ONLINE SURVEILLANCE: REMEMBERING THE LESSONS OF THE WIRETAP ACT

Susan Freiwald *

 Professor, University of San Francisco School of Law. My work on this Article has benefited immeasurably from the comments of the following people: Patricia Bellia, Jeffrey Brand, Julie Cohen, Joshua Davis, David Franklyn, Mark Lemley, Arti Rai, Joshua Rosenberg, Pamela Samuelson, and Lee Tien. Erin Dolly and Jennifer Lynch provided excellent research assistance, for which I am grateful.

I. INTRODUCTION

Modern readers of the classic study of electronic surveillance, suggestively titled *The Eavesdroppers,* likely experience a strong sense of déjà vu.[1] The book's introduction describes Americans in the early 1950s as having two contradictory views about electronic surveillance.[2] On the one hand, they feared that eavesdroppers were using increasingly sophisticated electronic tools to violate their privacy and record their every move and conversation. On the other hand, they considered tales of such surveillance to be the overblown product of paranoia.[3] The public did not know whether to

1. SAMUEL DASH, RICHARD F. SCHWARTZ & ROBERT E. KNOWLTON, THE EAVESDROPPERS (photo. reprint 1979) (1959) [hereinafter DASH]. Dash was the director of the study, and the author of the first and largest section of the book that reports on the study's findings.

2. DASH, *supra* note 1, at 1-20.

3. DASH, *supra* note 1, at 3-4 (describing conflicting reports as generating much confusion); *see also* EDITH J. LAPIDUS, EAVESDROPPING ON TRIAL 2 (1974) ("The average individual jokes about wiretapping when he hears a click on his telephone, but his laugh is getting nervous.").

believe law enforcement's claim that, if it was using electronic surveillance at all, it was for a good cause and strictly limited.[4]

Today, we remain of two conflicting minds about the practice of electronic surveillance, particularly when it comes to government monitoring of the Internet. Popular accounts warn of the government's extensive power to track our online lives in almost infinite detail and to record such information in searchable electronic databases.[5] Yet few of us take steps to protect our privacy online, even as we engage in activities that we consider private. In recent years, Americans have pursued their hobbies, travel planning, shopping, political organizing, and even dating online, seemingly uninhibited by fears of government surveillance. Often, we reveal personal information in electronic mail we send to our friends and family—information we would never consider widely disseminating.[6] Though techniques are available to hide our online movements and to encrypt our communications, few of us use them.[7]

One can speculate as to why we fear extensive surveillance but do little to stop it. For one thing, most of us do not think much about electronic surveillance unless asked to do so. Perhaps we believe that the less we know about electronic surveillance, the less it hurts us.[8] When we do think about it, perhaps we believe, largely incorrectly, that our service providers protect our privacy for us. We may consider ourselves too unimportant to be monitored, or feel confident that we have nothing to hide. Or, just as some of our predecessors did in the 1950s, perhaps we believe our government's claim that its agents follow strict controls whenever they obtain information about our online activities and that they rarely, if ever, monitor us.

In researching *The Eavesdroppers*, Samuel Dash conducted a penetrating empirical study of electronic eavesdropping in the early 1950s.[9] Dash's study is widely cited in cases and commentary.[10] According to Dash, the

---

4. DASH, *supra* note 1, at 3.

5. *See, e.g.*, CHRISTIAN PARENTI, THE SOFT CAGE: SURVEILLANCE IN AMERICA (2003); JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004).

6. *See Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce*, 107th Cong. 5-11 (2001) [hereinafter *Information Privacy Hearings*] (testimony of Lee Rainie, Director, Pew Internet and American Life Project) ("At the same time they overwhelmingly express concern about their online privacy, American Internet users do a striking number of intimate and trusting things online."); *see also* Pew Internet and Am. Life Project, *Daily Internet Activities* (finding that 69 million Americans go online each day and engage in various activities), *available at* http://www.pewinternet.org/reports/asp.

7. *See Information Privacy Hearings*, *supra* note 6, at 4 (testimony of Lee Rainie) (reporting that just 9% of American Internet users have used encryption to scramble their e-mail and only 5% have used software to hide their identities from web sites); *see also* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 46-48 (1999) (explaining cryptography's "slow start").

8. *See infra* notes 113-15 and accompanying text.

9. *See* DASH, *supra* note 1, at 5-20 (describing his research methodology).

10. *See, e.g.*, Berger v. New York, 388 U.S. 41, 60 (1967) (citing Dash's study to support allegations that wiretapping has been used during organized crime investigations); Lopez v. United States, 373 U.S. 427, 467-70 (1963) (Brennan, J., dissenting) (crediting Dash with revealing the "true dimensions" of electronic surveillance). The Minnesota Law Review devoted a symposium to the book. *The Wiretap-*

seemingly paranoid view of electronic surveillance was quite sane.[11] Though the vast majority of citizens had no idea that it was going on, government agents at all levels commonly engaged in electronic eavesdropping, violating both state and federal laws.[12] Illegal surveillance was often conducted with the cooperation of local phone companies, who conspired with agents to keep surveillance secret in order to maintain public confidence in the telephone networks.[13] Many of Dash's interview subjects, usually local police officials, protested repeatedly that they never used electronic surveillance, until further probing forced them to concede the truth.[14] Subsequent studies confirmed Dash's findings of rampant illegal government surveillance during the first half of the twentieth century.[15]

Since then, numerous examples of illegal government surveillance have come to light. Among the more notable include the unlawful surveillance conducted by J. Edgar Hoover during his forty-eight years as the director of the FBI.[16] Reports of illegal wiretapping by the Nixon administration surfaced during the Watergate investigations. These high-profile cases represent examples of practices that have persisted throughout the history of the telephone and electronics. Governmental actors have consistently misused surveillance powers to further personal goals, support corruption, and harass opponents.[17]

---

ping-Eavesdropping Problem, Reflections on THE EAVESDROPPERS, A Symposium, 44 MINN. L. REV. 811 (1960). The contributors praised Dash's study. *See, e.g.*, Harold K. Lipset, *The Wiretapping-Eavesdropping Problem: A Private Investigator's View*, 44 MINN. L. REV. 873, 873 (1960) (calling the study "careful and objective"). A district attorney from New York City called the book "an innuendo-splattered 'thriller,'" but did not seriously undermine its findings. *See* Edward S. Silver, *The Wiretapping-Eavesdropping Problem: A Prosecutor's View*, 44 MINN. L. REV. 835, 835 (1960).

