

The Argument Against Technology-Neutral Surveillance Laws

Paul Ohm*

Introduction

Should Congress write tech-specific or tech-neutral laws? Those who have considered this question have almost always chosen neutrality: laws should refer to the effects, functions, or general characteristics of technology, but never to a particular type or class of technology.¹ Those who espouse tech neutrality come from across the political and ideological spectrum and embrace tech neutrality dogmatically, often referring to it as a “principle,” one presumably violated only in exceptional circumstances for the most compelling reasons.²

But a close examination of the arguments supporting tech neutrality reveals many underappreciated flaws. At least three arguments support tech neutrality—consistency, the need to avoid underinclusiveness, and the recognition of institutional shortcomings—but each is contingent and rebuttable, and in many situations does not apply.

While other scholars have called Congress’s blind adherence to the principle of tech neutrality into question,³ none have explored the neutrality of laws regulating government search and surveillance. This rich, important context bears close scrutiny because the path of surveillance law so often follows the twists and turns of evolving technology.⁴ Moreover, since 9/11, Congress has more than once replaced tech-specific surveillance laws with tech-neutral ones: for example, with the USA PATRIOT Act⁵ Congress

* Associate Professor of Law, University of Colorado Law School. I thank Professor Bobby Chesney and the editors of the Texas Law Review for the invitation to participate. I also thank the participants at both the Symposium and the University of Colorado workshop series for their comments. In particular, I would like to thank William Boyd, Joe Feller, Susan Freiwald, Jennifer Granick, Lisa Graves, Marcia Hoffman, Clare Huntington, Orin Kerr, Derek Kiernan-Johnson, Sarah Krakoff, Michael Kwun, Jon Michaels, Scott Moss, Helen Norton, John Radsan, Carolyn Ramsey, Andrew Schwartz, Harry Surden, and Wendy Seltzer for their comments.

1. See, e.g., *infra* notes 29–30 and accompanying text.

2. See *infra* note 36 and accompanying text.

3. See Lyria Bennett Moses, *Recurring Dilemmas: The Law’s Race to Keep Up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL’Y 239, 239 (complaining that tech-neutral drafting may not be effective as technology changes); Chris Reed, *Taking Sides on Technology Neutrality*, 4 SCRIPT-ED 263, 282–84 (2007) (advocating a three-step process lawmakers should undergo when deciding between tech-neutral and tech-specific legislation).

4. See, e.g., John Schwartz, *Debate over Full-Body Scans vs. Invasion of Privacy Flares Anew After Incident*, N.Y. TIMES, Dec. 29, 2009, at A14 (discussing potential legislation to regulate the use of newly developed full-body scanners in airports).

5. Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered titles of U.S.C.).

brought neutrality to the Pen Register and Trap and Trace Devices Act⁶ (Pen Register Act), and through the Protect America Act⁷ (PAA) it did the same for the Foreign Intelligence Surveillance Act⁸ (FISA).

We should worry about this trend because the arguments in favor of tech neutrality are especially misguided in the surveillance context. When it comes to surveillance, every argument supporting tech neutrality can be met with a powerful counterargument: Tech-neutral laws often force consistency, even when inconsistency is preferable; they avoid underinclusiveness by permitting overinclusiveness; and they address Congress's supposed institutional shortcomings by cutting Legislative oversight over surveillance, even though history has taught us to beware the surveillance of an unchecked Executive. Given the deep flaws in the arguments for tech neutrality in the surveillance context, we should stop treating tech neutrality as a principle and instead treat it as a choice.

Finally, the blind adherence to the principle of tech neutrality pushes Congress away from the many benefits of tech specificity. Most importantly, a tech-specific surveillance law, even one imposing few constraints on the agencies conducting surveillance, forces the Executive Branch to consult with Congress whenever technology changes in significant ways, which might help offset the troubling culture of secrecy in national security policy by bringing broader, more participatory democratic oversight to the conduct of national surveillance. Also, because technology evolves so rapidly and constantly, tech-specific surveillance laws operate as a technology sunset, expiring not on some arbitrarily defined timetable, but whenever the circumstances demand. Both of these benefits increase the Legislature's role in national surveillance and national security debates and restore checks against the Executive's power in ways that might have helped avoid some of the surveillance abuses and excesses of the recent past.

This Article proceeds in three Parts, offering, in turn, the best arguments for tech neutrality (Part I), the underappreciated counterarguments to those arguments (Part II), and the case for tech specificity (Part III). Ultimately, this Article tries to counter the pervasively held attitude that tech-specific laws are indefensible mistakes to be avoided. Quite often, tech specificity is the wiser course—the best way to balance the government's need to provide security with the right to privacy.

6. 18 U.S.C. §§ 3121–3127 (2006).

7. Pub. L. No. 110-55, 121 Stat. 552 (2007) (to be codified at 50 U.S.C. §§ 1803, 1805a–1805c).

8. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered titles of U.S.C.).

I. Tech-Neutral Laws

A. *Defining Tech Neutrality*

Whenever Congress writes a law to address a problem caused by technology, it must decide whether to draft tech-neutral or tech-specific provisions. Tech-neutral provisions refer to technology in general, vague, open-textured terms that specify purposes, effects, functions, and other general characteristics. While Congress has used tech neutrality for surveillance law inconsistently, for decades it has embraced neutral drafting in other tech-heavy fields such as telecommunications⁹ and copyright. Under the Copyright Act, for example, copies are defined in part as “material objects . . . in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.”¹⁰

In contrast, tech-specific provisions refer to specific types or classes of technologies. For example, the Pen Register Act, a surveillance law, once applied only to “a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached.”¹¹ In the USA PATRIOT Act, Congress replaced this tech-specific definition with a tech-neutral one that broadly covers all “dialing, routing, addressing, or signaling information.”¹² We will revisit this example later in the Article.¹³

Most tech-centric laws lie along a spectrum from tech specificity to tech neutrality with few as close to either endpoint as the laws just cited. Sometimes it can be tricky to tell near which end of the spectrum a statute falls. A definition may seem tech specific on first blush because it lists specific types of technologies, but sometimes the point of such a list is to exhaust possibilities, covering the definitional waterfront, signaling that the list is meant to cover everything neutrally. For example, the Computer Fraud and Abuse Act—a Federal anti-computer-hacking law—defines a computer to mean “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”¹⁴ Despite providing a long list of specific types of technology, Congress intended this definition to

9. See Reed, *supra* note 3, at 264 (recognizing that “technology neutrality has continued to be a pervasive concept” in telecommunications policy).

10. 17 U.S.C. § 101 (2006).

11. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 301, § 3126(3), 100 Stat. 1848, 1871.

12. USA PATRIOT Act of 2001, Pub. L. No. 107-56, sec. 216, 115 Stat. 272, 290 (codified at 18 U.S.C. § 3127(3) (2006)).

13. See *infra* notes 147–52 and accompanying text.

14. 18 U.S.C. § 1030(e)(1) (2006).

have a broadly neutral meaning, and indeed the Seventh Circuit has interpreted it to cover not only laptop and desktop computers but “[e]very cell phone and cell tower[,] . . . every iPod, every wireless base station in the corner coffee shop, and many another gadget.”¹⁵

Congress must often choose between tech neutrality and specificity when it drafts surveillance laws because the great challenge of surveillance is keeping up with the latest advances in technology. Over the decades, it has written surveillance laws that fit at different points along the spectrum. Consider one law in particular, the Wiretap Act,¹⁶ and take a single, complex subsection of this Act, 18 U.S.C. § 2511(2)(g), which lists exceptions to the general prohibition on wiretapping, and this subsection provides a menagerie of examples from across the specificity spectrum. Under § 2511(2)(g), it is not an illegal wiretap to intercept electronic communications that are “readily accessible to the general public”¹⁷—a classically tech-neutral rule—radio communications “transmitted by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services”¹⁸—a mostly tech-specific rule—or communications, “the transmission of which [are] causing harmful interference” to another radio “to the extent necessary to identify the source of such interference”¹⁹—which seems to fall somewhere in between.

Through the first few technological epochs of electronic surveillance—from the earliest telephone wiretaps,²⁰ to the spike mikes²¹ and room bugs²² of the mid-twentieth century, up until the early days of computer-network surveillance—Congress wrote many tech-specific surveillance laws. My strong sense is that in the past decade or so, it has switched to writing only tech-neutral ones. As one example, the precursors to the tech-specific Wiretap Act provisions listed above were included in the original 1968

15. *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005).

16. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–23 (codified as amended at 18 U.S.C. §§ 2510–2520, 47 U.S.C. § 605 (2006)).

17. 18 U.S.C. § 2511(2)(g)(i) (2006).

18. *Id.* § 2511(2)(g)(ii)(III).

19. *Id.* § 2511(2)(g)(iv).

20. *See Olmstead v. United States*, 277 U.S. 438, 456–57 (1928) (describing the wiretap as small wires inserted into the telephone lines coming from the petitioners’ houses).

21. *See Silverman v. United States*, 365 U.S. 505, 506–07 (1961) (describing the instrument used as a microphone with a spike attached to it that was inserted into the house to become a “conductor of sound”); *Goldman v. United States*, 316 U.S. 129, 131 (1940) (“They had with them another device . . . having a receiver so delicate as, when placed against the partition wall, to pick up sound waves . . .”).

