), https://perma.cc/2ZRX-VGH5.

345. *See* Michael D. Shear, *Obama, at South by Southwest, Calls for Law Enforcement Access in Encryption Fight*, N.Y. TIMES (Mar. 11, 2016), https://perma.cc/3MJY-L4ZS.

346. *See* Elizabeth Magill & Adrian Vermeule, *Allocating Power Within Agencies*, 120 YALE L.J. 1032, 1035 (2011).

distributed within them, we can relax the assumption made above that each agency is responsible for a single surveillance-related policy goal. In reality, every agency has multiple competing goals. The NSA, for example, has both an offensive mission to collect foreign intelligence and disrupt the operational capabilities of overseas adversaries—including by hacking their systems—and a defensive mission to safeguard national security systems used by the U.S. government.[347] Those within the NSA who are charged with its defensive responsibilities may have different policy preferences on matters like end-to-end encryption than those responsible for offensive operations.

In some cases, conflicting agency mandates are not equal in status. Rather, agencies have "secondary mandates" that are subordinate to their primary responsibilities but are still important.[348] For example, agencies like the FBI and DHS are mandated to safeguard privacy,[349] though these mandates are secondary to their law enforcement and public safety responsibilities.[350] Many different agency actors champion secondary mandates, from inspectors general[351] to a diverse array of what Margo Schlanger has termed "offices of goodness": agency offices that are advisory, value-infused, and internal to and dependent on the agency,[352] like the DHS's Office for Civil Rights and Civil Liberties[353] or the NSA's Civil Liberties and Privacy Office.[354]

For the same reasons as discussed above, resistance to surveillance by technology companies can help policy allies within the surveillance executive. When technology companies publicize information about government surveillance, these disclosures lend support to surveillance executive insiders who want to limit agency activities or at least to make them more transparent.

---

347. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1043 (2014) ("[T]he NSA must choose between offense and defense—between the two halves of its organization."); *Frequently Asked Questions: About NSA*, NAT'L SECURITY AGENCY, https://perma.cc/4JRS-VDPC (archived Oct. 22, 2017) (describing the NSA's "two interconnected missions").

348. *See* J.R. DeShazo & Jody Freeman, *Public Agencies as Lobbyists*, 105 COLUM. L. REV. 2217, 2219 (2005).

349. *See* 6 U.S.C. § 142 (2016) (mandating the appointment of a DHS privacy officer); FBI, Domestic Investigations and Operations Guide § 4 (2013), https://perma.cc/5CJA-E4ZW (outlining the FBI's privacy and civil liberties responsibilities).

350. *Cf.* Renan, *supra* note 29, at 1113.

351. *See* Shirin Sinnar, *Protecting Rights from Within?: Inspectors General and National Security Oversight*, 65 STAN. L. REV. 1027, 1032 (2013); *see also* Sinnar, *supra* note 48, at 309-15 (discussing the role of the Department of Justice's Office of the Inspector General).

352. Margo Schlanger, *Offices of Goodness: Influence Without Authority in Federal Agencies*, 36 CARDOZO L. REV. 53, 60-62 (2014) (capitalization altered).

353. *See id.* at 62-65.

354. *See* Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SECURITY J. 112, 193-99 (2015).

And the knowledge that technology companies will aggressively resist gives these entities a strong argument: Listen to us and avoid a bigger fight down the road.

IV. Surveillance Frontiers

We can summarize the story so far as follows: Surveillance intermediaries control the third-party environment and so constrain government surveillance, not only through their own actions but also by augmenting the power of others in both society at large and the government itself. In this final Part, I ask the normative question: In what ways are these constraints good or bad? In structuring this analysis, it's helpful to consider a preliminary question: How does a society go about deciding when, how, and of what its government conducts surveillance?

In their discussion of the proper role of courts and Congress in overseeing executive policymaking during national security emergencies, Eric Posner and Adrian Vermeule provide a useful model.[355] Drawing on neoclassical welfare economics, they put forward what they call the "tradeoff thesis": "Both security and liberty are valuable goods that contribute to individual well-being or welfare. Neither good can simply be maximized without regard to the other."[356] Thus, "The problem from the social point of view is to optimize: to choose the joint level of liberty and security that maximizes the aggregate welfare of the population."[357] To represent the relationship between security and liberty, Posner and Vermeule introduce the idea of the "security-liberty frontier": the "range of points at which no win-win improvements are possible."[358] At the security-liberty frontier, any increase in security requires a decrease in liberty, and vice versa. Policymaking does not necessarily occur on the frontier; it "might be stuck below the frontier," in which case it should be possible to increase security or liberty without diminishing the other.[359] But at the frontier this kind of optimization is no longer possible. Once a society finds itself at the frontier, it must choose some point along the constraint curve. Importantly, "the frontier itself conveys no information about where the optimal tradeoff point lies. There is no general answer to the question, which

355. *See* ERIC A. POSNER & ADRIAN VERMEULE, TERROR IN THE BALANCE: SECURITY, LIBERTY, AND THE COURTS 22 (2007).

356. *Id.*

357. *Id.*

358. *Id.* at 26.

359. *Id.* at 33.

depends entirely on the values or preferences of the people in the relevant society."[360]

The tradeoff thesis is not limited to security-liberty frontiers, or even two-value frontiers. It applies more generally to any situation in which we're trying to maximize a set of values, at least some of which conflict at least some of the time. Thus, we can broaden our perspective from security-liberty frontiers and focus instead on *surveillance frontiers*: tradeoff sets among the various goods that surveillance implicates (security, privacy, economic growth, and so on). The tradeoff thesis is helpful because it divides our normative analysis into two questions. The first question is about *frontier construction*: When surveillance intermediaries resist government surveillance, do they help or hinder society's effort to reach the surveillance frontier? The second question is about *frontier choice*: Does the resistance enhance or detract from the process by which society chooses to implement some point along the frontier?

It's important to recognize that the standards for measuring these two questions differ fundamentally. The problem of frontier construction is primarily one of *accuracy*: Have we identified all the relevant costs and benefits of various policy options, and have we thought creatively about ways to avoid certain tradeoffs through innovation (of technology, law, process, and so on)? Of course, how you build the tradeoff set will depend on how you define the underlying values, and these might be contested.[361] What counts, for instance, as privacy?[362] Does it matter how the public safety benefits of a surveillance program are distributed?[363] Experts cannot be perfectly neutral analysts because analysis always presupposes certain contestable value judgments. Nevertheless, experts can still build frontiers that are useful to the decisionmaker. This is true even if the experts neither know the preferences nor

360. *Id.* at 27. The tradeoff thesis has proved controversial, but its critics have not undermined its core insight: that there is always a point at which security and liberty (or some other value) conflict. *See* Adrian Vermeule, *Security and Liberty: Critiques of the Trade-Off Thesis*, *in* THE LONG DECADE: HOW 9/11 CHANGED THE LAW 31, 31-34 (David Jenkins et al. eds., 2014) (discussing and responding to various critiques of the tradeoff thesis).

361. *Cf.* W.B. Gallie, *Essentially Contested Concepts*, 56 PROC. ARISTOTELIAN SOC'Y (N.S.) 167, 169 (1956) (discussing the class of "concepts which are essentially contested, concepts the proper use of which inevitably involves endless disputes about their proper uses on the part of their users").

362. *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 489 (2006) (developing a taxonomy of privacy around "four basic groups of harmful activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion," each of which "consists of different related subgroups of harmful activities").

363. *See* Pozen, *supra* note 213, at 229 (noting the "distributional tradeoffs" that occur when "a policy . . . shift[s] privacy burdens or benefits from one group in the population to another" (emphasis omitted)).

are representative of the decisionmaker. For example, the average American (or member of Congress) might want more logging in our national parks than does the National Park Service bureaucrat who writes the relevant official report. But that report can still be useful in laying out, in a reasonably objective way, what the relevant tradeoffs are, even if it is not the last word on the matter. Part IV.A considers how surveillance intermediaries contribute and detract from the goal of constructing the most accurate frontier.

By contrast, the problem of frontier choice is one of *legitimacy*: What set of procedures will legitimately aggregate social preferences (taking into account side constraints like individual rights or constitutionally imposed structural requirements)? In other words, in a world of preference pluralism—where Alice cares a lot about public safety and is largely indifferent to the privacy harms that come from surveillance, while Bob feels the opposite—how do we pick the best point on the frontier? The standard approach in welfare economics is to posit a benevolent "social planner" who can aggregate individual preferences and identify what point along the frontier maximizes social welfare. But in reality there is no such social planner, and instead we rely on democratic constitutional politics. Thus, the question of frontier choice, the subject of Part IV.B, is whether the activities of surveillance intermediaries contribute to or detract from the practice of democratic constitutional politics in setting surveillance policy.