11. *See* DASH, *supra* note 1, at 3-20 (explaining the history and state of electronic surveillance as it relates to his study).

12. *See* DASH, *supra* note 1, at 34-35, 43-57, 79-95, 170, 173, 217, 247; *see also* JURIS CEDERBAUMS, WIRETAPPING AND ELECTRONIC EAVESDROPPING: THE LAW AND ITS IMPLICATIONS, A COMPARATIVE STUDY 15, 16, 19, 23 (1969) (describing law enforcement violation of wiretapping laws); *infra* note 15.

13. *See* DASH, *supra* note 1, at 26, 66, 93, 122-23; *see also infra* note 44 (discussing telephone company aid to wiretappers).

14. *See* S. REP. NO. 90-1097, at 134 (1968), *reprinted in* 1968 U.S.C.C.A.N 2112, 2223 (individual views of Sen. Long and Sen. Hart) (complaining that law enforcement officials "dishonestly denied" use of wiretapping or bugging in "instance after instance"); DASH, *supra* note 1, at 9, 121-22, 129, 144-51, 162, 167, 216, 218-19. Prior to his study, Dash had been a prosecutor who favored law enforcement wiretapping. *Id.* at 5.

15. *See, e.g.*, LAPIDUS, *supra* note 3, at 3, 12-13 (providing history based on myriad official sources, extensive interviews, and questionnaires); ALAN F. WESTIN, PRIVACY AND FREEDOM 103, 119-32 (1967) (finding pervasive illegal government surveillance on the basis of "[a] thorough search of legislative and administrative hearings, court records, police journals, technical magazines," thousands of newspaper clippings, and seventy-five personal interviews); Thomas C. Hennings, Jr., *The Wiretapping-Eavesdropping Problem: A Legislator's View*, 44 MINN. L. REV. 813, 814 (1960) (describing the corroborating findings of a Senate Subcommittee on Constitutional Rights).

16. *See, e.g.*, ALEXANDER CHARNS, CLOAK AND GAVEL: FBI WIRETAPS, BUGS, INFORMERS, AND THE SUPREME COURT (1992); ANTHONY SUMMERS, OFFICIAL AND CONFIDENTIAL: THE SECRET LIFE OF J. EDGAR HOOVER (1993).

17. See *infra* notes 168-69 and accompanying text for a full discussion of illegal surveillance in the 1950s and 1960s. For an up-to-date overview of the history of abuses, see JAMES X. DEMPSEY & DAVID COLE, TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY (2d ed. 2002). *See also* DIFFIE & LANDAU, *supra* note 7, at 137-65, 173-79 (reviewing the

The misuse of surveillance powers comes at a significant cost to society. A common misperception is that overzealous surveillance will hurt only the wrongdoers. In reality, few of us conform all aspects of our behavior to the extant laws. The power to use surveillance to uncover private acts is, then, the power to pressure and even prosecute those with unpopular views, such as those critical of the government.[18] Moreover, privacy rights shield not just illegal activities, but also those things we would prefer to keep to ourselves or among our trusted associates. If we reach a point where we can keep nothing from the government's prying eyes, then we will have lost not only our privacy, but the full exercise of our rights of speech, association, and dissent. In important ways we will have lost our democracy.[19]

This Article does not uncover current abuses of electronic surveillance law, as Dash did in his time, though certainly an updated empirical study would be useful.[20] Instead, Part II considers what historically has made electronic surveillance meaningfully different from other police investigative techniques. It begins by exploring how surveillance has been particularly appealing to law enforcement while posing a grave threat to privacy. Commentators consistently recognize the need to reconcile the competing interests of police prerogatives and communications privacy, but generally neglect the other unusual challenges that electronic surveillance poses for regulators. In particular, lawmakers must devise a comprehensible law for a remarkably complex practice. They must rein in law enforcement officers without crippling them. Finally, they must distinguish between prohibited and permissive conduct, while likely experiencing deep ambivalence about the practices themselves.[21]

In light of these challenges, the Wiretap Act of 1968 represents a considerable achievement.[22] In the wake of decades of hearings, numerous rejected bills, and intense public debate, the Wiretap Act achieved a workable compromise that has largely stood the test of time. All branches of government and countless experts had input into the design of the Wiretap Act.[23] It provides a comprehensive scheme that strictly limits law enforcement's use of electronic surveillance and provides several mechanisms to ensure that

---

history of government abuses of electronic surveillance); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004).

18. *See* ROSEN, *supra* note 5, at 22-25, 130-31.

19. *See* WESTIN, *supra* note 15; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1647-59 (1999) (arguing that information privacy on the Internet is critical to the citizens' ability to define themselves and engage in democratic deliberation).

20. The American Civil Liberties Union ("ACLU") has published anecdotal reports of recent abuses. *See, e.g.*, ACLU, FREEDOM UNDER FIRE: DISSENT IN POST-9/11 AMERICA (2003); ANNE BEESON & JAMEEL JAFFER, ACLU, UNPATRIOTIC ACTS: THE FBI'S POWER TO RIFLE THROUGH YOUR RECORDS AND PERSONAL BELONGINGS WITHOUT TELLING YOU (2003). The author serves on the Board of Directors of the ACLU of Northern California.

21. *See infra* Part II.D.

22. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522 (2002)). Commentators use either "Title III" or the more intuitive "Wiretap Act" to refer to the law.

23. For further discussion of the legislative process that led to the Wiretap Act, see *infra* Part IV.A.

surveillance stays within legal bounds. The Act relies on two Supreme Court cases decided the year before its passage to demarcate legal from illegal conduct.[24]

With that background in mind, Part III considers electronic surveillance of the Internet, or online surveillance. It argues that online surveillance is even more susceptible to law enforcement abuse and even more threatening to privacy. Therefore, one might expect regulation of online surveillance to be more privacy-protective than traditional wiretapping law. That could not be further from the truth. The law provides dramatically less privacy protection for online activities than for traditional telephone calls and videotapings. Additionally, what makes the Wiretap Act complex makes online surveillance law chaotic. Almost all of the techniques designed to rein in law enforcement have been abandoned in the online context. And, while Congress resolved much of its ambivalence towards wiretapping in 1968, current law suggests the outright hostility of all branches of government to online privacy.[25] Further, several important questions remain unanswered about the parameters of online surveillance law, even after amendments to that law in the USA PATRIOT Act.[26]

Part IV argues that we should remember the lessons of the Wiretap Act. It starts by comparing the process that yielded the Wiretap Act to that which created the modern framework, and argues that the former was much more informed and deliberate. It then explores whether something about the Internet, or about the modern era, counsels against drawing upon the lessons of the Wiretap Act. It finds no justification for either depriving the Internet of privacy protection or abandoning privacy in light of concerns about terrorism. In the absence of such justification, reform of online surveillance law is imperative.