22. *See Katz v. United States*, 389 U.S. 347, 348 (1967) (describing the device used as capable of intercepting communications while being placed outside of a structure).

Wiretap Act,²³ while the tech-neutral “readily accessible” provision was added much more recently.²⁴

B. *Tech Neutrality in National Security Surveillance Law*

Those who urge Congress to expand surveillance authorities to protect national security often argue for tech-neutral surveillance laws. For example, John Yoo and Eric Posner applauded the USA PATRIOT Act’s amendments to FISA for embracing tech neutrality.²⁵ Thanks to the USA PATRIOT Act, “FISA warrants . . . are now technology-neutral . . . [and] allow continuing surveillance of a terrorist target even if he switches communication devices and methods.”²⁶

While Yoo and Posner lauded the shift to a tech-neutral FISA warrant standard, others remained dissatisfied about lingering tech specificity in the law, even after the USA PATRIOT Act. In particular, in the middle part of the first decade of the twenty-first century, Executive Branch officials pressed Congress to fix one form of lingering specificity in FISA—the way it treated communications bouncing through satellites differently than communications carried on fiber-optic cables.²⁷ Under the widely accepted interpretation of the statute’s definitions, if the NSA wanted to monitor the communications of a foreigner (or, to use the statute’s term, a non-“United States person”) located outside the United States, it faced significant procedural hurdles if the communications happened to travel over a fiber-optic cable and almost no hurdles if they traveled via satellite.²⁸

23. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, sec. 802, § 2511(2)(a)–(b), 82 Stat. 197, 214.

24. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 101(b)(4), 100 Stat. 1848, 1850.

25. See John Yoo & Eric Posner, *The Patriot Act Under Fire*, AEI: ON THE ISSUES, Dec. 1, 2003, <http://www.aei.org/issue/19661> (describing tech neutrality as a “common-sense adjustment[]” of necessity).

26. *Id.*

27. See, e.g., *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 27–28 (2007) [hereinafter *Modernization of FISA*] (statement of Kenneth L. Wainstein, Assistant Att’y Gen. of National Security, United States Department of Justice) (describing the distinction running throughout FISA between wire communications and radio communications).

28. To state the complicated argument concisely, under the definition of “electronic surveillance,” FISA treats surveillance of “wire communications” differently than it treats surveillance of “radio communications.” Compare 18 U.S.C. § 1801(f)(2) (2006) (defining “electronic surveillance” to include wire communications acquired without regard to intent or a reasonable expectation of privacy), with *id.* § 1801(f)(3) (requiring intentional acquisition of the transmission and a reasonable expectation of privacy for acquisitions of radio transmissions to constitute electronic surveillance). Surveillance of radio is not regulated by FISA unless, among other things, “both the sender and all intended recipients are located within the United States.” *Id.* § 1801(f)(3). Thus, for radio surveillance, when the NSA knows at least one party is outside the United States, FISA does not apply. In contrast, surveillance of wire communications falls within FISA if only one party is “in the United States” and if the surveillance itself “occurs within the United States.” *Id.* § 1801(f)(2). This summary omits a few details.

Executive Branch officials found this distinction untenable. Beginning at least in 2006, officials from the Intelligence Community and Justice Department pressed Congress repeatedly for a fix to FISA. Ken Wainstein, the Department of Justice's first Assistant Attorney General in charge of the National Security Division, suggested,

Rather than focusing, as FISA does today, on *how* a communication travels or *where* it is intercepted, we should define FISA's scope by reference to *who is the subject of the surveillance*. If the surveillance is directed at a person in the United States, FISA generally should apply; if the surveillance is directed at persons overseas, it shouldn't.²⁹

Former Director of National Intelligence, Admiral Michael McConnell, agreed, testifying that “[o]ur job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the Nation’s security to a snapshot of outdated technology.”³⁰

Congress eventually gave the Executive Branch what it wanted. First, in 2007, it enacted the PAA, which erased the wire and radio distinction for some cases, but out of concern for a rushed legislative process,³¹ it set a six-month sunset on the law.³² After the PAA expired, Congress enacted the FISA Amendments Act of 2008,³³ which took a different textual approach than the PAA, albeit to the same ends. As amended by the FISA Amendments Act, FISA no longer draws a distinction between communications carried by satellite and those carried by fiber-optic cables when non-U.S. persons are the target of the surveillance.³⁴ Now, intelligence analysts can listen to those communications no matter how they are carried—whether by copper wire, fiber-optic cable, microwave radio, satellite radio, or something else—under the same low standard. And because this part of FISA is now tech neutral, the same rules will apply to any communications technology developed in the future, regardless of how it operates, where it is deployed, or if it implicates privacy in new ways.

C. *The Arguments in Favor of Tech Neutrality*

This story of how and why Congress made FISA more neutral is typical. In many legislative debates over surveillance law, one side or another will

29. *Modernization of FISA*, *supra* note 27, at 30 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. of National Security, United States Department of Justice).

30. *Id.* at 19 (statement of J. Michael McConnell, Director of National Intelligence).

31. James Risen, *Bush Signs Law to Widen Reach for Wiretapping*, N.Y. TIMES, Aug. 6, 2007, at A1.

32. Protect America Act of 2007, Pub. L. No. 110-55, sec. 6(c), 121 Stat. 552, 557 (to be codified at 50 U.S.C. § 1803).

33. Pub. L. No. 110-261, 122 Stat. 2436 (to be codified in scattered sections of 50 U.S.C.).

34. *Id.* sec. 101, § 702. As amended, FISA now allows the Intelligence Community to monitor communications of non-U.S. persons not known to be in the United States, whether carried over wire or radio, without prior judicial approval, subject to some safeguards and checks, including mandatory notice to the FISA Court. *Id.*

urge Congress to reject tech specificity in favor of tech neutrality.³⁵ Those who argue for tech neutrality too rarely explain in detail the reasoning behind their arguments. Quite often, tech neutrality is a principle or rule, and it almost seems to go without saying.³⁶ Even when proponents of neutrality explain their reasoning, they often do so cursorily. As a result, we lack satisfying theoretical explanations for tech neutrality.³⁷ Before I offer counterarguments, I must first present the best arguments I can for tech neutrality in the surveillance context in order to try to avoid taking on straw men.

The arguments for neutrality are not inherently flawed, and sometimes tech neutrality may be a good idea. Still, these arguments are not unassailable, and they certainly do not support elevating the idea of tech neutrality to the level of a principle. Instead, they have gaps and logical flaws that suggest the shortcomings of the approach, which I will explore in Part II. These arguments number three.

1. Consistency.—The most often recited argument in favor of tech neutrality is the need for consistency—the need to avoid arbitrary distinctions between technologies that should be treated alike.³⁸ When Congress enacts a tech-specific rule, it regulates a specific technology while leaving unregulated similar technologies.³⁹ It makes no sense to treat these similar technologies differently because the policy rationale justifying the rule usually focuses on the effects of the technology, not on the function or features of the technology.⁴⁰

35. See *supra* notes 25–30 and accompanying text.

36. See, e.g., Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1127–28 (2009) (postulating that use limits are a better way to regulate border searches of laptops because special-collection limits would “violate the principle of technological neutrality”).

37. Some scholars have developed lists of explanations for tech neutrality. Chris Reed cites three aims: “futureproofing, online and offline equivalence, and encouraging the development and uptake of the regulated technology.” Reed, *supra* note 3, at 275. Similarly, Ilse van der Haar argues that tech neutrality leads to “non-discrimination, durability, efficiency, and certainty.” Corine Schouten, *EU Failed to Apply Technology Neutrality in Regulating Communication Services*, INNOVATIONS REP., Nov. 12, 2008, http://www.innovations-report.com/html/reports/communication_media/eu_failed_apply_technology_neutrality_regulating_124187.html. Almost all of these laudable qualities appear in the three arguments I present below.

38. See Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 299 (2009) (relating that the FISA Amendments Act “proceed[s] in a technology-neutral and less arbitrary fashion” than FISA).

39. See *Modernization of FISA*, *supra* note 27, at 10 (statement of J. Michael McConnell, Director of National Intelligence) (“FISA was written to distinguish between collection [of communications] on a wire and collection out of the air.”).

40. See *id.* at 28 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. of National Security, United States Department of Justice) (explaining that by embedding tech-specific language in FISA, Congress “use[d] the manner in which communications [were] transmitted as a proxy for the types of targets and communications that the statute intended to reach”); *id.* at 30 (arguing that instead of focusing upon “*how* a communication travels or *where* it is intercepted, [Congress] should define FISA’s scope by reference to *who is the subject of the surveillance*”).