A. Frontier Construction

The *true frontier* is the frontier we would construct if we knew all the relevant facts and understood all the applicable dynamics between the various values we're trying to optimize: security, privacy, equity, economic growth, innovation, and so on. In the real world we lack such information and so can't construct the true frontier. Instead we settle for a *working frontier*, which will have some deviations from the true frontier. But the ideal of the true frontier is useful because it gives us a criterion by which we can normatively evaluate and rank different working frontiers: One working frontier is better than another if it more closely approximates the true frontier.

Let's start with the good: When surveillance intermediaries resist government surveillance, they can help bring the working frontier closer to the true frontier. The first way they do this is by generating information about how much surveillance is underway; we can't hope to optimize tradeoffs if we don't have accurate information about what those tradeoffs entail. I described above how transparency reports and other public reporting by surveillance intermediaries provide a trove of granular data.[364] Their resistance can also

364. *See supra* notes 263-76 and accompanying text.

prompt the disclosure of information, especially during litigation. For example, Apple's refusal to comply with the iPhone All Writs Act orders revealed how many times the government had previously asked Apple to unlock iPhones.[365] The litigation also led the Manhattan District Attorney to talk publicly about the hundreds of iPhones his office was unable to unlock.[366] Finally, public and noisy resistance to government surveillance by politically, culturally, and economically influential technology companies gets the attention of Congress and other institutions that check the surveillance executive. And the scrutiny they apply to the surveillance executive can spur the release of more information, whether in the form of congressional hearings, reports by oversight boards and inspectors general, or the surveillance executive's own voluntary disclosures.

In addition to raising awareness of the scope of surveillance, surveillance intermediaries help us understand its costs, especially the economic ones. To the surveillance executive, these costs are secondary concerns because they don't bear on the primary missions of public safety and national security. Thus, by virtue of its institutional position and perspective, the surveillance executive will tend to systematically underestimate—or at least deprioritize—important issues like the global economic competitiveness of U.S. technology companies.[367] I don't mean this as a criticism; ensuring public safety and national security is hard enough, and the surveillance executive's success in fulfilling its mission relies on its specialization. But that means that someone else has to zealously advocate for the legitimate economic issues at stake. Surveillance intermediaries help make sure that happens by explaining their concerns in public, providing more detailed information directly to the surveillance executive, and empowering what would otherwise be secondary government actors like the Department of Commerce and the National Economic Council. These added perspectives help realize Rascoff's observation that "[i]nterest group contestation in [the intelligence] area can be an important tool for allowing multiple viewpoints to be aired and normative judgments to be appropriately calibrated."[368] In other words, although with respect to surveillance policy (and indeed every other regulatory domain) the executive

365. *See supra* text accompanying note 145.

366. *See It's Not Just the iPhone Law Enforcement Wants to Unlock*, NPR (Feb. 21, 2016, 7:57 AM ET), https://perma.cc/E36G-YN7W (discussing, in an interview with Manhattan District Attorney Cyrus Vance Jr., the office's difficulty unlocking phones running iOS 8).

367. *See, e.g.*, Jason Healey, *The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers*, J. INT'L AFF. 14 (2016), https://perma.cc/67RV-ZPJJ (noting that "[i]t might not be the job of [U.S. intelligence] agencies to care about the security of the Internet and U.S. commercial concerns" but acknowledging that "these objectives have been a stated priority for the last three administrations back to 1998").

368. Samuel J. Rascoff, *Domesticating Intelligence*, 83 S. CAL. L. REV. 575, 629-30 (2010).

branch is "the most knowledgeable" branch,[369] surveillance intermediaries can yet make it smarter.

To be sure, technology companies are just as vulnerable as surveillance agencies to biases and other cognitive distortions, albeit in the opposite direction. If surveillance agencies tend to underestimate the economic costs of surveillance, surveillance intermediaries tend to underplay the security risks that come from diminished government access to data. But through the wisdom of crowds, collective biases might increasingly cancel out as the sources of information that feed a decision get more diverse. And until recently, the greatest institutional sources of power were firmly behind the national security and public safety sides of the ledger, with only poorly resourced civil society groups left to push other important interests. Thus, adding surveillance intermediaries' cognitive resources, biases and all, into the process of setting surveillance policy will likely improve the accuracy of the working frontier.

The second way surveillance intermediaries push societies toward the true frontier is by spurring structural innovations that avoid what Cass Sunstein calls "gratuitous costs": for instance, situations in which "some forms of surveillance produce no benefits or only de minimis benefits."[370] Avoiding gratuitous costs often requires institutional change, but because institutions naturally resist change and require strong incentives to reform their practices, gratuitous costs can stick around indefinitely as the institutions that generate them stay mired in a suboptimal equilibrium. But surveillance intermediaries have the necessary power—either on their own or in conjunction with government actors—to force the needed change. As an example of avoiding a gratuitous cost, Sunstein cites the recommendation of the Obama-era President's Review Group on Intelligence and Communications Technologies, of which he was a member, to shift retention of bulk telephony metadata from the government to private companies.[371] The USA FREEDOM Act, passed with the strong support of surveillance intermediaries, accomplished just

369. *Cf.* Sunstein, *supra* note 327, at 1607-08 (capitalization altered).

370. Cass R. Sunstein, Essay, *Beyond Cheneyism and Snowdenism*, 83 U. CHI. L. REV. 271, 287 (2016).

371. *See id.* at 288 (arguing that the recommendation "would deprive the government of exactly nothing that it is important for the government to have, while also providing a layer of protection against risks to privacy and free speech"); *see also* RICHARD A. CLARKE ET AL., PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 17 (2013), https://perma.cc/2UTH-7KTQ.

that.[372] Today the government can still access the data it needs, but the data is held by the companies themselves, which is thought to decrease the possibility of government abuse.

Innovations can also occur at the technological level. For example, some believe (though this is a minority view) that end-to-end encryption systems can be designed to accommodate lawful government access without meaningfully degrading security.[373] And the emerging technique of "homomorphic encryption" might in the future allow data to be processed (potentially for law enforcement or foreign-intelligence purposes) while in an encrypted state.[374] Of course, these techniques will never come to practical fruition without a great deal of expensive research and development. It's precisely the resistance of surveillance intermediaries to government surveillance that creates a market for such research and development, whether by the government, the private sector, or academia.

Finally, surveillance intermediaries can ensure that we're actually abiding by the tradeoff set rather than settling for inefficient alternatives (visualized in the standard diagram as a point below the frontier). In their model, Posner and Vermeule argue that "[o]rdinary politics will usually move government to or near the security frontier, rather than producing policies that fail to exploit mutual gains,"[375] but they concede that there are "rare cases" in which "policymaking gets stuck below the frontier."[376] Whether these cases are in fact rare or commonplace,[377] surveillance intermediaries can help ameliorate them. In particular, by scrutinizing government requests, intermediaries discipline requesting agencies to ask for only the information they truly need, or, in other words, to minimize the privacy costs for a given surveillance activity. Surveillance intermediaries also empower those within the government who oversee the surveillance executive, giving them extra

372. *See supra* note 74 (discussing the Act's provision ending bulk telephony metadata collection); *supra* note 272 and accompanying text (discussing surveillance intermediaries' support for the Act).

373. *See, e.g.*, Matt Tait, *An Approach to James Comey's Technical Challenge*, LAWFARE (Apr. 27, 2016, 7:00 AM), https://perma.cc/GE53-PV6A (proposing a cryptographic system built around nested "cryptographic envelopes"). *But see supra* text accompanying note 218.

374. For a nontechnical overview of the latest generation of homomorphic systems, see generally Brian Hayes, *Alice and Bob in Cipherspace*, 100 AM. SCIENTIST 362 (2012).

375. POSNER & VERMEULE, *supra* note 355, at 33.

376. *Id.* at 34.

377. *Cf.* WITTES & BLUM, *supra* note 213, at 129 (criticizing Posner and Vermeule's account on the grounds that "it is just not the case that functional democracies necessarily optimize the blending of security and liberty" and that "Posner and Vermeule overstate the extent to which democracies never miss opportunities—even significant ones—to enhance both liberty and security").

leverage to make sure their agencies are similarly minimizing their economic, privacy, and civil liberties footprints.[378]

But at the same time that resistance to surveillance by technology giants improves some aspects of the decisionmaking process, it can also create negative second-order surveillance effects that may not be captured in the working frontier. Unless these surveillance-surveillance tradeoffs[379] are recognized, they will distort the policymaking process.