Part V suggests that online surveillance law should draw upon both the Wiretap Act and the approach courts have taken to the regulation of video surveillance. In the mid-1980s, government video monitoring represented the emerging threat that online surveillance represents today, but the Wiretap Act said nothing about it. Nonetheless, seven Courts of Appeal extended the core protections of the Wiretap Act to government monitoring by video.[27] Revising the law to reflect the similarities among wiretapping, video surveillance, and online surveillance would go a long way towards improving online privacy.

---

24. *See infra* Part II.D.4.

25. *See infra* Part III.

26. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Supp. 2001).

27. *See infra* Parts III.E.2, V.

II. TRADITIONAL ELECTRONIC SURVEILLANCE: BEHIND THE WIRETAP ACT

A. Background

1. Definitions of Terms

The term "electronic surveillance" refers to law enforcement's use of electronic or mechanical devices to gather information about people's private activities. In limiting my focus to government surveillance, I do not mean to minimize the threat to privacy that surveillance by private entities poses.[28] In fact, the distinction between private and government surveillance may well be overdrawn. Nonetheless, the law has consistently distinguished between private and government surveillance as a matter of both constitutional law and policy.[29] In the interest of covering a complex topic in a manageable space, this Article addresses only government surveillance.

A few other aspects of the definition require discussion. It may seem oxymoronic to describe surveillance as disclosing "private activities." Activities that are successfully surveilled are no longer private in the usual sense. Privacy incorporates the notion of controlling the dissemination of information about oneself, which the target of non-consensual surveillance clearly does not do.[30] I use "private activities" to mean those that would be private but for the surveillance. To elaborate, people engage in private activities when they do things that they either assume are not watched or that should not be watched in a free and democratic society. That definition should suffice for now, though the difficulty of dividing private from non-private activities has seriously challenged lawmakers.[31]

Electronic surveillance, as I have defined it, covers a wide range of techniques, many of which this Article does not discuss. For example, bugging, or the planting of listening devices that do not intercept phone calls, is covered only as it relates to wiretapping or the interception of telephonic information.[32] I do not discuss the use of parabolic microphones, laser

---

28. *See generally* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Philip E. Agre & Marc Rotenberg eds., 1997) (collecting essays about personal privacy in digital information); Clifford S. Fishman, *Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media*, 72 GEO. WASH. L. REV. 1503 (2004); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1195-202 (1998) (discussing private surveillance of online activities); Paul M. Schwartz, *supra* note 19.

29. The Fourth Amendment, for example, protects against state action only and does not apply to surveillance by private entities.

30. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting) ("As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.").

31. *See infra* Part II.D.4.

32. In keeping with modern practice, I use the term "electronic surveillance" as the overarching term, and I generally use "eavesdropping" as a synonym for "bugging." Historically, those terms were reversed, with eavesdropping being the overarching term, and electronic surveillance being limited to bugging. *See, e.g.*, LAPIDUS, *supra* note 3, at 3.

beams, radio interceptions, and cable-tapping, except to the extent that those technologies are used to intercept telephonic information or internet data.[33]

Where one sits largely determines one's position on the propriety of electronic surveillance.[34] Traditionally, law enforcement personnel have viewed electronic surveillance as a highly desirable investigatory technique. In contrast, privacy proponents, including sociologists, historians, civil libertarians, and members of all branches of government, have viewed electronic surveillance with considerable skepticism. This dichotomy is simplified by separating the two groups into distinct camps. In fact, law enforcement agents oppose surveillance that violates the law that they swear to uphold.[35] Similarly, privacy proponents recognize the need for law enforcement to uphold the laws and protect public safety.[36] Thus, both groups have, to some extent, recognized the need for regulation to balance the interests of law enforcement and privacy.[37]

Before considering how Congress achieved this balance in the Wiretap Act, I first elaborate on what makes electronic surveillance particularly appealing to law enforcement and threatening to privacy. To provide background for the 1968 regulation, I consider the practice within that historical context.

2. *Electronic Surveillance: Its Appeal to Law Enforcement*

To law enforcement, electronic surveillance has meant a safer, cheaper, more powerful, and more effective way to investigate. Not surprisingly, law enforcement representatives have portrayed electronic surveillance as an invaluable weapon in their fight to combat crime and maintain order. With few exceptions, they have vigorously opposed efforts to constrain government use of electronic surveillance.[38] They have claimed it to be of particu-

---

33. *See, e.g.*, CEDERBAUMS, *supra* note 12, at 9-10 ("The variety of devices seems to be limited only by the unlimited imagination of science and technology."). I also do not consider the heat-sensing thermal-imaging device that was the subject of a recent Supreme Court decision. *See* Kyllo v. United States, 533 U.S. 27 (2001).

34. The symposium devoted to *The Eavesdroppers* provides a good illustration. *See supra* note 10. It consisted of articles from "five men, with diverse points of view"—a prosecutor, a legislator, a professor, a private investigator, and a defense attorney. *See, e.g.*, Yale Kamisar, *The Wiretapping-Eavesdropping Problem: A Professor's View*, 44 MINN. L. REV. 891 (1960); Edward Bennett Williams, *The Wiretapping-Eavesdropping Problem: A Defense Counsel's View*, 44 MINN. L. REV. 855 (1960).

35. Law enforcement agents prosecute individuals for violating electronic surveillance laws. *See, e.g.*, United States v. Councilman, 245 F. Supp. 2d 319 (D. Mass. 2003) (distinguishing "intercepting" and taking wire communications out of "storage"), *aff'd*, 373 F.3d 197 (1st Cir. 2004), *reh'g en banc granted, opinion withdrawn by*, 385 F.3d 793 (1st Cir. 2004); *infra* note 313 (discussing the case). Of course, agents' responsibilities do not conflict when the pertinent privacy protections are weak, as they are for online surveillance. *See infra* Part III.

36. *See, e.g.*, Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting).