Consistency sits at the heart of the Executive Branch arguments in favor of the PAA and FISA Amendments Act. Admiral McConnell, Assistant Attorney General Wainstein, and other Executive Branch officials repeatedly argued against treating satellite and fiber-optic communications differently.⁴¹ Consistency arguments often invoke happenstance and chance. Should the fact that a terrorist's communications happen to be carried over fiber-optic cable rather than via satellite have any bearing on whether the NSA can listen to them? Of course not, the tech-neutrality proponents argue.⁴²

2. *Keeping Up with Technological Change.*—Many argue that laws should be written neutrally because technology changes too quickly for the legislative process to keep up.⁴³ According to this argument, specificity leads inevitably and rapidly to anachronism because by the time a bill becomes a law, the technology will have evolved.⁴⁴ To support Admiral McConnell's call for tech neutrality in FISA, Andrew McCarthy of the *National Review* argued, "Any statute that focuses on technology will become obsolete (or worse, counterproductive) when technology changes"⁴⁵ Those making particularly strong forms of this argument seem to hold tech neutrality up as a form of enlightened modernity; a recognition by Congress that something in society—technology—moves too quickly for the legislative process.⁴⁶ Outside the surveillance context, the Seventh Circuit explained, "[L]egislators . . . know that complexity is endemic in the modern world and that each passing year sees new

41. See *id.* at 13 (statement of J. Michael McConnell, Director of National Intelligence) ("FISA's definitions of 'electronic surveillance' should be amended so that it no longer matters how collection occurs (whether off a wire or from the air.);"); *id.* at 34 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of National Security, United States Department of Justice) ("In keeping with the preference for technological neutrality, we would eliminate the distinction between 'wire' and 'radio' communications that appears throughout [FISA].").

42. See *id.* at 11 (statement of J. Michael McConnell, Director of National Intelligence) ("Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated technology.").

43. See *id.* at 15 (advocating amendments that would "make FISA technology-neutral, so that as communications technology develops—which it absolutely will—the language of the statute does not become obsolete").

44. See, e.g., *id.* at 33 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of National Security, United States Department of Justice) ("As a result of revolutions in communications technology since 1978, . . . the current definition of 'electronic surveillance' sweeps in surveillance activities that Congress actually intended to *exclude* from FISA's scope.").

45. Andrew C. McCarthy, *FISA Reform: The Bad Bill That Beats No Bill*, NAT'L REV. ONLINE, Feb. 14, 2008, <http://article.nationalreview.com/348094/fisa-reform-the-bad-bill-that-beats-no-bill/andrew-c-mccarthy?page=1>.

46. See *Modernization of FISA*, *supra* note 27, at 33 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of National Security, United States Department of Justice) ("Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. . . . We should not have to overhaul FISA each generation simply because technology has changed.").

developments. That's why they write general statutes rather than enacting a list of particular forbidden acts."⁴⁷

Furthermore, tech-specific laws do not simply become unacceptably anachronistic, but rather, they tend to become underinclusive with time. Once the specific type or class of technology targeted by a tech-specific law evolves into a new successor form, the law no longer applies. For those who support the policy underlying the law, this makes the law underinclusive, as they would prefer a law that expands to cover new versions of old technology.

Proponents of the PAA and FISA Amendments Act complained that the evolution of technology from satellite to fiber-optic cable communications had narrowed FISA.⁴⁸ According to their version of history, in 1978, when Congress enacted FISA, almost all transoceanic communications bounced through satellites using radio waves.⁴⁹

Times and technologies had changed. Thousands of miles of new fiber-optic cable had been laid since 1978, and the telecommunications industry had moved much of its operations from satellites to the new, cheaper, plentiful fiber-optic alternative.⁵⁰ By the time of the debates over the PAA, telephone companies were carrying most long-haul-phone calls over cables including, of course, the calls of terrorists and agents of foreign powers, creating an underinclusive, technological anachronism in the law.⁵¹ What Congress had chosen not to regulate in 1978, evolving technology had re-regulated.⁵²

The narrower FISA severely burdened the Intelligence Community. Admiral Michael McConnell argued, "Because technology has changed but the law has not, this statute—meant to protect against domestic abuses—instead protects potential foreign terrorists. We are significantly burdened in

47. *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005).

48. *See infra* note 51 and accompanying text.

49. *See Modernization of FISA, supra* note 27, at 10 (statement of J. Michael McConnell, Director of National Intelligence) ("When the law was passed in 1978, almost all local calls were on a wire and almost all long-haul communications were in the air . . .").

50. *See* Declan McCullagh & Anne Broache, *NSA Eavesdropping: How It Might Work*, CNET NEWS, Feb. 7, 2006, http://news.cnet.com/NSA-eavesdropping-How-it-might-work/2100-1028_3-6035910.html?tag=mncol (explaining that today "an undersea web of fiber-optic cables spans the globe—and those carry the vast majority of voice and data that leave the United States" so that "99 percent of the world's long-distance communications travel through fiber links [and t]he remaining 1 percent . . . are satellite-based").

51. *See Modernization of FISA, supra* note 27, at 10–11 (statement of J. Michael McConnell, Director of National Intelligence) (explaining that, in 1978, because most local calls were wire communications and most international calls were wireless communications, FISA's scope included wire communications; today, "the situation is completely reversed").

52. *See id.* at 19 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of National Security, United States Department of Justice) (explaining that technological "advances have largely upended FISA's intended carve-out of intelligence activities directed at persons overseas" so that "considerable resources of the Executive Branch and the FISA Court are now expended on obtaining court orders to monitor the communications of terrorist suspects overseas").

capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States.”⁵³ Similarly, Assistant Attorney General Wainstein testified that “sweeping changes since 1978—both in the nature of the threat that we face and in telecommunications technologies—have upset the delicate balance that Congress sought to achieve when it enacted FISA.”⁵⁴

3. *Institutional Competence.*—Finally, tech-neutral provisions respond to institutional concerns, helping Congress do what it does well and avoid doing what it does poorly. Those who argue against tech-specific statutes often intimate or assert that Congress is not equipped to understand complicated new technologies.⁵⁵ These arguments echo themes from each of the prior arguments—about consistency and the rate of technological change—tying them specifically to Congress’s perceived institutional shortcomings. As Bruce Berkowitz of the Hoover Institution puts it, “Intelligence officials know what they really require to do their mission, and legislators know how to write authorizing legislation.”⁵⁶ General Michael Hayden, then-Director of Central Intelligence, testifying about FISA, suggested that legislators were not equipped to keep up with changing technology: “Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should you. . . . [T]he statute we develop should be technology neutral.”⁵⁷

II. The Problems with Tech Neutrality

On the surface, these arguments have undeniable persuasive force, but they fare poorly under closer scrutiny. Every purported benefit of tech neutrality—consistency, avoidance of underinclusiveness, and institutional competence—can be recast as a shortcoming instead. These shortcomings are best illustrated through laws other than FISA, allowing us to draw lessons from older debates about the laws governing criminal surveillance. Consider the significant downsides of tech neutrality.

53. Mike McConnell, Letter to the Editor, *Protecting Americans and Their Rights*, N.Y. TIMES, May 5, 2007, at A12.

54. *Modernization of FISA*, *supra* note 27, at 24 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. of National Security, United States Department of Justice).

55. Often arguments like these carry a hint of superiority and maybe even a sense of ridicule. Perhaps other societal institutions can keep up with technology, but not Congress, which is stodgy and out of touch, full of elderly members who are the same. *See, e.g.*, Jim Puzzanghera, *Weighing High-Tech Bills in Analog: Political Issues Pile Up in the Fast-Evolving Sector, but Congress’ Expertise Isn’t Up To Date*, L.A. TIMES, Aug. 7, 2006, at C1 (cataloging the frustration of business leaders in educating Congress on technology and noting the substantial ridicule heaped on former Senator Ted Stevens for describing the Internet as “a series of tubes”).

56. Bruce Berkowitz, *The Wiretap Flap Continues*, WALL ST. J., Sept. 18, 2007, at A15.

57. *FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 8 (2006) (statement of Michael V. Hayden, Director, Central Intelligence Agency).

A. *Treating Differences Alike*

While the law should not treat different technologies differently when doing so would reward happenstance and chance, it is also true that some differences deserve to be treated differently. If instead Congress, trying not to violate the “principle” of tech neutrality, treats such differences alike, it will produce ineffective laws with unpredictable or pernicious effects.

As many have written, in our modern, information-driven world, technology acts like architecture, constraining and enabling certain human behavior.⁵⁸ But because different technologies constrain to different degrees and in different ways,⁵⁹ we should not regulate any specific technology until we take the time to study it to allow us to tailor our laws and regulations to the idiosyncrasies of the specific context. Policy makers fail to do this when they enact tech-neutral laws.

Many information-privacy scholars have recognized this point, arguing that policy makers should respond to the diversity of technology by tailoring and differentiating regulation to the specific context. Helen Nissenbaum has argued that expectations of privacy turn entirely on deeply contextualized differences between situations.⁶⁰ Dan Solove has written extensively about how changing technology brings new challenges to privacy.⁶¹ In part because of the diversity of privacy-impacting technologies, he concludes that privacy cannot be described monolithically but instead should be considered as a complex of different values that relate to one another only through Wittgensteinian “family resemblances.”⁶²

Scholars writing about national security and criminal law have drawn similar conclusions. Orin Kerr has written extensively about how specific new forms of technology enable both new forms of surveillance and new methods for committing crime.⁶³ He argues that these differences matter to criminal procedure and suggests rules that take these subtle differences into account.⁶⁴ Similarly, Jack Balkin and Sandy Levinson write persuasively about how “new technologies of surveillance, data storage, and computation”

58. *See, e.g.*, LAWRENCE LESSIG, *CODE: VERSION 2.0*, at 77–79 (2006) (arguing that the way in which any given technology is implemented—and selected from among the many potential architectures—is an exercise of power with political and social consequences).