One unintended consequence flows from the hydraulic nature of surveillance: Like water under pressure (here the imperatives—real or perceived—of public safety and national security), surveillance tends to force its way around obstacles, reappearing in unexpected places and often making a bigger mess than if it had been allowed to flow freely. Consider three examples:

First, by shielding overseas data from U.S. law enforcement agencies, *Microsoft Ireland* incentivizes foreign countries to impose data localization measures.[380] The effect is a net loss for global privacy (not to mention economic efficiency) given that the United States's data privacy regime is far stronger than those of most countries.[381]

Second, in *Riley v. California* (widely considered a victory for digital privacy[382]), the Supreme Court held that the search-incident-to-arrest exception to the Fourth Amendment's warrant requirement did not extend to searches of cellphones seized from arrestees.[383] The Court clarified, however, that police could still rely on the exigent circumstances exception to search a smartphone in a "'now or never' situation" where the alternative to the immediate search was that the evidence might become permanently inaccessible.[384] Given the realities facing police—most smartphones automatically lock after a short time, this feature can't be disabled without knowing the unlock code, and smartphone manufacturers like Apple are

---

378. *Cf.* Katyal, *supra* note 325, at 2325 ("Differing perspectives allow agencies to function more like laboratories, by devising new solutions to new problems. . . . Without bureaucratic overlaps, agencies are not pushed to develop innovative ways of dealing with problems and may ossify.").

379. *Cf. supra* text accompanying note 213.

380. *See* Daskal, *supra* note 32, at 390.

381. *See* Woods, *supra* note 32, at 751-53. Even when compared with Europe, which has particularly high levels of privacy protection for personal data, the United States imposes greater restrictions on law enforcement access to such data. *See* Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the U.S. Are "Stricter" Than Each Other for the Privacy of Government Requests for Information*, 66 EMORY L.J. 617, 636-47 (2017).

382. *See* Shawn Marie Boyne, *Stingray Technology, the Exclusionary Rule, and the Future of Privacy: A Cautionary Tale*, 119 W. VA. L. REV. 915, 916 (2017).

383. 134 S. Ct. 2473, 2484-85 (2014).

384. *See id.* at 2487 (quoting Missouri v. McNeely, 133 S. Ct. 1552, 1561 (2013)).

increasingly unable or unwilling to unlock phones—*Riley*'s exigency exception could encourage police to search smartphones at the point of arrest without any judicial oversight.[385]

Third, after a certain point, the government's demand for surveillance becomes highly inelastic. Crimes have to be solved, and intelligence has to be collected. Once the system is emptied of slack (the amount of surveillance investigators could make do without but ask for to make their lives easier), the government will try hard to surveil at the same level, even if that surveillance imposes high costs on the government or society. For example, some information security experts have proposed lawful government hacking as an answer to the "going dark" problem.[386] Although the government might still be able to limit the amount of irrelevant data obtained,[387] lawful hacking that gives the government full control over a device can reveal more of the real-time data stream than had the government requested specific categories of user data from the company. In addition, by decreasing the government's incentive to share information about vulnerabilities with the private sector (lest the government lose the ability to exploit the vulnerabilities), lawful hacking could have an overall detrimental effect on security. Most generally, if surveillance intermediary resistance to surveillance resulted in a catastrophic terrorist attack or a sharp increase in crime (whether in reality or merely in the public imagination), the government's response could be to sharply increase surveillance past the level it would have sought had the intermediaries cooperated in the first place. The net result could be a further loss of civil liberties.[388]

The second important category of unintended consequences comes from surveillance intermediaries' own surveillance. Whatever one thinks about the scope of U.S. surveillance practices, technology companies have far more access to our data, and thus know far more about us, than does the government.[389]

385. *See* Orin Kerr, *Apple's Dangerous Game*, WASH. POST: VOLOKH CONSPIRACY (Sept. 19, 2014), https://perma.cc/H5ST-DKWL.

386. *See* Bellovin et al., *supra* note 240, at 5 ("Instead of building wiretapping capabilities into communications infrastructure and applications, government wiretappers can behave like the bad guys. That is, they can exploit the rich supply of security vulnerabilities already existing in virtually every operating system and application to obtain access to communications of the targets of wiretap orders."); *cf.* Herb Lin, *A Biometric Approach as a Partial Step Forward in the Encryption Debate*, LAWFARE (Dec. 3, 2015, 3:22 AM), https://perma.cc/G3PJ-MVD7 (suggesting that biometric encryption would enable the government to access data belonging to a suspect in custody without the security downsides of giving the government a traditional decryption key).

387. *See* Bellovin et al., *supra* note 240, at 33-35.

388. *See* Sunstein, *supra* note 370, at 281, 285.

389. *See, e.g.*, WU, *supra* note 210, at 323 ("[S]everal commercial entities [are] now compiling ever more detailed dossiers on every man, woman, and child. It is a more thoroughly invasive effort than any NSA data collection ever disclosed—and one of even more

footnote continued on next page

Even as companies deploy end-to-end encryption and thus cut themselves off from some of our data, Google knows all our searches, and Facebook all our friends. And unlike the government, these companies are free to use this data for purely commercial purposes, such as selling advertisements. Thus it's no surprise that these companies have come under heavy criticism from privacy advocates.[390] Resisting government surveillance gives these companies the opportunity to recast themselves as champions of user privacy and thus get away with more user surveillance than the public might otherwise allow. And as noted above, companies frequently use opposition to government surveillance to improve their reputation with privacy groups.[391]

In the end, whether the net effect of surveillance intermediary resistance on frontier construction is positive or negative depends on whether its good effects outweigh its bad ones. This is another of the empirical questions that is hard to answer without a larger sample of case studies. My guess is that at least so far, the benefits—the disciplining effects on government officials and the addition of new information into the policymaking process—have outweighed the costs. But there's no guarantee that this positive state of affairs will remain the case. The overall picture is dynamic, and there's no reason to think that the current arrangement represents an equilibrium. Stay tuned.

B. Frontier Choice

Recall the difference between creating a frontier and picking a policy along its perimeter. Specifically, the more a working frontier—the one from which we choose policy—approximates the true frontier, the better that working frontier is. The legitimacy of a specific policy choice *along* that frontier is judged by an altogether different standard; what's important is that the policy be chosen through constitutional democratic politics.

By constitutional democratic politics I mean nothing more than how Americans, at a high level, ordinarily make large-scale policy decisions: democratic politics subject to the constitutionally imposed constraints regarding structure and individual rights. I'm intentionally defining constitutional democratic politics at a high level because I want to avoid debates about how institutions should be structured to better realize democratic and constitutional values. I'm thus agnostic as to whether decisions

dubious utility."); Philip B. Heymann, *An Essay on Domestic Surveillance*, 8 J. NAT'L SECURITY L. & POL'Y 421, 421 (2016) ("After all, the government probably gathers only a fraction of what private organizations do to learn about our interests, concerns, etc. for their commercial purposes, knowledge they use to create and sell new products and services.").

390. For a good recent statement, see SCHNEIER, *supra* note 29.

391. *See supra* text accompanying note 196.

should be made at the state versus federal levels, or in Congress versus the administrative agencies, or in the political branches versus the courts. It's enough that the government enact a law, or an administrative agency promulgate a regulation, or a court rule on some legal issue. The point is to contrast public sphere decisions—those made through government process—with private sphere decisions—those made by private actors operating in the market. Only if surveillance policy is set by public sphere decisions can we ensure *surveillance self-government*.

This Subpart has three components. The first defends the proposition that the level and type of government surveillance should be determined through public sphere, rather than private sphere, decisionmaking. The second describes the ways that surveillance intermediaries both enhance and detract from surveillance self-government. And the third offers some preliminary thoughts on how to curb technological unilateralism's negative effects on surveillance self-government.

1. Surveillance self-government defended

As long as government surveillance is set de jure through public sphere decisionmaking, why should we object if the private sphere sets government surveillance de facto? Might that not in fact be a benefit? If Apple adds end-to-end encryption to its iPhones and people keep buying them, doesn't that suggest that end-to-end-encrypted iPhones are good for society? After all, we generally trust markets, through competition and the price mechanism, to efficiently allocate scarce resources and make tradeoffs among competing values so as to maximize overall utility. And with respect to communications technology, a certain amount of faith in the market is certainly justified. It's because the market did such a good job at innovating that we're willing to turn our data over to surveillance intermediaries. And it's precisely this willingness that makes electronic surveillance so useful to the government. The market giveth and it taketh away. What's the problem?