37. One cannot read about electronic surveillance law without confronting this balance. *See, e.g.*, Nardone v. United States, 308 U.S. 338, 340 (1939) (discussing the need to "harmonize two opposing concerns," "the stern enforcement of the criminal law," and "the protection of that realm of privacy left free by Constitution and laws but capable of infringement either through zeal or design"); *infra* notes 55-60 and accompanying text for further discussion of this balance.

38. *See, e.g.*, DASH, *supra* note 1, at 99-100, 221-22; Hennings, *supra* note 15, at 815, 818.

lar value in investigations of organized crime.[39] Also, since criminals have used electronic surveillance, proponents have claimed that fundamental fairness dictates providing the government with the same tools.[40]

The hidden nature of electronic surveillance makes it significantly safer to use than the alternatives. Live officers, whether in uniform or undercover, run the risk of serious injury when they infiltrate criminal activities. If targets ever discover electronic surveillance, the devices themselves run a greater chance of being harmed than the agents. Historically, the risk of discovery has been fairly low. Miniaturization made it increasingly difficult to discover electronic bugs. Wiretappers, for their part, soon developed the technical sophistication to avoid the suspicion of users of monitored phone lines.[41] Telephone networks offer several possible locations for taps, many at some distance from the target.[42] Samuel Dash studied some jurisdictions in which phone companies provided access to an entire jurisdiction's phone calls from a spot within police headquarters.[43] With widespread telephone company cooperation, agents could acquire both access and the necessary tools to conduct electronic surveillance relatively cheaply and easily.[44]

Electronic surveillance promised superior performance to the live agents it replaced.[45] Agents tire, but electronic surveillance can continue indefinitely. Though humans have limited memories that fade over time, electronic surveillance can create permanent and extensive records. While agents cannot surveil from a great distance or hide in tiny places, electronic devices can do both. Additionally, electronic surveillance improves upon the human senses. It permits one person to hear both sides of a telephone conversation and amplifies sounds that would otherwise be inaudible. In general, electronic surveillance has permitted law enforcement agents to be where they could not otherwise be, to perceive what they could not otherwise perceive, to have nearly infinite endurance, and to retain information forever.

When they have recognized the threat electronic surveillance poses to privacy, law enforcement representatives have typically claimed that legal requirements, such as the active involvement of a judge, afford sufficient protection against abuse.[46] They have largely dismissed the concerns of

---

39. *See, e.g.*, DASH, *supra* note 1, at 37-39, 43-44; THE CHALLENGE OF CRIME IN A FREE SOCIETY, A REPORT BY THE PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND THE ADMINISTRATION OF JUSTICE 468-73 (E.P. Dutton & Co. 1969) (1967) [hereinafter 1967 PRESIDENT'S COMMISSION] (reporting on these arguments and recommending, with some dissent, legislation to authorize electronic surveillance under stringent limitations).

40. *See, e.g.*, Berger v. New York, 388 U.S. 41, 73 (1967) (Black, J., dissenting).

41. *See* DASH, *supra* note 1, at 317-18.

42. *See id.* at 314 (discussing the use of "leased lines").

43. *See id.* at 279.

44. *See, e.g.*, *id.* at 58, 165, 219, 245-46; NATIONAL LAWYERS GUILD, RAISING AND LITIGATING ELECTRONIC SURVEILLANCE CLAIMS IN CRIMINAL COURT § 2.6 (1977) (detailing cooperation of telephone companies in wiretapping).

45. Of course, the devices did not always function properly. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 131 (1942) (describing the failure of a government installed "listening apparatus").

46. *See, e.g.*, Silver, *supra* note 10, at 839-41; *infra* note 459 (describing the involvement of judges

those who view electronic surveillance as the precursor to totalitarianism. For example, the almost invariable references to George Orwell's nightmare vision in 1984 may be met with a reminder that Orwell wrote fiction.[47] In short, those who support government surveillance maintain that fears about surveillance are entirely overwrought. I turn to those fears next.

3. *Electronic Surveillance: Its Threat to Privacy*

The same features of electronic surveillance that appeal to law enforcement agents threaten privacy. In particular, the hidden nature of surveillance, its ability to monitor continuously, and its very power and effectiveness have all concerned privacy proponents. Law enforcement's ability to conduct electronic surveillance in secret threatens privacy by inhibiting the public's ability to keep abreast of electronic surveillance practices and ensure agents stay within appropriate limits.

The hidden nature of electronic surveillance makes it more likely that an investigation will reveal private information. One is more inclined to reveal intimate facts on a wiretapped phone than to a law enforcement agent, even when the agent is undercover. Compared to unaided hearing, electronic surveillance is more sensitive to sound. People tend to regard as private the information they convey in whispers or hushed tones, but electronic surveillance may turn whispers into shouts in the ears of third party auditors.

Electronic surveillance monitors continuously, increasing the likelihood that people other than the target of the surveillance will have their private information disclosed. Even hardened criminals talk to their mothers and lovers, and these conversations are recorded along with their criminal plots.[48] Electronic surveillance is "indiscriminate" in the sense that it may obtain information that has no link to criminal activity.[49] Any number of entirely innocent people may either call or be called from a wiretapped phone. Electronic surveillance casts a far wider net than a traditional search for evidence of a crime at a target's home or business.[50]

---

in electronic surveillance investigations).

47. GEORGE ORWELL, 1984 (New American Library 1949). *See, e.g.*, Silver, *supra* note 10, at 848 (describing wiretapping opponents as having "vivid imagination[s]" and reminding that "facts are more reliable than fiction").

48. Even as to criminal plots, electronic surveillance may not always disclose the truth. Electronic records may be altered, meaning that false electronic surveillance evidence may improperly convince a factfinder. *See, e.g.*, DASH, *supra* note 1, at 368 (describing modification that was nearly impossible to detect). *But see* Lipset, *supra* note 10, at 876-85, 887-88 (describing the superiority of electronic surveillance for ascertaining the truth and suggesting the possibility of detecting editing).

49. *See, e.g.*, Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Proposal*, 52 COLUM. L. REV. 165, 170-71 (1952) (describing the illegal wiretapping of attorney-client strategy sessions); Williams, *supra* note 34, at 857-58 (describing wiretapping of "countless" people not suspected of any offense).

50. *See* Berger v. New York, 388 U.S. 41, 56 (1967) ("By its very nature eavesdropping involves an intrusion on privacy that is broad in scope.").