59. *See id.* at 203–07 (cataloging the privacy consequences inherent in the specific architecture of several modern technologies).

60. HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 2–3* (2009).

61. *See, e.g.*, DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 9* (2004) (decrying the inadequacy of existing law protecting information privacy in response to the emergence of digital dossiers).

62. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1090–91 (2002).

63. *E.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 864–67 (2004) (charting Fourth Amendment treatment of various technological developments).

64. *See id.* at 868–75 (contrasting the institutional competence of the Legislature and Judiciary in addressing the implications of new technology on these areas of law).

have contributed to the rise of what they call the “National Surveillance State,” characterized by a significant increase in the amount of intelligence and surveillance the government conducts in the name of protecting national security.⁶⁵

The message from the overwhelming weight of legal scholarship about technology, privacy, and national security recommends subtlety and nuance, yet when Congress embraces uncritically the principle of tech neutrality, it abandons subtlety and nuance in the name of consistency.

Consider the ongoing Fourth Amendment debate over the search of laptops at international borders. The Supreme Court has held that government agents at international borders can conduct a wide range of suspicionless searches without violating the Fourth Amendment because of the need to protect American sovereignty and because people crossing borders should and usually do expect less privacy.⁶⁶ Scholars have debated whether this rule should extend to files stored on laptops being carried across the border.⁶⁷

Civil liberties groups argue that laptops are special technologies that merit special treatment under the Fourth Amendment at the border.⁶⁸ Because laptops store vast amounts of information and because the information can be of a highly personal nature, laptops become extensions of the self, more akin to a home than a pad of paper in a traveler’s backpack.⁶⁹

Former Bush Justice Department official, now law professor, Nathan Sales disagrees, arguing that the “principle of technological neutrality” demands a rule that treats pads of paper and laptops consistently.⁷⁰ But Professor Sales errs if he means to invoke a freestanding principle of neutrality, one that must be “violated” only with good justification. The only principle Congress should invoke is this one: Treat similar technologies alike and differing technologies differently. Arguing that a technology is not sufficiently different to outweigh a principle of neutrality is to double count.

To be fair, Professor Sales relies not only on the principle of neutrality; he also compares the privacy risks from searches of laptops to searches of

65. Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 *FORDHAM L. REV.* 489, 520–22 (2006).

66. See *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) (“Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant Automotive travelers may be stopped at fixed checkpoints near the border without individualized suspicion even if the stop is based largely on ethnicity” (citations omitted)).

67. E.g., Symposium, *The Fourth Amendment at the International Border*, 78 *MISS. L.J.* 241 (2008).

68. Brief for Amici Curiae Ass’n of Corporate Travel Executives & Electronic Frontier Foundation in Support of Defendant-Appellee at 4, *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008) (No. 06-50581).

69. *Id.* at 11–12.

70. Sales, *supra* note 36, at 1115.

“letters, address books, photo albums, and similar items.”⁷¹ The comparison, however, should be the entire analysis; the invocation of a principle should add nothing.

B. *Technological Change*

Tech-neutral laws too often avoid the problem of underinclusiveness by permitting overinclusiveness. They expand to cover new technologies and new circumstances. Consider the Communications Assistance for Law Enforcement Act⁷² (CALEA), a law that requires telecommunications providers to design their systems to be readily wiretappable to accommodate lawful government requests for access to customer communications.⁷³ CALEA is a tech-neutral law, one directed at “telecommunications carrier[s]” that governs what they must do with “equipment, facilities, or services” that can be used by a customer to “originate, terminate, or direct communications.”⁷⁴

When CALEA was enacted in 1994, both the Justice Department, which pressed for the law, and Congress focused mostly on problems associated with digital telephone networks.⁷⁵ Although the Internet was growing in importance at the time, almost all of the attention in hearings and committee reports centered on how digital telephone switches were foiling lawfully authorized wiretaps.⁷⁶ Motivated by such a tech-specific fear, Congress could have written a tech-specific law, one focused on digital telephony or perhaps even one that cited particular protocols or products by name. Instead, Congress wrote a tech-neutral law.

As we should have anticipated, tech-neutral CALEA has expanded over time. In 2005, the Federal Communications Commission (FCC), using power delegated to it in CALEA, granted the Justice Department’s petition to apply CALEA to providers of broadband-Internet and interconnected-Voice-over-IP (VoIP) services.⁷⁷ The FCC came to this conclusion over the objections of privacy groups and affected service providers, most vocally groups representing libraries and universities that worried they would be required to

71. *Id.*

72. 47 U.S.C. §§ 1001–1021 (2006).

73. *Id.* § 1002(a).

74. *Id.* Under the law’s definitions, a “telecommunications carrier” is “a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire,” *id.* § 1001(8)(A), but excludes “information services,” *id.* § 1001(8)(C), those that “offer[] . . . a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications,” *id.* § 1001(6)(A).

75. *See, e.g.*, H.R. REP. NO. 103-827, at 14 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3492 (calling on Congress to respond to the “‘digital telephony’ revolution”).

76. *See id.* at 10–16, *reprinted in* 1994 U.S.C.C.A.N. 3490–96 (summarizing the hearings on CALEA).

77. *In re Commc’ns Assistance for Law Enforcement Act and Broadband Access to Servs.*, 20 F.C.C.R. 14,989, 14,989 (2005).

include surveillance backdoors in their networks.⁷⁸ Ultimately, the D.C. Circuit rejected the challenges to the rulemaking.⁷⁹

Even one who agrees with this interpretation of the language of CALEA should concede that Congress did not say much about VoIP and broadband Internet when it considered whether to enact CALEA. When a tech-neutral law like CALEA expands over time, it loses its tether to the evidence Congress considered, the experts consulted in hearings, and the pages of research compiled into committee reports.

C. *Imprudent Delegation*

Of all of the arguments that support tech neutrality, the most important and the most flawed is the argument about institutional competence. Although Congress may sometimes have difficulty understanding the subtle nuances of technology or national security, a tech-neutral surveillance law rarely delegates Congressional power to an expert agency better equipped to understand such complexities. Instead, such a law almost always delegates power solely to the Executive Branch, which is often no better situated than Congress to understand such complexities.⁸⁰ When Congress switched from regulating “numbers dialed” to “dialing, routing, addressing, and signaling information,”⁸¹ it surrendered its role in future discussions about evolving technology because a tech-neutral law always expands with changing technology, placing the power entirely in the White House, NSA, and Justice Department.⁸²

D. *How to Decide Between Neutrality and Specificity*

Thus, every argument that supports the principle of tech neutrality can be met with a strong counterargument. We should never again treat legislative tech neutrality as a principle, default choice, or presumption; it is merely one of two paths we might take, and whether it is the right path depends on many circumstances. For example, to choose between tech neutrality and tech specificity, legislators need to understand how the technologies work, have been deployed, and have been used. Only by gathering accurate and

78. See, e.g., Final Brief for Petitioners at 43–44, *Am. Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006) (No. 05-1404) (arguing, with libraries and universities among the petitioners, that the FCC’s interpretation would force private broadband providers to comply with surveillance-capability requirements).

79. See *Am. Council on Educ.*, 451 F.3d at 232–36 (rejecting petitioners’ claims that Internet broadband and VoIP services classify as “information services” under CALEA).

80. See *infra* subpart III(A).

81. See *supra* notes 11–12 and accompanying text.

82. See Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 76, 89 (2008) (discussing privacy-impact-assessment requirements that apply to new technology and privacy risks and also highlighting increased involvement by the White House in administrative action).

complete information about these topics, can legislators decide, for example, whether to treat two technologies alike or differently.

Unfortunately, in the debates surrounding the PAA and FISA Amendments Act, Congress might not have had accurate information about these critical circumstances, because according to some nongovernmental observers, Executive Branch officials had painted a misleading picture about the critical factual claim that “almost all transoceanic communications were [satellite] radio communications.”⁸³ This factual statement supported every single Executive Branch argument for making FISA tech neutral, thus serving as the foundation for Congress’s decision to expand the surveillance power under FISA.

At the time the Executive Branch was making this factual claim, Kate Martin and Lisa Graves of the Center for National Security Studies were rebutting it in congressional testimony:

[E]ven a general examination of telecommunications history reveals that the scenario [administration officials] posit claiming that virtually all international calls of Americans were via satellite radio and therefore intended to be obtained by the government is not accurate. While satellites were increasingly used in the 1970s for television broadcasting and some telecommunications, American telephone companies were continuing to rely on trans-oceanic cables for international calls, with newer transatlantic cables sunk even the year after FISA passed⁸⁴

The pair concluded, “A more accurate statement than the administration’s description would be that for [the] past 29 years, US telecommunications has relied on both wire and radio technology for domestic and international calls.”⁸⁵

These conclusions were corroborated by David Kris, writing at the time as a private citizen but now the Assistant Attorney General (AAG) for National Security in the Obama Administration. Mr. Kris rebutted the Administration’s claims about the evolution from satellite to wireline communications, finding them “exaggerated,” because “in and around 1978, transoceanic communications were made in relatively large quantities by *both* satellites (radio) *and* coaxial cables (wire); both kinds of systems were expected to continue in service for many years; and the use of fiber optics was already anticipated for undersea cables.”⁸⁶

83. *Modernization of FISA*, *supra* note 27, at 29 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. of National Security, United States Department of Justice).