There are three. First, as an empirical matter, we can't infer from the economic success of surveillance intermediaries that the market assigns a high value to technologies that enhance security and privacy at the extreme margin of frustrating government surveillance. Despite all the publicity around security-enhancing technologies, we don't know whether consumers actually care about them—that is, whether they buy the new iPhone because it has end-to-end encryption rather than because it has a bigger screen. As a rule, communication services that have marketed themselves on the basis of their security features have struggled.[392] Contrary to what consumers tell

392. *See* Samuel Gibbs, *We Know People Care About Privacy, So Why Won't They Pay for It?*, GUARDIAN (July 8, 2016, 3:00 EDT), https://perma.cc/VEB8-6FF7; Declan McCullagh,
footnote continued on next page

technology journalists, their revealed preferences suggest that they often care less about improvements to privacy and security than about useful features and free service.[393]

Second, as a structural matter, markets are bad at internalizing socially diffuse, long-run values like security (or for that matter, privacy[394]). This is clear from other regulatory domains, such as the environment, in which an unregulated market can lead to dramatic negative externalities.[395] Security has social dimensions the market can't capture. If a murder goes unsolved because the evidence is on a locked iPhone,[396] the market can't force Apple to internalize the cost to public safety of its choice to implement end-to-end encryption.

Third, as a conceptual matter, the market is the wrong forum in which to litigate questions of fundamental government structure. This is easiest to demonstrate if one accepts that large-scale markets, even (and especially) ones that call themselves "free," are always creatures of an underlying set of political choices and governmental action.[397] But even if you're unwilling to go that far,

---

It's Been 10 Years: Why Won't People Pay for Privacy?, CNET (Jan. 28, 2010, 10:55 AM PST), https://perma.cc/L5F3-LUAL.

393. *Cf.* Benjamin Wittes & Jodie C. Liu, Ctr. for Tech. Innovation at Brookings, The Privacy Paradox: The Privacy Benefits of Privacy Threats 10-15 (2015), https://perma.cc/WW2Z-ZKP3 (discussing the highly sensitive search queries that consumers enter into Google).

394. *See* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 387, 425 (2015) (arguing that "privacy is a public good" that "requires group coordination"); Michaels, *supra* note 14, at 937-38.

395. *See* Jedediah Purdy, *Coming Into the Anthropocene*, 129 HARV. L. REV. 1619, 1642 (2016) (book review). Indeed, the environmental analogy has entered the political discussion over law enforcement access to encrypted data. As Senator Sheldon Whitehouse argued during a hearing on the "going dark" issue:

> It strikes me that one of the balances that we have in these circumstances where a company may wish to privatize value by saying, "Gosh, we're secure now. We got a really good product. You're going to love it"—that's to their benefit. But for the family of the girl that disappeared in the van, that's a pretty big cost. And when we see corporations privatizing value and socializing cost so that other people have to bear the cost, one of the ways that we get back to that and try to put some balance into it, is through the civil courts, through a liability system. If you're a polluter and you're dumping poisonous waste into the water rather than treating it properly, somebody downstream can bring an action and can get damages for the harm that they sustain, can get an order telling you to knock it off . . . .

Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy at 1:20:47-1:21:55, COMMITTEE ON JUDICIARY (July 8, 2015), https://perma.cc/V4HX-WMD7 (statement of Sen. Whitehouse during testimony of James B. Comey, Jr., Director, FBI).

396. *See, e.g.*, Peter Holley, *A Locked iPhone May Be the Only Thing Standing Between Police and This Woman's Killer*, WASH. POST (Feb. 26, 2016), https://perma.cc/24SS-J5KM.

397. *Cf., e.g.*, Cohen, *supra* note 250, at 388 ("Markets are structured by and depend on the stability of regulatory institutions . . . .").

it's still the case that many political arrangements—especially structural ones—cannot be reformulated as market transactions. Although answers to structural questions must obviously be informed by market realities (because such realities might constrain what is possible to achieve), they cannot logically be dictated by them. We would not be content with the market deciding whether government should be able to collect taxes or enforce civil rights or wage war; we properly view these as public sphere questions that should be resolved through democratic and constitutional politics. If the market gets in the way, we often take that as a reason to change not our politics, but instead the market. Indeed, the twentieth century's great constitutional innovation—the New Deal settlement—was about precisely this issue: It affirmed that the government would have the powers it needed to fundamentally reshape a market whose harsh contours society was no longer willing to accept.[398]

What's left is to recognize that these questions of fundamental government structure encompass the issue of government surveillance—specifically, what forms of surveillance we expect, even demand, the government to conduct. This fact is often overlooked because when we talk about government surveillance as a matter of constitutional law, we do so in the context of the Fourth Amendment. Thus we naturally limit ourselves to questions about what the Constitution *prohibits* rather than what it affirmatively *authorizes*. But this focus obscures the fact that our system is not meant merely to "incapacitat[e]" by "eliminating or withholding some of the tools or resources that contribute to state capacity";[399] rather, our system seeks to simultaneously "build and constrain state power."[400] Nor does the Fourth Amendment place a thumb on the scale against surveillance; it rather seeks to introduce a balancing mechanism. Thus, when applying the Fourth Amendment through its command that searches and seizures be "reasonable" (as courts increasingly do[401]), courts' evaluation of government activity is "relaxed and deferential,"[402] in contrast to the more demanding tests, such as strict or intermediate scrutiny, often used when government action implicates constitutional rights.[403] And the Fourth Amendment permits warrants—which at the Founding were a

398. *Cf.* David Freeman Engstrom, *"Not Merely There to Help the Men": Equal Pay Laws, Collective Rights, and the Making of the Modern Class Action*, 70 STAN. L. REV. 1, 18 n.70 (2018) (discussing the New Deal as a period "when the federal government substantially expanded its coordination of the economy").

399. *See* Daryl J. Levinson, *Incapacitating the State*, 56 WM. & MARY L. REV. 181, 197 (2014).

400. *See id.* at 206.

401. *See* Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133, 1134 (2012).

402. Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness,"* 98 COLUM. L. REV. 1642, 1687 (1998).

403. *See* Kenji Yoshino, *The New Equal Protection*, 124 HARV. L. REV. 747, 755-56 (2011).

powerful grant of immunity to federal officials from civil trespass liability[404]—merely on the basis of probable cause and particularity (and not, for instance, on the severity of the crime being investigated or the necessity of the search or seizure to the investigation).[405]

The flip side of these substantive and procedural limitations is that once the government satisfies its legal obligations (not just under the Fourth Amendment but also under other constitutional provisions as well as applicable statutes and regulations), it is entitled to the information it seeks. It is entitled because the government represents the people, and targets of surveillance have a communitarian obligation to the people that permits their surveillance for lawful purposes. Corresponding to this obligation is a public entitlement: the principle, invoked most frequently in the context of the grand jury's broad subpoena power,[406] but applicable more broadly, that "the public . . . has a right to every man's evidence."[407]

If this sounds radical, it's only because our terminology gets in the way. Because our cultural discourse around the Constitution (unlike the Constitution itself) emphasizes rights *from*, rather than *to*, government power, choosing to sacrifice civil liberties for security is borderline taboo. To resolve this cognitive dissonance, we often call the surveillance we want something other than "surveillance," so we can conveniently forget what it is we've asked for. Thus, as Benjamin Wittes and Gabriella Blum note, "When we station a police officer to patrol an inner-city playground, we call it 'community-oriented policing.' When we scan letters for anthrax spores, which the US Postal Service began doing after the anthrax attacks, we call it 'screening,' a word we also use to describe airport security measures."[408] Wittes and Blum criticize this "trick [as] comforting but mindless."[409] And they continue: "There are countless examples of communities and society as a whole making similar choices—often requiring sustained, serious surveillance—in the interests of liberty as they perceive it."[410] Surveillance may be a necessary evil, but in that way it is no different from other exercises of the government's coercive power

404. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 777-78 (1994).

405. *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

406. *See, e.g.*, Amar, *supra* note 404, at 783.

407. *See* United States v. Bryan, 339 U.S. 323, 331 (1950) (quoting 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2192 (3d ed. 1940)).