Finally, electronic surveillance cannot be effective unless it is secret. At a micro level, people will generally not reveal criminal activities on a line they know is tapped. At a macro level, they may avoid telephones altogether if they believe that wiretapping is common. More likely, targets will engage in counter-surveillance techniques such as using pay phones, code words, or disguising their voices. There has been an ongoing arms race between law enforcement agents who want to use electronic surveillance and those who want to avoid monitoring.[51] Law enforcement can minimize costs and increase the effectiveness of surveillance by keeping it secret.

Perhaps the most enduring privacy-based objection to electronic surveillance powers is that their very appeal will lead law enforcement to abuse them.[52] Though we agree that use of electronic surveillance should be limited, we cannot agree on the likelihood that those limits will be ignored. Privacy proponents look at a history of abuses and forecast more of the same; surveillance proponents look at the same facts and see a few aberrant cases and an overall record of compliance with legal requirements.[53] Whatever the truth, it cannot be denied that the more surveillance operates in secrecy, the more opportunity there is for abuse. Compared to traditional searches, where surely the neighbors and even the target would complain if the police engaged in large scale civil rights violations, law enforcement agents can use electronic surveillance investigations to flout the law without notifying anyone.[54]

Privacy proponents advocate a critical view of this pervasive formulation: the need to balance society's interest in effective law enforcement against the individual's right to privacy protection.[55] First, accepting the need to balance does not mean accepting a moderate amount of surveillance. The proper balance could well require that all surveillance be banned.[56] Moreover, privacy should not yield to surveillance when there are other ways to achieve the same law enforcement goals that do not invade

---

51. *See* DASH, *supra* note 1.

52. *See, e.g.*, Hennings, *supra* note 15, at 818 (finding "most disturbing" the violation of the law by police).

53. *Compare* S. REP. NO. 90-1097, at 71 (1968), *reprinted in* U.S.C.C.A.N 2112, 2160 (finding that New York officers had not abused electronic surveillance, and it was "idle to contend otherwise"), *with id.* at 137, *reprinted in* U.S.C.C.A.N 2112, 2226 (decrying "appalling" rampant illegal electronic surveillance by almost every metropolitan police department) (individual views of Sen. Long and Sen. Hart). *See also* DASH, *supra* note 1, at 40-42 (reporting that Justice Douglas reported 58,000 wiretap orders in New York City alone, but District Attorney Silver reported a total of only 480 orders in the same place and period).

54. CEDERBAUMS, *supra* note 12, at 24 (comparing searches of recorded conversations to conventional searches); Louis B. Schwartz, *On Current Proposals to Legalize Wire Tapping*, 103 U. PA. L. REV. 157, 163-64 (1954) (comparing wiretapping to search warrants); *see also* Silver, *supra* note 10, at 836 (noting the lack of signs that unlawful wiretaps have been made).

55. *See, e.g.*, LAPIDUS, *supra* note 3, at 196-98 (discussing the difficulty of measuring competing societal and individual interests and applying the balancing metaphor).

56. *See, e.g.*, Lopez v. United States, 373 U.S. 427, 464 (1963) (Brennan, J., dissenting) ("If in fact no warrant could be devised for electronic searches, that would be a compelling reason for forbidding them altogether. . . . Electronic searches cannot be tolerated in the name of law enforcement if they are inherently unconstitutional.").

privacy. Security is not always advanced by privacy-intruding techiniques. Often, people incorrectly assume that in exchange for privacy they will receive security.[57] At times, people may give up privacy in ways that harm security,[58] or in situations where improving security does not necessitate losing privacy.[59] Privacy should be reduced only when it results in a significant gain to investigative efficiency, and where no less restrictive means to promote law enforcement's goals exist.[60]

In sum, the nature of electronic surveillance makes it both appealing to law enforcement and destructive of an individual's privacy. The two are related in that the appeal of surveillance makes it likely that law enforcement will use it in ways that invade our privacy. The more we fear impropriety, the more we will look to the law to restore a proper balance. The next part discusses three particular challenges posed to legislators who sought to regulate electronic surveillance in 1968; it explores the complexity of wiretapping, the difficulty of controlling abuses, and society's ambivalence about it.

B. Accommodating Complexity

1. The Practices and Stages of Wiretapping

There are many different ways to conduct electronic surveillance, making it difficult to regulate by focusing on surveillance techniques.[61] For example, though wiretapping (involving the tapping of telephone wires) and bugging (requiring the placement of electronic listening devices) seem analytically distinct, the distinction between the two breaks down. Some de-

---

57. Those who have studied the public's choices regarding the privacy-security trade-off have observed a tendency to sacrifice privacy even when those sacrifices do not enhance security. *See, e.g.*, ROSEN, *supra* note 5, at 8, 34 (describing the public's interest in "feel-good" measures that bring no "demonstrable security benefits"); BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 38 (Paul Farrell et al. eds., 2003) (calling such actions as placing national guardsmen in airports in the wake of 9/11 "security theater" rather than security enhancing); *id.* at 251 ("People felt that they must be getting *something* because they were giving up so much [in the wake of 9/11].").

58. Some short-term measures may help reduce public panic. If maintained in the long term, however, they detract from effective efforts to enhance security and erode privacy and liberty. *See* ROSEN, *supra* note 5, at 8, 90-91; SCHNEIER, *supra* note 57, at 162-63, 243-49 (arguing that broadening surveillance powers may be "counterproductive" and never worth the loss to liberty and safety).

59. SCHNEIER, *supra* note 57, at 250 (finding the "association" between security and privacy to be "simplistic and misleading" because "the best ways to increase security are not necessarily at the expense of privacy or liberty").

60. Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Instrusive Alternative Analysis*, 63 N.Y.U. L. REV. 1173 (1988) (suggesting that courts look for less-privacy restrictive surveillance means when conducting the Fourth Amendment balancing test); *cf.* Marc Rotenberg, *Privacy and Secrecy After September 11*, 86 MINN. L. REV. 1115, 1134 (2002) ("[I]t remains critical that every proposal put forward by Congress after September 11 explains how new state authority will be balanced by new means of oversight."). For a statement of the view that no such case need be made, see Berger v. New York, 388 U.S. 41, 72 (1967) (Black, J., dissenting) (rejecting the need for empirical studies or statistics to prove effectiveness of electronic surveillance).