84. *Modernization of FISA*, *supra* note 27, at 195 (statement of Kate Martin, Director, and Lisa Graves, Deputy Director, Center for National Security Studies).

85. *Id.*

86. David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act 9* (Counterterrorism & Am. Statutory Law Series, Working Paper No. 1, 2007), *available at* http://www.brookings.edu/~media/Files/rc/papers/2007/1115_nationalsecurity_kris/1115_nationalsecurity_kris.pdf.

In other words, according to AAG Kris, the core factual premise underlying the Executive Branch's argument for tech neutrality might have been exaggerated. This might mean, as Ms. Martin and Ms. Graves argued and contrary to the Executive Branch's claims, that when Congress enacted FISA in 1978, it had good reason to treat radio and wireline communications differently.⁸⁷ Perhaps those reasons still merited inconsistent treatment in 2007 and 2008. My research has not yet confirmed which of the two versions of history should be believed. My point here is merely to suggest that one reason Congress might have failed to do a better job untangling these inconsistent histories is because it might have failed to see the importance of the inquiry, once it placed too much stock in the principle of tech neutrality.

III. The Argument for Tech-Specific Surveillance Laws

To this point, I have offered only arguments that challenge unchallenged claims for tech neutrality. There is no freestanding principle of tech neutrality, and arguments to shift from a specific to a neutral rule should be weighed on their own merits. But rejecting tech neutrality is not the same thing as defending tech specificity. Policy makers should take care not to make the same type of mistake in favor of tech specificity I have argued the proponents of tech neutrality have made; treating tech specificity as a freestanding principle is as bad as doing so with tech neutrality.

In this final Part, however, I will try to make that argument without making that mistake, giving reasons to often favor tech-specific laws over tech-neutral ones for surveillance. The most important reason was introduced in Part II: Tech-specific rules check the Executive Branch by authorizing narrow and circumscribed new forms of surveillance, permitting the Executive Branch the freedom to act with the Legislature's blessing, but only for a particular type of technology. We should prefer the active participation in surveillance decision making of two branches of government rather than one.

In order to embrace tech specificity, however, we need to deal with two practical difficulties, neither insurmountable. First, tech-specific laws expire as people switch from using the specified technology to using a replacement technology, leaving us adrift without legislative guidance. This would be unacceptable if it permitted either unchecked surveillance or untraceable crime or terrorism, but neither extreme is likely thanks to what I call the "background rules of surveillance."⁸⁸ Second, once law makers decide to create a tech-specific rule, they must decide how specific to make the rule, requiring a difficult textual balancing act.

87. See *Modernization of FISA*, *supra* note 27, at 195 (statement of Kate Martin, Director, and Lisa Graves, Deputy Director, Center for National Security Studies) ("[F]or [the] past 29 years, US telecommunications has relied on both wire and radio technology for domestic and international calls. From the beginning, FISA was written to accommodate that reality.").

88. See *infra* section III(B)(1).

Finally, tech-specific rules serve one unappreciated benefit: they sunset when new technologies are introduced. A law that governs only the use of a telephone, for example, will not govern the use of the Internet. Technology sunsets should be viewed as significant improvements over the traditional time-based sunsets that Congress seems to favor for surveillance laws lately. Technology sunsets enjoy many of the benefits and few of the downsides of their traditional counterparts. For all of these reasons, Congress should consider drafting tech-specific surveillance laws much more often than they have.

A. *Why We Should Prefer Specificity*

Sometimes Congress should delegate its authority to experts—to those with relative institutional advantages—but history has taught us to doubt that surveillance is a proper situation for delegation. The Executive Branch sees only one side to debates between security and privacy, and it tends to expand its authority and decrease oversight at every step. History has proven this repeatedly, from the well-documented wiretapping abuses at the FBI under J. Edgar Hoover,⁸⁹ to the intelligence abuses at the CIA that led to the Church Committee⁹⁰ and the enactment of FISA,⁹¹ to the NSA's Terrorist Surveillance Program,⁹² and to abuses of the national security letter process at the FBI.⁹³ The modern surveillance state needs information, and left without proper oversight, the analysts and agents in the field always seem to choose the path to more information and fewer administrative hurdles.⁹⁴ The Executive Branch, especially one bent on finding hidden terrorists, has shown that it cannot be trusted to act unchecked.⁹⁵

The Legislative Branch also brings another institutional advantage over the Executive Branch. The Executive Branch, especially the NSA, shrouds

89. See WHITFIELD DIFFIE & SUSAN LANDAU, *PRIVACY ON THE LINE* 163–64 (updated & expanded ed. 2007) (detailing the wiretapping of seventeen people for political purposes during the Nixon administration); Robert Bloom & William J. Dunn, *The Constitutional Infirmary of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147, 148–52 (2006) (comparing President Bush's warrantless wiretapping to Nixon's extensive wiretapping).

90. S. REP. NO. 94-755, at 24 (1976).

91. See S. REP. NO. 95-701, at 5 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3973–74 (providing a history of FISA and attempting to “make more explicit the statutory intent, to provide further safeguards for individuals subjected to electronic surveillance”).

92. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

93. See Dan Eggen, *FBI Found to Misuse Security Letters*, WASH. POST, Mar. 14, 2008, at A3 (describing the FBI's use of national security letters to obtain personal data from U.S. citizens rather than foreigners).

94. See Kevin Poulsen, *FBI Seeks Internet Telephony Surveillance*, SECURITY FOCUS, Mar. 27, 2003, <http://www.securityfocus.com/news/3466> (detailing a request by the FBI and the Justice Department to require companies to make technical changes making eavesdropping easier).

95. See, e.g., Risen & Lichtblau, *supra* note 92 (detailing how President Bush allowed the United States to monitor phone calls without court intervention).

its entire operations in secrecy.⁹⁶ Although the Legislative Branch deals with national security matters through classified hearings, select committees, and security clearances, its members are all quintessentially public figures who probably think more about the public's interest than a typical, nameless Executive Branch analyst.

Thus, the Legislative Branch should not delegate away its checking power. But that is precisely what it does when it writes a tech-neutral surveillance law.

B. Implementation

Before we can embrace tech specificity wholeheartedly though, we need to address two important implementation challenges. First, tech-neutral laws have one clear advantage over tech-specific laws—longevity. A tech-specific law applies only so long as people use the specific technology, and when people shift to using other, newer technology, we are left with uncertainty. The good news is that surveillance tends to be governed by good enough background rules. Second, legislators drafting a tech-specific law will struggle to set the proper level of specificity, and below I set out some rules of thumb.

1. Background Rules.—Tech-specific laws, by definition, do not expand or shift with every advance in technology; instead they expire as technology progresses, sometimes quickly and sometimes gradually. The expiry of an important surveillance law may seem like catastrophe, deregulating both surveillance and privacy protection, permitting either undetectable crime and terrorism, unchecked surveillance, or worse, both. These worst-case scenarios should not worry us, however, once we recognize that surveillance and privacy tend to be protected by important background rules that step in to fill the void when statutes do not.

At the outset, note a seeming irony: background rules tend to be tech-neutral rules.⁹⁷ Background rules apply when tech-specific rules expire precisely because they are not tied narrowly to a particular technology. Thus, although this Article argues against tech-neutral statutes, it cannot dismiss tech neutrality entirely. Without tech-neutral background rules, we would not be able to enact tech-specific laws.⁹⁸

The most important source for background surveillance rules is the Fourth Amendment to the U.S. Constitution.⁹⁹ The Fourth Amendment sits

96. See JAMES BAMFORD, *THE PUZZLE PALACE* 357 (1983) (describing NSA's informal nickname, "No Such Agency").

97. See *infra* note 103 and accompanying text.

98. I thank Joe Feller for suggesting this point.

99. The Fourth Amendment provides,

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall

in the background because the Supreme Court interprets it in a generally tech-neutral manner, but this has not always been the case. Before *Katz v. United States*,¹⁰⁰ the Supreme Court construed the Fourth Amendment with tech specificity, for example, distinguishing between “spike mike” recording devices that intruded physically into the offices of the people being monitored and those that did not.¹⁰¹ The seeming hyperspecificity of this rule prompted the D.C. Circuit to note that it was “unwilling to believe that the respective rights are to be measured in fractions of inches.”¹⁰² Beginning with *Katz*, however, the Court has construed the Amendment more neutrally, asking whether new forms of surveillance invade a person’s “reasonable expectation of privacy.”¹⁰³

A neutral Fourth Amendment is necessary but not sufficient to serve as an appropriate tech-neutral background for tech-specific surveillance statutes. The Fourth Amendment must also avoid extreme conclusions—absolute prohibitions or permissions for new surveillance techniques. If the Fourth Amendment’s default background rule for surveillance were an absolute prohibition on the use of new surveillance technologies, then the Intelligence Community would lose access to information, and in the worst case, it would lose track of those trying to harm us. On the other hand, if the Fourth Amendment’s rule were absolute permission, meaning any unregulated surveillance technology could be used to its fullest extent with no possibility of review, then we would end up with far too many invasions of privacy than we are willing to tolerate. Either result would be unacceptable.