408. WITTES & BLUM, *supra* note 213, at 186.

409. *Id.*

410. *Id.*

for regulatory purposes.[411] When the government has chosen a social or economic policy that is appropriate and lawful in both its content and how it was chosen, we expect that the government will carry it out, including by enforcing it against recalcitrant private actors, be they individuals or companies. Surveillance is no different.

2. Surveillance intermediaries' effects on surveillance self-government

Surveillance intermediaries both enhance and detract from surveillance self-government. The positive side of the ledger is substantial and should not be understated. To begin with, surveillance intermediaries enhance the public's engagement with surveillance policy. By generating information on government surveillance, providing a richer accounting of its costs and benefits, and focusing attention on the issue through litigation and political mobilization, intermediaries counter the voter ignorance that is so harmful to democratic government.[412]

In addition, by empowering actors within the government that can check executive branch surveillance—whether the other branches of government or intra-executive actors—surveillance intermediaries help ensure that a wider (and thus more representative) cross-section of the government generates surveillance policy.

Finally, surveillance intermediaries address the problem of "who watches the watchers?" by helping to ensure that the surveillance executive abides by the law. Surveillance intermediaries reject surveillance requests that are obviously defective, and their reputation within the surveillance executive for recalcitrance incentivizes the government to act with extra care. And by bringing justiciable cases, intermediaries help courts enforce surveillance law.

What all these positive effects have in common is that they don't come from surveillance intermediaries acting alone. Proceduralism, litigiousness, and policy mobilization either operate on or through the government—Congress, the courts, or the executive branch—or the public itself. This is the reason they are compatible with, and indeed can enhance, surveillance self-government.

By contrast, technological unilateralism—end-to-end encryption, data offshoring, and so on—makes surveillance more difficult solely on the will of the surveillance intermediaries. Not only does it impede the enforcement of

411. *See* Rascoff, *supra* note 368, at 584-85 (arguing that "domestic intelligence is essentially a regulatory activity"); Sunstein, *supra* note 370, at 283 (arguing for a "risk management" model of national security).

412. For a discussion of how voter ignorance harms democracy, see ILYA SOMIN, DEMOCRACY AND POLITICAL IGNORANCE: WHY SMALLER GOVERNMENT IS SMARTER (2d ed. 2016).

public policy, but its distinctive advantages as a technique of resistance also have the second-order effect of interfering with future policymaking; because technology is sticky, creates path dependencies, and can be implemented (and reimplemented) faster than government can respond to it,[413] it's costlier to regulate technology than it is to regulate other fields. The resulting democratic deficit arises even when intermediaries are engaging in perfectly legal behavior—for example, encrypting data or storing it outside the country—or acting for reasons unrelated to thwarting government surveillance.

The democracy-based critique of surveillance companies' technological unilateralism has largely been ignored. One reason for this is that companies often carefully cast their resistance as inevitable technological improvements, not contestable political arguments. In the San Bernardino dispute, Apple framed its opposition to the FBI's request as a consequence of the technological superiority of end-to-end encryption, not an objection as such to law enforcement access to smartphones.[414] When Microsoft stores data outside the United States, it is careful not to say that it does so to put the data outside the reach of domestic warrants; rather, it emphasizes that it's more efficient to store data next to where users (claim to) live.[415] Similarly, the most influential public defense of end-to-end encryption from the security research community was framed largely in terms of technology, not politics.[416] Public debate over encryption and other security technologies has been dominated by what computer scientist Arvind Narayanan has called "crypto-for-security" framing, which focuses on the security of communications and data.[417] This is in contrast with "crypto-for-privacy," which "often has social and political goals" like opposing government surveillance, and which gets substantially less public exposure.[418]

Only a few companies, like WhatsApp, and a handful of Silicon Valley influencers, like Marlinspike and Rogaway, are willing to say what many engineers feel: Government surveillance has become excessive, and the playing field needs to be rebalanced in the direction of user privacy.[419] This reticence to

413. *See supra* notes 248-52 and accompanying text.

414. *See* Apple's Motion to Vacate, *supra* note 6, at 1-5.

415. *See, e.g.*, Brief for Appellant, *supra* note 197, at 11 ("To address the problem [of network latency], Microsoft built datacenters closer to its customers and endeavors to store customers' communications at the closest datacenter.").

416. *See* ABELSON ET AL., *supra* note 31, at 2.

417. *See* Arvind Narayanan, *What Happened to the Crypto Dream?, Part 1*, IEEE SECURITY & PRIVACY, Mar./Apr. 2013, at 75, 75.

418. *See id.*

419. *See* Metz, *supra* note 91 ("There was a middle period where the government had a broad ability to surveil, but if you look at human history in total, people evolved and civilizations evolved with private conversations and private speech. If anything, we're

footnote continued on next page

openly confront the political implications of security technology is unlike the early days of public-key cryptography, when crypto-anarchists and "cypherpunks" explicitly presented cryptography as a way to empower the individual at the expense of the state.[420] It is also unfortunate because it obscures, for all sides, the fact that "cryptographic work is deeply tied to politics."[421] As Phil Zimmerman, the creator of the encryption program PGP and co-founder of the secure-communication service Silent Circle, explained: "[I]n the Information Age, cryptography is about political power, and in particular, about the power relationship between a government and its people."[422] And in our system, absent extraordinary circumstances, the only legitimate politics is democratic politics.

One could object that we find ourselves in such extraordinary circumstances: that our current surveillance regime does not in fact reflect democratic preferences, so resistance by surveillance intermediaries is, although a second-best corrective, useful and normatively justifiable. But both this premise and remedy are highly contestable.

As to the premise, critics of government surveillance have not demonstrated that current levels of surveillance are so out of line with public preferences that it's worth incurring further democratic deficits to fix the problem. Unsurprisingly for such a complicated and technical issue, polls paint a picture of public opinion as muddled and at times incoherent,[423] as well as

bringing that back to individuals [by using end-to-end encryption in WhatsApp]." (quoting Brian Acton, Co-founder of WhatsApp)); Rogaway, *supra* note 92, at 25-30; *We Should All Have Something to Hide, supra* note 95.

420. *See* THOMAS RID, RISE OF THE MACHINES: A CYBERNETIC HISTORY 257 (2016). Given their radical political libertarianism and suspicion of state power, it is unsurprising that the crypto-anarchists and cypherpunks borrowed the slogans of the gun lobby; hence the famous war cries "crypto = guns" and "[i]f crypto is outlawed, only outlaws will have crypto." *Id.* at 258, 269.

421. *See* Rogaway, *supra* note 92, at 3.

422. SIMON SINGH, THE CODE BOOK: THE EVOLUTION OF SECRECY FROM MARY QUEEN OF SCOTS TO QUANTUM CRYPTOGRAPHY 296 (1999) (quoting PHILIP R. ZIMMERMANN, THE OFFICIAL PGP USER'S GUIDE, at xvi (2d prtg. 1995)).

423. *See, e.g.*, George Gao, *What Americans Think About NSA Surveillance, National Security and Privacy*, PEW RES. CTR. (May 29, 2015), https://perma.cc/4JF8-VMSH ("Fourteen years after the Sept. 11 terrorist attacks, and two years after Edward Snowden's revelations about extensive U.S. government surveillance of phone and internet data, Americans continue to have mixed—and sometimes conflicting—views about government surveillance programs.").

highly sensitive to how the question is framed[424] and to contextual factors like perceptions of threat and trust in government.[425]

Better evidence comes from the aftermath of national security surveillance disclosures. When a secret surveillance program becomes public, its ultimate legislative fate is a useful test case. Because secret programs are, by definition, developed in secret, the risk of agency slack—that the government will, intentionally or unintentionally, deviate from public preferences[426]—is highest. And the manner in which secret surveillance programs become public—suddenly, unexpectedly, and often with media coverage that gets important details wrong and tends to err on the side of emphasizing potential abuses—can lead to what Posner and Vermeule have called "libertarian panics."[427]

Yet the legislative aftermath of the highest-profile disclosures of secret surveillance—the disclosure of bulk telephony metadata collection under section 215 of the USA PATRIOT Act and of broad foreign-intelligence collection under section 702 of FISA—paints an equivocal picture.[428] Although the USA FREEDOM Act ended the section 215 program as it had been practiced and enshrined an anti-bulk collection principle into U.S. surveillance law,[429] it preserved the government's operational ability to analyze telephony metadata. As to section 702, its reauthorization past 2017 was still pending as this Article went to print.[430] But two important surveillance watchdogs—the Privacy and Civil Liberties Oversight Board and the Obama-era President's Review Group on Intelligence and Communications Technologies—

424. *See, e.g.*, Lee Rainie & Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RES. CTR. (Feb. 19, 2016), https://perma.cc/Z8UN-8BFJ.