61. *See generally* DASH, *supra* note 1, at 303-81 (describing electronic surveillance tools in detail); WESTIN, *supra* note 15, at 69-90.

vices use the phone network to transmit bugged information, while some bugs are planted in telephones. During the period in which Congress prohibited wiretapping but not eavesdropping, myriad cases created confusing and arbitrary distinctions between permissible and impermissible practices.[62] I focus on wiretapping here, since it is most analogous to online surveillance.[63]

The numerous stages of a wiretapping investigation complicate efforts to regulate it. These stages may include: acquiring conversations, recording them, sharing them with agents in the same agency, sharing them with other agents, using them to obtain leads, using them to prosecute, notifying the target of them, introducing them in court, introducing evidence obtained by using them in court, divulging the existence of a wiretap, and reporting on wiretaps. During the years preceding the Wiretap Act, prosecutors seized on distinctions among these stages to support their ability to wiretap even though wiretapping was explicitly prohibited by federal law.[64]

Though the Wiretap Act is not free of the ambiguity that must attend regulation of electronic surveillance, it significantly clarified the prior law. The Act makes it illegal for anyone to use electronic surveillance to intercept wire or oral communications, thereby prohibiting both wiretapping and eavesdropping, unless such surveillance fits into the set of narrowly circumscribed exceptions.[65] It prohibits the interception of communications, their disclosure to others, and their use as evidence in court.[66] Segregating the different stages of investigation makes the legislation itself complicated, but the Act is comprehensive in scope.[67]

2. *Protecting Intangible Communications*

In 1967, the Supreme Court decided that electronic surveillance should be more strictly regulated than conventional searches.[68] In doing so, the Court removed a hurdle that had previously prevented it from treating electronic surveillance as a constitutionally regulated search. Since the *Olmstead* decision in 1928, the Court had required that surveillance physically intrude upon a constitutionally protected area, such as a home, in order to implicate the Fourth Amendment.[69] In *Katz v. United States,* the Court

62. *See* Lopez v. United States, 373 U.S. 427, 471 (Brennan, J., dissenting) (describing as "anomalous" the federal prohibition against wiretapping but not bugging); *see also infra* note 71 (discussing odd distinctions). Some commentators viewed the federal law prior to 1968 as entirely wrongheaded because they viewed bugging as the greater threat to privacy. *See, e.g.,* Hennings, *supra* note 15, at 815; Williams, *supra* note 34, at 862.

63. *See infra* Part V.

64. See *infra* Part II.D.1 for a detailed discussion of these arguments.

65. *See id.*

66. *Id.* § 2511(1)(a) (prohibiting interception); *Id.* § 2511(1)(c) (prohibiting disclosure); *Id.* § 2515 (prohibiting use as evidence in court).

67. According to one court, the "complex . . . Wiretap Act" is "famous (if not infamous) for its lack of clarity." Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

68. Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967).

69. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

famously announced that the "Fourth Amendment protects people, not places" and dispensed with the physical trespass requirement.[70] The Court thereby eliminated the silly technicality that led it tie Fourth Amendment protection to whether the listening device penetrated the wall of the target's home.[71]

In addition to the physical trespass requirement, the intangibility of conversations obtained by wiretapping posed a significant hurdle to constitutional regulation of electronic surveillance.[72] Finally, cases in the 1950s and 1960s established that the Fourth Amendment protects intangible conversations as well as tangible people and effects.[73] However, as late as 1967, Justice Black maintained that the Fourth Amendment applied only to tangible things and that conversations may not be searched or seized in a constitutional sense.[74]

Though the Supreme Court overcame its reluctance to view the spoken word as within the Fourth Amendment's purview, the intangibility of communications has complicated electronic surveillance law. For one thing, a conversation may be searched and seized without the target ever knowing.[75] Also, intangible conversations are more complicated than tangible objects, which typically have a form, a location, and an owner. Intangible conversations lack form, but they have other attributes. They occur somewhere in time, between participants who may be separated by space. They vary in their duration, in the media in which they occur, and of course, in their content. Conversations may even have multiple parties, some or all of whom may be difficult to identify.

When Congress passed the Wiretap Act, it covered almost all aspects of an intangible conversation, thereby obviating the complexity that would have arisen if it distinguished between its various attributes. The Wiretap Act protected the "contents" of communications, but expansively defined

---

70. *Katz*, 389 U.S. at 351-53.

71. *Compare* Goldman v. United States, 316 U.S. 129, 134 (1942) (finding no constitutional violation when sensitive "detectaphone" did not penetrate target's wall), *with* Silverman v. United States, 365 U.S. 505, 512 (1961) (finding a constitutional violation because a "spike mike" intruded an inch into the target's wall). *See also id.* ("We find no occasion to re-examine *Goldman* here, but we decline to go beyond it, by even a fraction of an inch.").

72. In *Olmstead*, the Court found it problematic that targets who contested electronic surveillance sought constitutional protection for intangibles. *See* 277 U.S. at 464-65 (construing the Fourth Amendment as limited to material things). Twenty-four years later, the Court stated that while the defendant might have had a constitutional claim if the government had seized his tangible property, he had none when his intangible conversations were obtained without physical trespass. On Lee v. United States, 343 U.S. 747, 753 (1952); *see also* Lopez v. United States, 373 U.S. 427, 438 (1963) (distinguishing between the surreptitious seizure of "something" and the acquisition of "statements").

73. *See, e.g.*, Wong Sun v. United States, 371 U.S. 471, 485-86 (1963) (excluding intangible statements overheard during the course of an unlawful search); Silverman v. United States, 365 U.S. 505, 512 (1961).

74. *See Katz*, 389 U.S. at 364-65 (Black, J., dissenting); *Berger*, 388 U.S. at 78-81 (Black, J., dissenting).

75. It is not entirely clear how to distinguish the search of a conversation from its seizure. For two attempts to do so, see *Berger*, 388 U.S. at 97-98 (Harlan, J., dissenting) and Larry Downes, *Electronic Communications Law and the Plain View Exception: More "Bad Physics,"* 7 HARV. J.L. & TECH. 239, 263-65 (1994).