The good news is that the Fourth Amendment’s background rules for surveillance almost never sit at either extreme. Instead, the Fourth Amendment tends to operate somewhere in the middle, thanks to a feature of its jurisprudence that is never celebrated by scholars—its lack of clarity.

To quote the first line of Anthony Amsterdam’s seminal article, “For clarity and consistency, the law of the fourth amendment is not the Supreme

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.

U.S. CONST. amend. IV.

100. 389 U.S. 347 (1967).

101. Compare *Goldman v. United States*, 316 U.S. 129, 133–34 (1942) (holding that the use of a spike mike that did not enter the apartment was not a search), with *Silverman v. United States*, 365 U.S. 505, 509 (1961) (holding that the use of a spike mike that made contact with an apartment baseboard was a search).

102. *Silverman v. United States*, 275 F.2d 173, 178 (D.C. Cir. 1960), *rev’d*, 365 U.S. 505 (1961).

103. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Despite the apparent neutrality of the reasonable-expectation-of-privacy test, the Court still seems to treat different technologies differently. See Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 307 (arguing that although *Katz* “was designed . . . to achieve some kind of technology neutrality within search and seizure law, . . . its impact on the law has been surprisingly narrow”).

Court's most successful product."¹⁰⁴ Other scholars have complained that "the Court has produced a series of inconsistent and bizarre results that it has left entirely undefended."¹⁰⁵ But for a background rule, inconsistency has a silver lining.

The muddiness of the Supreme Court's rule causes intelligence agents (and even more so their lawyers) to hesitate before charging ahead. As Carol Rose has said in praising muddy rules in property law, "When a court introduces ambiguity into the fixed rules that the parties initially adopted, it in effect reinstates the kind of weighing, balancing, and reconsidering that the parties might have undertaken if they had been in some longer term relationship with each other."¹⁰⁶ Because of the Fourth Amendment's muddiness, rarely should a government lawyer, pressed to analyze some new surveillance technology, tell an agent that he or she should proceed without worrying about the law.

Specifically, the Supreme Court and the federal courts of appeals have left unanswered two Fourth Amendment questions that arise in many contemporary surveillance situations: How does the Fourth Amendment apply to the Internet, and how does the Fourth Amendment apply to national security investigations involving foreign persons? We have only partial answers to these questions. *Smith v. Maryland*¹⁰⁷ stands for the proposition that government surveillance of some of the noncontent characteristics of electronic communication (specifically, the numbers dialed on a telephone) are not protected by the Fourth Amendment.¹⁰⁸ *United States v. District Court (Keith)*¹⁰⁹ stands for the proposition that the Fourth Amendment applies to national security investigations of domestic persons.¹¹⁰ These cases leave many important questions unanswered: Are the websites visited in a Web browser like the numbers dialed on a telephone and thus unprotected under *Smith*? Can *Keith* be extended to cover investigations of foreign persons? These are important questions that the Court should answer.

But recognize how the confusion over the Fourth Amendment plays a salutary role in the face of technological uncertainty. *Smith* provides a cautious green light to some aggressive new forms of surveillance, and *Keith* puts up at least a yellow light about national security investigations. The cases give government lawyers hope that they might be able to permit what their agents want to do without legislation, especially when the facts are important enough, but prevent them from charging forward without imposing

104. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 349 (1973).

105. Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 29 (1988).

106. Carol M. Rose, *Crystals and Mud in Property Law*, 40 STAN. L. REV. 577, 608-09 (1988).

107. 442 U.S. 735 (1979).

108. *Id.* at 742.

109. 407 U.S. 297 (1972).

110. *Id.* at 316-17.

some limits and controls on agents, as a hedge against future, adverse interpretations of the Fourth Amendment.

I have made two descriptive claims about the Fourth Amendment: After *Katz*, Fourth Amendment rules tend to be tech neutral, and the neutrality of these rules acts as a safety net, giving Congress the freedom to pass tech-specific statutes without worrying too much about what happens when the technology changes. But, turning to the normative, should the Fourth Amendment's rules be tech neutral, in light of the arguments against tech-neutral statutes in Part II? If so, then why might we value tech neutrality in our Constitution but reject it for statutes?

This normative question allows me to wade a bit into an illuminating debate that occurred between Professors Orin Kerr and Daniel Solove.¹¹¹ Although the pair disagreed about many things, they started from a point of fundamental agreement: both Congress and the courts play important roles in developing the rules of criminal procedure—Congress by passing the kind of surveillance statutes discussed throughout the instant Article, and the courts as interpreters of the Fourth Amendment.¹¹² Solove referred to this as a “dualist system of criminal procedure.”¹¹³

The pair disagreed, however, about which branch we should trust more to come up with good rules for criminal procedure, especially those designed to respond to new technology. Kerr argued that the Legislature has comparative institutional advantages over the courts for this task,¹¹⁴ while Solove wanted courts to play a more aggressive role than they had in the past.¹¹⁵ Rather than take a side in this debate, I argue that it is good to have *both* branches creating rules of criminal procedure. If nothing else, given institutional differences between the branches, they are likely to come to different conclusions about some surveillance practices, giving us more than one take on a subject, allowing us to use the different branches as laboratories to play out different ideas. Best of all, these approaches can support one another, each doing what the other does not. While the Constitution might serve as the wellspring of principle and baseline values, the statutes can fill in the details, policing the specifics of privacy and security. As Professor Kerr

111. The back-and-forth took place in three law review articles. Kerr, *supra* note 63; Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 *FORDHAM L. REV.* 747 (2005); Orin S. Kerr, *Congress, the Courts, and New Technologies: A Response to Professor Solove*, 74 *FORDHAM L. REV.* 779 (2005) [hereinafter *Kerr, Response*].

112. See Kerr, *supra* note 63, at 855 (“A broader look at the legal standards that govern criminal investigations involving new technologies suggests that Congress has often taken the lead, and . . . decisions interpreting the Fourth Amendment generally have played a secondary role. In some instances, congressional action has followed Supreme Court decisions interpreting the Fourth Amendment.”); Solove, *supra* note 111, at 753 (“The rules regulating government investigations have increasingly been those of federal statutes, not Fourth Amendment law.”).

113. Solove, *supra* note 111, at 747.

114. Kerr, *supra* note 63, at 858.

115. Solove, *supra* note 111, at 777.

noted, “[W]e should not expect the Fourth Amendment alone to provide adequate protections against invasions of privacy made possible by law enforcement use of new technologies. . . . Congress will likely remain the primary source of privacy protections in new technologies thanks to institutional advantages of legislatures.”¹¹⁶ At the same time, when tech-specific statutes, with their focus on detail and specifics, fail to apply because of changes in technology, the Constitution’s principles will provide the bulwark.

But even the advantages of interbranch diversity fail to explain fully why tech neutrality is so often a bad thing for Congress but not for the courts. This answer lies in one important institutional difference between the branches: courts adjudicate on a case-by-case basis, while legislatures design rules of general applicability.¹¹⁷ Given this difference, the amount of harm caused by a bad rule is much higher for legislative rules than judicial rules. When a legislature misreads the effect on privacy or security of a new technology or makes a bad prediction about the evolution of a future technology, the flawed general rule it creates as a result will apply broadly and will be hard to reverse. After enacting the rule, Congress will likely pay less attention to the question, making it hard for it to detect the effects of the bad rule. Further, in order to reverse the bad rule, Congress will need to muster the political will it needs to pass an amendment or repeal.

In contrast, when a judge crafts a rule based on a misreading of technology, it directly impacts only the parties in one case. In subsequent cases, judges applying the bad rule will have an opportunity to see how it applies to a new set of facts, which might expose the rule’s flaw. Law enforcement agencies or criminal defendants who disagree with the rule will have both the incentive and the opportunity in later cases to point out problems and to argue why the rule should be narrowed or reversed.

In addition to the Fourth Amendment, a second set of “rules” similarly sits somewhere between prohibition and permission, although it might seem odd to call these rules. They flow from the increasing intermediation of communications networks. In the early twentieth century, telephone and telegraph networks carried communications in the form of simple, easily captured analog signals, and surveillance targets tended to communicate from fixed locations like stationary landline telephones.¹¹⁸ On such simple analog networks, the government could conduct surveillance often without the help of an intermediary, for example attaching alligator clips to a wire

116. Kerr, *supra* note 63, at 838.

117. *Id.* at 884.