425. *See* Darren W. Davis & Brian D. Silver, *Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America*, 48 AM. J. POL. SCI. 28, 43-44 (2004).

426. *See* POSNER & VERMEULE, *supra* note 355, at 98.

427. *Id.* at 77. Writing before the Snowden disclosures, Posner and Vermeule used the USA PATRIOT Act as their example of a contemporary—and in their view unjustified—libertarian panic over surveillance. *See id.* at 79-80.

428. An interesting but separate argument is Michael Glennon's claim that the career national security bureaucracy, not Congress or executive branch political appointees, sets long-term surveillance policy. *See* MICHAEL J. GLENNON, NATIONAL SECURITY AND DOUBLE GOVERNMENT 6-7 (2015). Glennon's account has a high degree of descriptive accuracy, but it does not establish that the preferences of the national security bureaucracy deviate substantially from those of the public. Nor does it establish that if those preferences *did* deviate from the public's, the political process would be unable to ultimately rein the bureaucracy in—as Congress did when it passed FISA.

429. *See, e.g.*, 50 U.S.C. § 1861(b), (c)(3) (2015).

430. *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, § 2, 126 Stat. 1631, 1631 (codified at 18 U.S.C. § 2511 (2016), 50 U.S.C. §§ 1801, 1881a-1881g) (reauthorizing section 702 until December 31, 2017).

recognized section 702's importance for U.S. national security,[431] suggesting that section 702 or something very much like it will remain a permanent part of the U.S. foreign intelligence landscape.

With regard to remedy, we shouldn't rely on surveillance intermediaries to cure any democratic deficits that may exist in surveillance policymaking. This is largely for reasons already discussed. Surveillance intermediaries often have idiosyncratic ideological views on surveillance. The market does not provide a sufficiently precise incentive for surveillance intermediaries to bring government surveillance in line with popular preferences. Surveillance intermediaries may use the opportunity to oppose government surveillance to generate trust that may ultimately prove unearned if they use it to increase their own surveillance. And in another manifestation of the hydraulic nature of surveillance, if Congress or the courts feel that surveillance intermediaries can meaningfully check the executive branch, they may relax restrictions on executive branch surveillance. In fact, they may even broaden executive surveillance authorities to compensate for this additional opposition, thus exacerbating whatever agency slack might already exist in the system.[432]

One might accept this argument and still approve of any constraint on government surveillance on the ground that current levels of government surveillance are far above what they would optimally be. Considered as bare preferences, such views are no better or worse than any others. The difficulty is in establishing that they are *correct*, and the problem is one of putting forth enough data—either quantitative or in the form of relevant case studies—for meaningful welfarist analysis. Criticism of broad surveillance programs thus struggles to get beyond high-level discussion of risks[433] or appeals to prior baselines without adequate normative defenses of those baselines, a move that Posner and Vermeule criticize as "a virulent strain of the naturalistic fallacy: whatever complex of legal rules happens to exist at some status quo point is taken to be good, and any shift in the direction of greater security is taken to be

431. *See* CLARKE ET AL., *supra* note 371, at 145; PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 65, at 2.

432. This point structurally mirrors Bill Stuntz's argument that greater procedural protections for criminal defendants can lead to harsher overall outcomes by giving legislatures incentives to stiffen criminal sentences. *See* William J. Stuntz, *The Uneasy Relationship Between Criminal Procedure and Criminal Justice*, 107 YALE L.J. 1, 51 (1997) ("Fourth Amendment law makes drug investigations somewhat costlier, because it forbids most sweeps, blanket searches, and suspicionless street stops. This may have played some part in legislatures' decisions to ratchet up drug sentences over the past generation: The costlier it is to catch offenders, the more important it is to punish them severely when caught." (footnote omitted)).

433. For an otherwise excellent example of such a discussion, see Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1945-58 (2013).

bad."[434] But as they explain, "[I]f the status quo can embody too much liberty, rather than just the right amount, that picture is arbitrary."[435]

Of course, the critics of government surveillance may still be right even if their arguments are insufficient. The United States has its own sorry history of surveillance abuses,[436] and as good Bayesian updaters we should adjust our judgments in light of new data. Thus, for instance, some have decided that in the wake of the Snowden disclosures and the outcome of the 2016 election, the risk of surveillance abuse is too high, no matter what the democratic process thinks.[437] But even if one is convinced that the tradeoff is worth making, it is still a tradeoff, and one we must recognize if we are to have an honest accounting of the costs and benefits of our current system.

3. Curbing technological unilateralism

How can we preserve the ways surveillance intermediaries enhance surveillance self-government while curbing the ways they undermine it? Specifically, how do we combat the technological unilateralism that lets surveillance intermediaries dramatically constrain otherwise lawful surveillance activity? The point is not to beat up on surveillance intermediaries for constraining government surveillance. As noted above, while there are instances where private companies oppose public policy for their own ideological purposes, there are many examples where their technological changes—including those that constrain government surveillance—are motivated primarily by a desire to improve functionality, increase security, or

434. *See* POSNER & VERMEULE, *supra* note 355, at 145.

435. *Id.*

436. *See* DONOHUE, *supra* note 23, at 4-8.

437. *See, e.g.*, Susan Landau, *Protecting the Republic: Securing Communications Is More Important Than Ever*, LAWFARE (Nov. 21, 2016, 7:54 AM), https://perma.cc/RW34-V4D2. But even on this position's own terms, technological unilateralism may not be the answer. As discussed above, surveillance's hydraulic tendencies mean that getting rid of government surveillance that relies on cooperation from surveillance intermediaries will force the government to use more intrusive means that may be more harmful to both civil liberties and information security. *See supra* notes 379-88 and accompanying text. Security researcher Matt Tait has made this point in the context of postelection debates over the appropriateness of third-party access:

> Even if I'm wrong, and the United States is now doomed to enter a dark era of top-down illegal misuse of law enforcement, with Trump able to quickly steamroll over all institutional safeguards and obstacles, civil libertarians should be lining up in support of exceptional access mechanisms; it is only by moving law enforcement towards the technically constrainable and enforceable transparency of exceptional access mechanisms and away from unconstrained, non-transparent capabilities such as device hacking that there can be any hope of technically containing or exposing a president's illegal misuse of law enforcement.

Matt Tait, *Exceptional Access in a Trump Administration*, LAWFARE (Dec. 1, 2016, 9:38 AM), https://perma.cc/7HQ3-AAMS.

decrease costs.[438] Telling companies they should respect democratic constitutional politics by itself gives them no guidance on whether to make particular technological changes.

To solve this problem, we may have to regulate the internet like we do other industries and technologies. For example, it is broadly uncontroversial that the government requires environmental assessments before a company can build a building, or safety inspections before an auto manufacturer designs a new car or a pharmaceutical manufacturer releases a new drug—though there is of course disagreement at the margin as to how rigorous those assessments should be and what substantive standards they should incorporate. Similarly, we could demand technological impact assessments before a technology company develops a product or service that disrupts a key government function like effective surveillance.[439] Indeed, CALEA provides a historical example of how regulating the telecommunications industry can satisfy law enforcement needs without crippling security or innovation.[440]

Of course, designing such a regulatory system is easier said than done (and is far outside the scope of this Article). Politically, the same power that surveillance intermediaries use to lobby Congress against surveillance will no doubt be used to oppose regulations that cut into profits.[441] The field of digital communications is still young and dynamic, and thus it is important to regulate with a light touch so as not to unnecessarily slow innovation.

438. *See, e.g.*, *supra* notes 218-22 and accompanying text.

439. Scholars have begun to explore environmental impact statements as a model for regulating information industries, especially in the context of surveillance, though their aims are to restrict surveillance, not enable it. *See, e.g.*, A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1715. But whatever the form such a regulatory regime would take, what standards it would use is a separate and even more difficult question. As Julie Cohen notes, "The tension between cost-benefit and precautionary approaches—and between the different regulatory ideologies that each has come to signify—has emerged as a defining feature of the information-era regulatory landscape." Cohen, *supra* note 250, at 393. One could imagine a spectrum of regulatory presumptions—ranging from a precautionary principle tilted toward innovation, to more "neutral" cost-benefit analysis that tries to balance economic and privacy values versus public safety and national security, to a precautionary principle tilted toward security (as could happen in the wake of an increase in crime or a serious national security incident).