"contents" as "any information concerning the identities of the parties to such communication or the existence, substance, purport, or meaning of that communication."[76] This simple approach maintained a high level of communications privacy that later, more complex, distinctions would erode.[77]

C. Reining in Electronic Surveillance

1. Justifying Wiretapping

During the debates that preceded passage of the Wiretap Act, three different perspectives emerged on the propriety of electronic surveillance by law enforcement.[78] One group viewed electronic surveillance as too dangerous to permit under any circumstances, no matter what the asserted justification.[79] The second group viewed it as generally inappropriate for law enforcement, but permissible if used solely to protect national security, so long as it was strictly regulated.[80] The third group claimed that a narrowly tailored law could provide sufficient safeguards to make electronic surveillance acceptable for law enforcement investigations of serious crimes as well as for national security investigations.[81]

Though the Attorney General and President Johnson belonged to the second group, the third group emerged victorious after a heated battle.[82] Nevertheless, while the supporters of law enforcement wiretapping won, they recognized the need to circumscribe electronic surveillance. Therefore, the Wiretap Act permits electronic surveillance only for investigation of serious crimes or those connected to organized crime.[83]

It is difficult to assess whether or not the list of crimes is too long and whether or not electronic surveillance has been used in the way its support-

---

76. 18 U.S.C. § 2510(8) (1968). The definition of contents was designed to be comprehensive. *See* S. REP. NO. 90-1097, at 91 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2179 (defining "contents" to include "all aspects of the communication").

77. *See infra* Part III.B.2 (discussing the complexity of online surveillance of communications, communications attributes, and web browsing).

78. *See* Berger v. United States, 388 U.S. 41, 113 (White, J., dissenting) (describing the three positions as having emerged during hearings).

79. *See* Lipset, *supra* note 10, at 873 (describing this view as the "presumption" among the public, legislators, and judges).

80. *See, e.g.*, DIFFIE & LANDAU, *supra* note 7, at 170-71 (presenting views of several law enforcement officials who opposed law enforcement wiretapping); Williams, *supra* note 34, at 868; *infra* note 118 (discussing national security surveillance).

81. *See, e.g.*, William P. Rogers, *The Case for Wire Tapping*, 63 YALE L.J. 792, 793 (1954); Silver, *supra* note 10, at 844-51.

82. *See Berger*, 388 U.S. at 113-15; Right to Privacy Act of 1967, S. 928, 90th Cong. (1st Sess. 1967) (containing the Administration's proposal to prohibit wiretapping except for national security purposes); LAPIDUS, *supra* note 3, at 13, 40. Twenty-one Senators co-sponsored the Right to Privacy Act. *See* S. REP. NO. 90-1097, at 161 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2223.

83. *See* 18 U.S.C. § 2516(1). Some contemporary commentators viewed the organized crime rationale as only partly genuine, in that law enforcement used electronic surveillance as much to support corruption and bribery as to catch criminals. *See, e.g.*, DASH, *supra* note 1, *passim*; Hennings, *supra* note 15, at 822-23 (quoting those who saw wiretapping as more useful to support corruption than to catch criminals). The public's fear of organized crime contributed to its support of the Act. *See infra* note 112.

ers claimed it would.[84] The reports designed to permit public assessment of electronic surveillance yield ambiguous data.[85] What is not ambiguous is that the Wiretap Act endeavors to keep electronic surveillance practices tightly controlled. Most of those controls are constitutionally mandated, as the next subpart details.

2. *Meeting the Constitutional Requirements*

When Congress passed the Wiretap Act in 1968, it benefited from the Supreme Court's recent guidance. The year before, the *Katz* case held that wiretapping and eavesdropping by law enforcement agents was a constitutional search that would need to satisfy the Fourth Amendment prerequisites.[86] Six months earlier, in *Berger v. New York*, the Court delineated exactly what was required by the Fourth Amendment in the context of electronic surveillance.[87] In *Berger*, the Court invalidated a New York eavesdropping statute that it found so permissive as to be an unconstitutional general warrant.[88]

The *Berger* decision was quite controversial at the time.[89] To those who opposed law enforcement surveillance, the Court invited legislatures to pass a law permitting the practice at a time when federal law entirely prohibited electronic surveillance.[90] At the same time, the requirements the Court set out were so restrictive that proponents questioned whether law enforcement surveillance could ever pass constitutional muster.[91]

In *Berger*, the Court required any court order approving electronic surveillance to be issued only upon a finding of probable cause.[92] Applying the text of the Fourth Amendment, the Court required that applications for court orders state with particularity the offense, the place to be searched, and the

---

84. In the 1970s, gambling and narcotics were the most popular crimes investigated, rather than murder and the like. *See* LAPIDUS, *supra* note 3, at 76. While those investigations may have involved low-level mob figures, it seems clear that the top echelon were not surveilled. *See id.* at 60-66, 142-43, 212-13. *But see*, Silver, *supra* note 10, at 843-44 (defending the use of wiretaps to investigate gamblers, who are often linked with organized crime). State agents may use electronic surveillance in pursuit of evidence of "murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year." 18 U.S.C. § 2516(2) (2002).

85. *See* LAPIDUS, *supra* note 3, at 210-11, 216-19.

86. Katz v. United States, 389 U.S. 347, 353, 356-57 (1967).

87. 388 U.S. 41, 64 (1967).

88. *Id.*

89. The *Berger* decision has three dissents. On the other hand, Justice Harlan later argued that *Berger* was part of a natural progression rather than a distinct break. *See* United States v. White, 401 U.S. 745, 780 (1971) (Harlan, J., dissenting).

90. *See, e.g.*, CEDERBAUMS, *supra* note 12, at 15-16; LAPIDUS, *supra* note 3, at 11-12, 14-15; *infra* note 119 and accompanying text.

91. *See, e.g.*, *Berger*, 388 U.S. at 71 (Black, J., dissenting); *id.* at 111 (White, J., dissenting); *White*, 401 U.S. at 779-80 (Harlan, J., dissenting) (recounting that the government made the same argument in *Berger*).