118. See K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, N.Y.U. REV. L. & SECURITY, 7 SUPP. BULL. ON L. & SECURITY, Spring 2006, at 3, available at <http://ssrn.com/abstract=889120> (“When FISA was being drafted it made sense to speak exclusively about the interception of a targeted communication—one in which there were usually two known ends and a dedicated (‘circuit-based’) communication that could be ‘tapped.’”).

atop a telephone pole or in an office building's basement.¹¹⁹ Things are much more complicated today. Digital packets have replaced analog signals, surveillance targets can access their e-mail accounts or use their cell phones from any place, and intermediaries can track communications that would have been untrackable before.¹²⁰

Now that the government needs help from private parties to conduct new forms of surveillance,¹²¹ a second background rule operates. Large corporate telecommunications providers worry about being sued by their customers for assisting the government. They worry especially about requests for novel forms of surveillance that may be inconsistent with specific congressional authority or at least unaccompanied by judicial order.¹²² Sometimes, providers overcome this reluctance, as when telephone and Internet providers complied with Bush Administration requests for assistance following 9/11.¹²³ Despite the pressure to cooperate with such requests, however, some providers have resisted government requests that they have felt might contradict the law.¹²⁴ Like the Fourth Amendment's muddy rules, intermediary risk aversion and exposure to liability leads to moderation. Nervous intermediaries will resist overly aggressive, broadly worded, or incompletely authorized new forms of surveillance, but they will also bend to the will of law enforcement and the Intelligence Community when a case seems important or urgent enough, as in the days following 9/11.

Both of these sets of background rules, Fourth Amendment rules and intermediary conservatism, help prevent the worst scenarios after a tech-

119. See *Olmstead v. United States*, 277 U.S. 438, 456–57 (1928) (describing the government's means of wiretapping as inserting small wires along ordinary telephone wires).

120. See Taipale, *supra* note 118, at 1 (describing FISA's inadequacy in addressing new technological developments).

121. Kenneth R. Logsdon, Note, *Who Knows You Are Reading This? United States' Domestic Electronic Surveillance in a Post-9/11 World*, 2008 U. ILL. J.L. TECH. & POL'Y 409, 419 (discussing the government's use of the private telecommunications industry in a new surveillance program).

122. See H.R. REP. NO. 99-690, at 15–16 (1986), *reprinted in* 1986 U.S.C.C.A.N. 5327, 5341–42 (noting that private parties are concerned with issues of liability when cooperating with FBI investigations); Albert Gidari, Jr., Keynote Address at the University of San Francisco Law Review Symposium: Companies Caught in the Middle (Oct. 28, 2006), *in* 41 U.S.F. L. REV. 535, 546–47 (2007) (describing cell-phone providers resisting requests for location-tracking information).

123. See Gidari, *supra* note 122, at 541 (“September 11 . . . changed a lot of things for service providers.”); Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (asserting that AT&T, Verizon, and Bellsouth all furnished the NSA with customer records after 9/11); Risen & Lichtblau, *supra* note 92 (describing a massive, warrantless monitoring effort made on thousands of international phone calls and e-mails from people inside the United States).

124. See Cauley, *supra* note 123 (“Among the big telecommunications companies, only Qwest has refused to help the NSA Qwest declined to participate because it was uneasy about the legal implications of handing over customer information to the government without warrants.”); Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 20, 2006, at A1 (describing Google's refusal to comply with a broad subpoena for copies of its search-query records); Declan McCullagh, *DOJ Abandons Warrantless Attempt to Read Yahoo E-mail*, CNET NEWS, Apr. 16, 2010, http://news.cnet.com/8301-13578_3-20002722-38.html (describing Yahoo's refusal to comply with a court order for evidence in a criminal investigation).

specific rule lapses—unchecked permission or absolute prohibition. The background rules, therefore, should give Congress the reassurances it needs to build narrowly crafted tech-specific rules without worrying about chaos after the new law expires. At the same time, because the Fourth Amendment and intermediary cautiousness lead inherently to doubt and conservatism, these rules must usually stay in the background only, and Congress should eventually regulate to replace laws that expire.

2. *How Specific?*—After identifying and weighing background rules, if Congress chooses to enact a tech-specific law, it next needs to describe the technology at the proper level of specificity. Congress should strive to write statutes that talk about technology specifically enough to allow for the benefits of tech specificity but generally enough to prevent the need to revisit the statute every six months.

Striking the balance between breadth and specificity can be difficult. To start, Congress should look at the specific technology or technologies that motivated it to act. Perhaps a news story or anecdote about a specific type of surveillance technology brought the issue to Congress's attention. For example, consider the barrage of media attention paid in late summer, 2000, to Carnivore.¹²⁵ Carnivore was the name given by the FBI to a packet-sniffing-and-filtering device that could be used to track Internet behavior.¹²⁶ Although the tool was originally vilified in the press and by privacy groups,¹²⁷ with the benefit of time, this criticism seems a bit mistargeted. According to several scholars, the tool was used only with a court order and only when an Internet Service Provider (ISP) lacked the expertise to conduct the ordered surveillance itself.¹²⁸

Nevertheless, in 2000, Congress expressed concern and outrage over Carnivore. Within weeks of the first news reports, Congress held hearings in which members criticized Justice Department and FBI officials for having

125. See, e.g., Neil King Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-mail Spark Concern*, WALL ST. J., July 11, 2000, at A3 (describing how Carnivore is “[e]ssentially a personal computer stuffed with specialized software [and] represents a new twist in the federal government’s fight to sustain its snooping powers in the Internet Age”).

126. See Trenton C. Haas, Note, *Carnivore and the Fourth Amendment*, 34 CONN. L. REV. 261, 271–73 (2001) (providing a detailed description of Carnivore).

127. See, e.g., Ted Bridis & Neil King Jr., *Carnivore E-mail Tool Won't Eat Up Privacy, Says FBI*, WALL ST. J., July 20, 2000, at A28 (discussing concerns about invading the privacy of Americans not under investigation for crimes).

128. See, e.g., Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1445 (2004) (describing Carnivore as a “tool the FBI developed to overcome difficulties service providers had in isolating and delivering the contents of electronic communications or addressing or routing information in response to court orders”); Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 653 (2003) (noting that, at times, “ISPs lack the expertise or the willingness to implement court orders on law enforcement’s behalf”).

developed the device.¹²⁹ Congress turned this criticism and concern into legislation, including in the USA PATRIOT Act a little-discussed provision specifically targeting Carnivore and similar tools. Section 216 of the Act obligates law enforcement to file a sealed report with a court when it uses tools like Carnivore.¹³⁰ Congress did not refer to Carnivore by name, choosing instead to refer to any “pen register or trap and trace device on a packet-switched data network.”¹³¹

This law seems appropriately tech specific, but consider other paths Congress might have taken. One year after the USA PATRIOT Act, with lingering fears about Carnivore on its mind, Congress passed another new reporting law, one which required much more detailed reporting while at the same time being much more narrowly defined.¹³² In this new law, Congress referred specifically to the name and model number given to Carnivore after the publicity fiasco, DCS-1000.¹³³ This law required the Attorney General to provide detailed reports about “the use of the DCS 1000 program (or any subsequent version of such program)” for two years.¹³⁴

Congress made a mistake drafting such a specific provision. Surveillance laws should not refer to specific tools by model and version number, even with the caveat applying the law to “any subsequent version.” While this type of hyperspecificity might make sense for the expert pronouncements of an administrative agency, Congress itself should rarely, if ever, refer to technology by a specific model number.

But this lesson in overspecificity provides a road map for finding the right level of generality. For any technology, one can recite a series of descriptions of increasing generality.¹³⁵ In the case of Carnivore, we progress from the most specific—DCS-1000—all the way to the most general—surveillance software or, even more generally, software.¹³⁶ Congress should avoid both extremes, the former being too specific, the latter too neutral by its generality. One possible target is to describe the technology at one or two steps above the most specific level. In this case, perhaps the ideal level of

129. See, e.g., *Fourth Amendment Issues Raised by the FBI's “Carnivore” Program: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. 107 (2000) (statement of Rep. Bob Barr, Member, H. Comm. on the Judiciary) (noting that the impact of Carnivore on the privacy rights of U.S. citizens is “immense”).

130. USA PATRIOT Act of 2001, Pub. L. No. 107-56, sec. 216, 115 Stat. 272, 289 (codified at 18 U.S.C. § 3123(a)(3)(A) (2006)).

131. *Id.*

132. 21st Century Department of Justice Appropriations Authorization Act, Pub. L. No. 107-273, 116 Stat. 1758 (2002) (to be codified in scattered titles of U.S.C.).

133. *Id.* sec. 305.

134. *Id.*

135. Copyright law embraces a similar “abstractions test,” first recited by Judge Learned Hand. *Nichols v. Universal Pictures Corp.*, 45 F.2d 119, 121 (2d Cir. 1930).

136. See Kerr, *supra* note 128, at 653–54 (discussing Carnivore and “its progeny” the “DCS-1000” in comparison to other software).

abstraction would be “packet-capture device” or maybe “filtered-packet-capture device.”