440. This is not to say that CALEA has been cost free on either front, *see* Bellovin et al., *supra* note 240, at 19, 30, or that it should be straightforwardly expanded to cover encryption and other impediments to law enforcement surveillance. It is merely an argument that CALEA provides a model that is prima facie worth considering.

441. *Cf.* Eric A. Posner & Adrian Vermeule, *Inside or Outside the System?*, 80 U. CHI. L. REV. 1743, 1749 (2013) (warning against "the temptation . . . to diagnose problems by impeaching the motivations of officials or other political actors, then to propose solutions that rest on high-minded premises about the motivations of whoever [sic] the analyst is asking to supply the solutions").

Nevertheless, because digital communications will be a key site of economic and social regulation in the twenty-first century, and as the current debates over net neutrality and social media content exemplify, regulation of the internet cannot be avoided. To pretend otherwise is to adopt an "Internet-centrism" that unjustifiably assumes that the internet is—unique among technologies—immune from the pathologies, externalities, and unintended consequences of the unregulated market.[442]

In the short term, courts can, even if modestly, shape relevant doctrine in ways that promote surveillance self-government. The litigation between Apple and the FBI over the San Bernardino iPhone is a good case study of the policy considerations courts should take into account. Had the case not been mooted, the court would have been right to reject Apple's broad argument that the First Amendment prevents the government from requiring companies to modify their systems to permit government access to communications. This argument is likely to arise in future disputes between the government and surveillance intermediaries, and it exemplifies how sensitivity to the value of democratic self-government can be operationalized doctrinally; it is thus useful to look at it closely.

In its opposition to the All Writs Act order in the San Bernardino case, Apple argued that compelling it to write and digitally sign a modified operating system would violate its First Amendment right against compelled speech.[443] In particular, Apple argued that the code used to write the operating system on the San Bernardino iPhone "announced the value [Apple] placed on data security and the privacy of citizens by omitting a back door that bad actors might exploit."[444] Apple characterized the government's requested relief as "compel[ling] Apple to write new software that advances [the government's] contrary views"—that is, "viewpoint discrimination"—and argued that the government could not satisfy the attendant strict scrutiny standard.[445]

Whatever the doctrinal merits of Apple's position,[446] it illustrates the dangers of technological development unfettered by the demands of democratic self-government. The logic of Apple's argument could potentially give any company a First Amendment argument against any government regulation. After all, given the prevalence of computers in modern life, it is

442. *See* EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM 15-16 (2013).

443. *See* Apple's Motion to Vacate, *supra* note 6, at 32-34.

444. *Id.* at 33.

445. *Id.* at 33-34.

446. For useful analysis of Apple's doctrinal arguments, see Andrew Keane Woods, *Trust, Apple, and the First Amendment*, LAWFARE (Feb. 23, 2016, 5:44 PM), https://perma.cc/J6K4-FMH2; and Neil Richards, *Apple's "Code = Speech" Mistake*, MIT TECH. REV. (Mar. 1, 2016), https://perma.cc/5QY5-9Q7H.

difficult to imagine any large-scale regulation of economic activity that would not involve the writing of computer code of one sort or another.[447] Of course, a company might have to prove that it has an ideological, rather than merely economic, objection to the regulation at issue, and the regulation might still survive strict scrutiny.[448] But even the *prospect* of heightened constitutional scrutiny would upend the post-New Deal settlement in constitutional law; rather than reserve heightened judicial scrutiny for the narrow class of cases that implicate individual rights and apply the highly deferential rational basis review to most economic regulations, the courts would transmogrify large swaths of economic regulation into restrictions on free speech.[449] The result would be a Silicon Valley *Lochner*ism that replaces the Fifth Amendment's due process guarantees with the First Amendment's free speech protections.[450]

Political realities make Apple's decision not to cite *Citizens United*[451] in its brief understandable. But Apple's argument is a natural extension of the Supreme Court's defense of corporations' broad First Amendment rights.[452] In

447. *See* Richards, *supra* note 446 ("If courts were to accept the simple proposition that 'Code = Speech,' regulation of our digital society would become very difficult as well, because so much of our society depends on computer code to function.").

448. *Cf.* Adam Winkler, *Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts*, 59 VAND. L. REV. 793, 795-96 (2006) ("Courts routinely uphold laws when applying strict scrutiny, and they do so in every major area of law in which they use the test. . . . Rather than 'fatal in fact,' strict scrutiny is survivable in fact.").

449. *See* Robert Post, *Participatory Democracy and Free Speech*, 97 VA. L. REV. 477, 477 (2011) ("If every state regulation touching on what we call, in ordinary language, 'communication' were to be subject to constitutional review under the standards of the First Amendment, large swaths of perfectly common forms of regulation would be constitutionalized."). Courts have recognized similar points. *Cf., e.g.*, United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1128 (N.D. Cal. 2002) ("In the digital age, more and more conduct occurs through the use of computers and over the Internet. Accordingly, more and more conduct occurs through 'speech' by way of messages typed onto a keyboard or implemented through the use of computer code when the object code commands computers to perform certain functions. The mere fact that this conduct occurs at some level through expression does not elevate all such conduct to the highest levels of First Amendment protection. Doing so would turn centuries of our law and legal tradition on its head, eviscerating the carefully crafted balance between protecting free speech and permissible governmental regulation.").

450. *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1211-17 (2005); *cf.* Amanda Shanor, *The New* Lochner, 2016 WIS. L. REV. 133 (characterizing the growth of First Amendment protections for commercial speech as a "new *Lochner*"). *See generally* Lochner v. New York, 198 U.S. 45 (1905), *overruled by* W. Coast Hotel Co. v. Parrish, 300 U.S. 379 (1937).

451. Citizens United v. FEC, 558 U.S. 310 (2010).

452. *See, e.g., id.* at 342-43, 365. The media generally ignored this angle of the dispute, though it was not lost on all commentators. *See, e.g.*, John Villasenor, *Some Key Issues in the Apple iPhone Decryption Matter*, FORBES (Feb. 21, 2016, 5:09 PM), https://perma.cc/4S3U-YX3R (contending that *Citizens United* "offers strong support for Apple"); *cf.* Chelsea Langston,

footnote continued on next page

fact, Apple's argument is far more extreme than the holding of *Citizens United*; it goes beyond political speech and into the world of basic, everyday economic activity.[453] On the ground of democratic self-government, Apple's argument represents a deeply unattractive reading of the First Amendment, and courts should reject it.

Ultimately, I don't have a comprehensive answer for how to balance technological innovation with accountability to society as a whole. But recognizing the problem—the purpose of this Subpart—is a start. As David Singh Grewal reminds us, we must subject to "critical scrutiny" any "large-scale social structures [that] emerge through the accumulation of decentralized, individual decisions without necessarily involving political intervention."[454] Such vigilance is especially warranted when the individuals involved are a handful of giant, profit-driven corporations. We may, and in many cases likely will, decide that the social changes are worth embracing. But we should never assume that they cannot, or ought not, be constrained and shaped by values of democratic self-government.

Conclusion

In this Article, I argued that *surveillance intermediaries*, the small group of giant technology companies that provide the vast majority of consumer digital communications and data processing services, meaningfully constrain the government's ability to conduct electronic surveillance. Financial and ideological incentives drive three categories of resistance: (1) *proceduralism*, the refusal to cooperate with the government outside formal process, and *litigiousness*, a willingness to challenge the government in court; (2) *technological unilateralism*, architectural changes that make government surveillance more difficult; and (3) *policy mobilization*, the use of traditional social and political influence, along with public dissemination of data on government surveillance, to change surveillance policy. In the process surveillance intermediaries help ensure that the *surveillance executive* is checked by other governmental actors, whether *interbranch* (Congress and the courts), *intrabranch* (other executive branch agencies), or *intra-agency* (subdivisions of the surveillance executive

What Apple's Encryption Fight Has to Do with Religious Freedom, CHRISTIANITY TODAY (Mar. 29, 2016), https://perma.cc/RE2G-WX69 ("[B]y claiming [First Amendment] protections as a corporation, [Apple's] defense recalled another company in the headlines for resisting government orders: Hobby Lobby."). *See generally* Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751 (2014).

453. See *Citizens United*, 558 U.S. at 365. For the connection between *Citizens United* and *Lochner*, see Jedediah Purdy, *Neoliberal Constitutionalism:* Lochner*ism for a New Economy*, 77 LAW & CONTEMP. PROBS., no. 4, 2014, at 195, 198-203.

454. DAVID SINGH GREWAL, NETWORK POWER: THE SOCIAL DYNAMICS OF GLOBALIZATION 44 (2008).

itself). This descriptive account enriches our understanding of how one of the government's most important powers—the ability to surveil for law enforcement and foreign-intelligence purposes—is distributed, checked, and balanced in the public and private spheres.

To make judgments about these constraints, I also developed a two-part normative framework. The first part, the question of *frontier construction*, asked whether intermediaries help society identify and minimize tradeoffs between security and competing values like privacy and economic competitiveness. I argued that intermediaries contribute by adding more information about surveillance costs and by incentivizing the government to limit nonessential surveillance. But intermediary resistance brings unintended consequences that can distort surveillance decisionmaking—for example, by forcing the government to surveil more invasively or freeing intermediaries to collect more of their users' data.

The second part of the framework, the question of *frontier choice*, asked whether surveillance intermediaries facilitate or impede surveillance self-government. Proceduralism, litigiousness, and policy mobilization can all increase surveillance self-government by keeping the surveillance executive on the legal straight and narrow, as well as by empowering the public and potential sources of intragovernmental checks. But I cautioned that technological unilateralism threatens to undermine surveillance self-government when it obstructs otherwise lawful surveillance activity. In the short term, courts should be wary of arguments that the Constitution—especially the First Amendment—prevents the government from imposing obligations on surveillance intermediaries to facilitate lawful surveillance.

Although I focused on a discrete policy issue—resistance by large technology companies to government surveillance—the method I've advanced in this Article can be applied more broadly. In particular, it can help illuminate an emerging area of legal and policy challenges: the displacement of public by private power. In analyzing this dynamic, scholars so far have focused on government privatization,[455] private power in the political process post-*Citizens United*,[456] and the relationship between inequality and U.S. constitutionalism.[457] This Article is a case study of another, starker instance of

455. *See, e.g.*, Jody Freeman & Martha Minow, *Introduction: Reframing the Outsourcing Debates*, *in* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY 1, 20 (Jody Freeman & Martha Minow eds., 2009).

456. The literature is immense, overwhelmingly critical, and focused on limiting corporate influence on elections. *See, e.g.*, Molly J. Walker Wilson, *Too Much of a Good Thing: Campaign Speech After* Citizens United, 31 CARDOZO L. REV. 2365, 2368-69 (2010).

457. *See, e.g.*, K. Sabeel Rahman, *Domination, Democracy, and Constitutional Political Economy in the New Gilded Age: Towards a Fourth Wave of Legal Realism?*, 94 TEX. L. REV. 1329, 1330-31 (2016); Ganesh Sitaraman, Essay, *Economic Structure and Constitutional Structure: An Intellectual History*, 94 TEX. L. REV. 1301, 1302-03 (2016); Ganesh Sitaraman, *The Puzzling*

footnote continued on next page

private actors wielding public power: when, by virtue of their opposition to a core government activity, they challenge traditional conceptions of state sovereignty and thereby transform into "supercitizens."[458]

Nowhere have supercitizens risen higher and faster than in cyberspace. In this Article, I explained how internet companies challenge the state's monopoly over security, the very locus of traditional conceptions of sovereignty.[459] This explanation can help us better understand other areas where internet companies wield immense power, whether as creators and administrators of digital public squares[460] or as independent actors in cyberconflict.[461]

More generally, this account can illuminate broader issues of governance on the internet. For example, the first generation of cyberlaw scholarship was consumed by a debate between utopian visions of the internet as a separate, virtual world free of the control of traditional sovereigns[462] and realist

---

Absence of Economic Power in Constitutional Theory, 101 CORNELL L. REV. 1445, 1451-55 (2016). Constitutional historians are also looking anew through economic lenses. *See, e.g.*, MICHAEL J. KLARMAN, THE FRAMERS' COUP: THE MAKING OF THE UNITED STATES CONSTITUTION 5 (2016); Joseph Fishkin & William E. Forbath, *The Anti-oligarchy Constitution*, 94 B.U. L. REV. 669, 672-73 (2014).

458. DAVID ROTHKOPF, POWER, INC.: THE EPIC RIVALRY BETWEEN BIG BUSINESS AND GOVERNMENT—AND THE RECKONING THAT LIES AHEAD 309-10 (2012) (capitalization altered).

459. *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 475 n.23 (2017) (noting that Weber defined the state as "a human community that (successfully) claims the *monopoly of the legitimate use of physical force* within a given territory" (quoting MAX WEBER, POLITICS AS A VOCATION (1919), *in* FROM MAX WEBER: ESSAYS IN SOCIOLOGY 77, 78 (H.H. Gerth & C. Wright Mills eds. & trans., 1946))); *see also* WITTES & BLUM, *supra* note 213, at 81, 95-107.

460. *See, e.g.*, Jack M. Balkin, Lecture, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016); Benjamin F. Jackson, *Censorship and Freedom of Expression in the Age of Facebook*, 44 N.M. L. REV. 121, 121 (2014); Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1376 (2012).

461. For example, Google's Project Shield uses the company's infrastructure to defend news, human rights, and elections monitoring sites from what are known as distributed denial-of-service (DDoS) attacks, in which an adversary overwhelms a server by sending massive amounts of traffic to it from many different sources. *See* PROJECT SHIELD, https://perma.cc/NX59-7NKZ (archived Oct. 14, 2017). DDoS attacks are commonly used by repressive countries to attack news outlets, *see* Freedom House, Freedom on the Net 2017, at 3 (2017), https://perma.cc/8K7U-32NN; Project Shield thus puts Google, a private U.S. company, in direct conflict with repressive foreign governments.

462. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996); John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), https://perma.cc/AL3U-QUXS.

critiques that emphasized the continuing dominance of states.[463] It's increasingly apparent that this debate presented a false choice: Neither radically decentralized nor straightforwardly dominated by states, the internet is profoundly influenced by the small number of technology and communications companies that act as intermediaries for ordinary users. Beyond its technological and economic consequences, this insight has profound political and social implications. We live our lives in cyberspace—more precisely, in what Julie Cohen has called the "networked space" of physical reality overlaid with information and communications technologies.[464] We ought to know who besides the government might be sovereign in this realm.[465]

Surveillance intermediaries are not the United States's first corporate supercitizens and quasi-sovereigns. A century ago our society was one of railroads. The railroad companies not only shaped space but also created it, setting up societies and markets and spurring the development of the law.[466] Our technology giants are the railroad companies of the twenty-first century. They create and govern our networked space and thus control our lives to an extent unmatched by any other private entity.

The railroads ultimately lost their independence. Their overreaching was a major impetus for the decades-long process of statutory and constitutional transformation that culminated in the birth of the administrative state and the New Deal settlement; in the end, they were thoroughly regulated.[467] Whether technology companies will ultimately go the same way is an open question. But it will be a defining one for U.S. society, politics, and law in the first decades of the twenty-first century. Developing an understanding of how technology companies wield power, how their power both constrains and empowers government, and whether this power is legitimate and desirable will be one of

463. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD, at viii-ix (2006).

464. *See* COHEN, *supra* note 101, at 33; *see also* Julie E. Cohen, Essay, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 237-43 (2007).

465. *See, e.g.*, REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 154 (2012) ("These friendly and intelligent, young, blue jeans-wearing Californians[, Facebook's "hate and harassment" team,] play the roles of lawmakers, judge, jury, and police all at the same time. They operate a kind of private sovereignty in cyberspace."); Anupam Chander, *Facebookistan*, 90 N.C. L. REV. 1807, 1811 (2012) ("Facebook differs from the multinational corporations of the past in ways that raise the question of sovereignty more sharply."); Frank Pasquale, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, 17 THEORETICAL INQUIRIES L. 487, 512 (2016) ("It is almost as if the platforms see themselves as virtual worlds, whose users have essentially accepted (via terms of service) near-absolute sovereignty of corporate rulers.").

466. *See* JAMES W. ELY, JR., RAILROADS AND AMERICAN LAW, at vii-viii (2001).

467. *See, e.g.*, THOMAS K. MCCRAW, PROPHETS OF REGULATION: CHARLES FRANCIS ADAMS, LOUIS D. BRANDEIS, JAMES M. LANDIS, ALFRED E. KAHN 61-63 (1984).

the key projects for both law and legal scholarship as society pushes ever more completely into the digital age.