Although the standard outlined in this section is necessarily vague, it may prove easy to apply. Consider a few other surveillance technologies that in recent years have sparked the public’s imagination: In order to regulate these technologies, Congress should target “keystroke logging software” but never “Magic Lantern” (too specific) nor “spyware” (too general);¹³⁷ regulate “heat sensing cameras” rather than the “Agema Thermovision 210” or cameras;¹³⁸ and “whole-body scanners” instead of “L-3 Provision” or “radiation scanners.”¹³⁹

C. *Technological Sunsets*

Because tech-specific laws expire when technology changes, we can think of them as alternatives to traditional sunset provisions—legislative enactments that expire after a set period of time. In the surveillance context, Congress has enacted a number of sunset provisions in the past decade.¹⁴⁰ Tech-specific laws and laws with sunsets have much in common. Jacob Gersen, who has written frequently about sunset provisions,¹⁴¹ gives three reasons legislators enact sunset provisions: to offset information asymmetries, reduce error costs in the face of uncertainty, and correct limits of cognitive bias.¹⁴² Tech-specific provisions can also satisfy these three roles, by helping offset the doubt and uncertainty legislators have about the evolution of technology.

For example, imagine that a legislative proposal authorizing a new form of surveillance has a little less than a majority of Congress in support and a vocal contingent fiercely opposed. To help muster the few more votes they need, proponents of the bill might offer a traditional time-limited sunset provision, expiring say in four years. This serves two purposes: it helps

137. See Ted Bridis, *FBI Develops Eavesdropping Tools*, WASH. POST, Nov. 22, 2001, at A15 (describing the FBI’s “Magic Lantern” technology that “would allow investigators to secretly install over the Internet powerful eavesdropping software that records every keystroke on a person’s computer”).

138. See *Kyllo v. United States*, 533 U.S. 27, 29 (2001) (discussing whether the use of an “Agema Thermovision 210” thermal imager to detect infrared radiation emitting from Kyllo’s home constituted a Fourth Amendment search).

139. See Schwartz, *supra* note 4 (debating the use of screening technologies that can show the contours of the body and reveal foreign objects in reference to risks of privacy invasion).

140. See, e.g., Protect America Act of 2007, Pub. L. No. 110-55, sec. 6(c), 121 Stat. 552, 557 (to be codified at 50 U.S.C. § 1803) (setting a 180-day sunset on select provisions of the Act).

141. See, e.g., Jacob E. Gersen, *Temporary Legislation*, 74 U. CHI. L. REV. 247 (2007) (analyzing the “historical, legal, and political implications of temporary legislation”); Jacob E. Gersen & Anne Joseph O’Connell, *Deadlines in Administrative Law*, 156 U. PA. L. REV. 923 (2008) (discussing the use of deadlines to control the timing of administrative agency actions); Jacob E. Gersen & Eric A. Posner, *Timing Rules and Legal Institutions*, 121 HARV. L. REV. 543 (2007) (investigating constitutional, statutory, and internal congressional rules that affect the timing of legislative and executive actions).

142. Gersen, *supra* note 141, at 248.

convince undecided members to support the bill, by guaranteeing them a second vote in the near future, and it dampens the intensity of the opposition, who might fight less forcefully if they are guaranteed a future opportunity to kill the law. But the bill's proponents should recognize another way they might save the bill, by changing tech-neutral provisions into tech-specific provisions. If undecided and opposition law makers recognize that a tech-specific provision also expires at some point in the future, they may treat it the way they treat a traditional sunset.

More importantly, tech-specific laws overcome a significant limitation of ordinary sunsets. By "expiring" not according to an arbitrary timetable but instead precisely when changes in technology give reason to reopen policy debates, tech-specific laws offer the benefits of sunset without some of the downsides. To understand the relative advantages of technology sunsets, we need to understand some of the more technical details of Gersen's model as well as some of the model's shortcomings.

Gersen uses a transactions costs-public choice model to compare sunset legislation to permanent legislation.¹⁴³ Legislators must expend "enactment costs" when they enact or, in the case of a "sunsetting" law, reenact legislation, and they must expend "maintenance costs" at all other times.¹⁴⁴ For example, finding enough votes for passage is an enactment cost, while beating back an effort to repeal a law after it has been enacted is a maintenance cost.¹⁴⁵

As Gersen himself concedes, this model, although clarifying, proves difficult to apply because so much depends on unpredictable circumstances. How high are enactment costs versus maintenance costs? How much do legislators discount future enactment costs? Doubts about the answers to questions like these prevent Gersen from coming to many categorical conclusions about the differences between temporary and permanent legislation,¹⁴⁶ and they probably leave legislators making crude guesses about the effect of using a sunset or the amount of time to give to a sunset period.

Think of these difficulties as the products of a simple calibration problem. If a sunset period is set too far in the future, then the law may persist after the time when legislators would have otherwise wanted to revisit or even repeal the law. Even worse, if the sunset period is set to expire too soon, legislators will be forced to expend the costs of reenactment, even when there is no need for further review or debate. For any piece of

143. *Id.* at 261–66.

144. *Id.* at 263–65.

145. *Id.*

146. *See id.* at 266 ("While the analysis does not demonstrate that temporary legislation is clearly less costly than permanent legislation, it does show that temporary legislation is not clearly inferior—at least along the transaction-cost dimension."). Gersen comes to some tentative conclusions, for example arguing that "[i]t is almost certainly easier to block the repeal of legislation than to pass new legislation. As a result, continuing permanent legislation is less costly in the sunset year than reauthorizing temporary legislation." *Id.* at 264–65.

traditionally sunseting legislation, there is an ideal but unknowable term of expiration. The reason the ideal term cannot be known is because of the difficulty predicting the rate of change of important facts, particularly when those facts involve evolving technology.

Thinking of this as a calibration problem illuminates why tech-specific laws are better. A well-written tech-specific law is calibrated to expire precisely when the most important facts have changed enough to justify a reevaluation. As an example, consider how the technological shift from the telephone to the Internet expired an old version of the Pen Register Act at an optimal time.

The Pen Register Act regulates the government's ability to monitor the so-called envelope information associated with electronic communications.¹⁴⁷ For example, pen-register orders are needed to observe the numbers dialed by a telephone user.¹⁴⁸ Before the USA PATRIOT Act amended the Pen Register Act, it referred only to "numbers dialed,"¹⁴⁹ which meant it could expand without congressional reauthorization, but only to a point. As the telephony state of the art shifted from landline phones to cordless phones to mobile phones, the Pen Register Act expanded to cover each change, without wasteful congressional intervention.¹⁵⁰ This seems appropriate: although the surveillance of a mobile phone raises some issues not raised by the surveillance of a landline telephone, the two technologies seem similar enough to obviate the need for new congressional deliberation. The tech-specific law avoids the problem of laws tuned to expire too soon.

But then, people began to communicate over the Internet. Surely "numbers dialed" did not cover Internet-envelope surveillance, meaning Congress had to reconsider envelope surveillance as more people began to embrace this revolutionary new technology. The old technological sunset had expired. This seems well calibrated. Seen through both the privacy and law enforcement lenses, monitoring envelope information on the Internet seems a difference in kind not merely in degree from telephone surveillance. Precisely when the promise and peril of the Internet came into view, Congress was thrust back into the conversation. To be sure, great transaction costs were incurred—the first few times the Justice Department asked for changes to the Pen Register Act, Congress refused, partly because privacy advocates pushed back—but after it had time to deliberate fully, and once

147. 18 U.S.C. §§ 3121–3127 (2006).

148. *Id.* § 3121(a).

149. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 301, § 3126(3), 100 Stat. 1848, 1871.

150. *Cf. In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 749, 752–53 (S.D. Tex. 2005) (permitting the use of a pen register to obtain information from a mobile phone).

spurred by 9/11, Congress granted the new authority as part of the USA PATRIOT Act.¹⁵¹

Imagine how much less efficient it would have been for Congress to reevaluate the Pen Register Act on a fixed timetable, no matter what length of time it chose. If Congress had set the Pen Register Act to expire after four years, then at the end of the first term in 1990, there would have been very little to discuss. Communications did not change much in that time period. Congress would have been forced to expend resources to reenact the bill, perhaps placing it back under another four-year term, and it probably would have faced pressure after the first term to switch to a permanent term instead. The opposite problem might have occurred had the original sunset been set too far in the future, say ten years. In 1996, at the end of the first term, the Internet explosion would have been still in its infancy, and it might have been too soon to discuss an amendment. Then, if Congress had reenacted the Act with a second ten-year term, it is doubtful that it could have waited until the second date of expiry, in 2006, to finally get around to extending the Act to the Internet. Instead, the technological sunset forced a reevaluation at what seems to have been a near-optimal time: five years after Americans began to adopt the Internet in large numbers.¹⁵²

Conclusion

Conventional wisdom suggests that Congress should write tech-neutral surveillance laws most of the time. The conventional wisdom has it backwards. Congress should narrowly target surveillance laws at specific technologies most of the time. By doing so, it can assert its oversight role over the Executive Branch, which too often abuses its surveillance power when it acts unchecked, and shine a light on surveillance abuses.

151. See Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1194–95 (2004) (explaining how the amendments to the Pen Register Act mirrored those “the Justice Department had suggested for several years” before 9/11).

152. See U.S. CENSUS BUREAU, *COMPUTER AND INTERNET USE IN THE UNITED STATES: 2003* (2005), <http://www.census.gov/prod/2005pubs/p23-208.pdf> (reporting that between the years 1997 and 2000, the percentage of American households with Internet use at home rose from 18% to 41.5%).