92. *Berger*, 388 U.S. at 54-55. The Court refused to determine whether New York's reasonable grounds standard was equivalent to probable cause. *Id.* at 55. The Court required probable cause before granting extensions as well. *Id.* at 59.

things to be seized.[93] In fact, the Court said that in order to avoid giving investigators a "roving commission" to search any and all conversations, the conversations and person whose conversations were sought had to be identified in the court order application.[94] The Court expressed concern about the length of orders, which was up to two months under the New York eavesdropping statute. The Court required that electronic surveillance investigations could be no longer than necessary and that they cease upon finding the sought-after information.[95] The Court also discussed the need for a return of the warrant, so that the officer alone would not decide how to use the seized conversations. Overall, the Court emphasized the need for "adequate judicial supervision or protective procedures."[96]

Drafters of the Wiretap Act attempted to accommodate *Berger*. The Act permits law enforcement agents to use electronic surveillance only if a reviewing judge finds probable cause to believe the target "is committing, has committed, or is about to commit" a particular enumerated offense and that the surveillance will obtain incriminating communications about the offense.[97] The Act also requires that agents minimize the interception of non-incriminating communications.[98] The investigation must terminate as soon as the information is acquired, and in any case within thirty days, unless an extension is granted.[99] The Act requires notice to targets, which may be delayed until the investigation is complete.[100] It mandates the extensive involvement of a judicial officer in the entire process.[101]

Compared to the regulations that govern traditional searches, the requirements for electronic surveillance are much more restrictive. In fact, the Wiretap Act requires that electronic surveillance be used only as a last resort after conventional techniques have failed.[102] As a result of the Wiretap Act's heightened requirements, one commentator has labeled the court order required to conduct electronic surveillance a form of "super-warrant."[103]

Several commentators nonetheless viewed the Act's provisions as insufficient, particularly its failure to satisfy adequately the requirements of particularity, notice, and return of the warrant.[104] Ultimately, however, its con-

---

93. *Id.* at 56.
94. *Id.* at 59.
95. *Id.* at 59-60.
96. *Id.* at 60.
97. 18 U.S.C. § 2518(3) (2000).
98. *Id.* § 2518(5).
99. *Id.* Judges must make the same findings of probable cause before issuing any extensions. *Id.*
100. *See* 18 U.S.C. § 2518(8)(d). The Court in *Berger* mentioned that notice was a constitutional requirement, but that it could be delayed upon a showing of exigent circumstances. *Berger*, 388 U.S. at 60.
101. *See infra* notes 151-54 and accompanying text (discussing involvement of the judge in investigations).
102. *See* 18 U.S.C. § 2518(3)(c) (2000) (granting judge must first determine 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").
103. Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 630 (2003).
104. *See* Lopez v. United States, 373 U.S. 427, 463-64 (1963) (Brennan, J., dissenting) (discussing

stitutionality was established.[105] But in upholding the Act's provisions, courts have spilled considerable ink detailing the threat to privacy that law enforcement surveillance poses. The carefully circumscribed procedures and the active involvement of a judge in approving and monitoring investigations have allowed the Wiretap Act to pass constitutional muster.[106]

D. Resolving Ambivalence

The Supreme Court's 1967 decisions were a watershed moment for communications privacy. After decades of debate and failed bills, Congress finally passed a new law regulating electronic surveillance the following year. But while the Wiretap Act brought critically needed uniformity to federal surveillance law, it replaced a prior federal law that should have obviated that need. The Communications Act of 1934 had explicitly prohibited all law enforcement use of wiretapping.[107] Surprisingly, some viewed the Court's extension of constitutional protection to surveillance targets as the only way to give teeth to a prohibition that was widely ignored.[108]

The widespread use of wiretapping by both federal and state law enforcement agents in violation of federal and often state law reflects this country's historical ambivalence about electronic surveillance.[109] These mixed feelings spring from several sources. The topic can be quite often emotion-laden, with both sides projecting catastrophic consequences if they lose. Wiretapping proponents have charged that if we fail to permit law enforcement surveillance, we will be overridden by criminals and saboteurs.[110]

---

the Act's failure to satisfy the requirements of particularity and return of warrant); LAPIDUS, *supra* note 3, at 179 (discussing the Act's failure to satisfy the requirements of particularity and notice). However, the Act does provide that the judge may require periodic progress reports of investigations and should be provided any recordings of intercepts. 18 U.S.C. §§ 2518(6), (8)(a) (2000).

105. *See, e.g.*, United States v. Donovan, 429 U.S. 413, 429 n.19 (1977) (finding the notice and return provisions of the Wiretap Act to "satisfy constitutional requirements"); United States v. Tortorello, 480 F.2d 764, 773 (2d Cir. 1973) (finding the Wiretap Act to satisfy the particularity requirement).

106. *See, e.g.*, United States v. United States Dist. Ct., 407 U.S. 297, 316-17 (1972) (recognizing that the Fourth Amendment requires pre-investigation judicial review for domestic surveillance); S. REP. NO. 90-1097, at 96 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185 (describing the "practical and constitutional demand that a neutral and detached authority be interposed between the law enforcement officers and the citizen").

107. *See infra* note 119 and accompanying text.

108. *See, e.g.*, On Lee v. United States, 343 U.S. 747, 759-60 (1952) (Frankfurter, J., dissenting) (decrying the "pervasive disregard" for the Communications Act by law enforcement officers and advocating that *Olmstead* be overruled); Williams, *supra* note 34, at 868-71 (discussing the extension of Fourth Amendment protection to surveillance targets).

109. *See, e.g.*, LAPIDUS, *supra* note 3, at 1 ("The public, confused by conflicting contentions, is uncertain and uneasy."); Hennings, *supra* note 15, at 818 (calling "the conflict of the law . . . symptomatic of the doubts and indecision of both the public and the lawmakers . . . on how best to deal with wiretapping").

110. *See, e.g.*, Nardone v. United States, 302 U.S. 379, 387 (1937) (Sutherland, J., dissenting) ("[I]n the light of the deadly conflict constantly being waged between the forces of law and order and the desperate criminals who infest the land, [prohibiting government wiretapping to protect privacy means] the necessity of public protection against crime is being submerged by an overflow of sentimentality."); Hennings, *supra* note 15, at 816 (quoting a police chief who predicted the end of free society if law enforcement agents could not wiretap); Silver, *supra* note 10, at 844-51 (arguing that wiretapping is

Opponents invoke a picture of totalitarian oppression by an omniscient government.[111] Each side's vehemence and even persuasiveness may lead people to flip-flop. Perhaps views vary based on people's relative fears of crime and government oppression.[112] It is difficult to make a clear choice between the two positions, because each rests on future predictions. By the time we get to either a chaotic criminal society or a Big Brother government, it will be too late. But the question remains: What do we do today?

One choice for the ordinary citizen is to remain ignorant of the extent of government surveillance.[113] That strategy may be rational because it significantly reduces the inhibiting effect of government surveillance. Surveillance opponents worry that if we believe we are being watched, we will be inhibited from expressing ourselves and associating with others.[114] If we do not think about monitoring, we lose those inhibitions. Even if our government *is* watching us, if we don't know about it, in some sense it cannot hurt us—so long as we are never prosecuted or otherwise harmed by the disclosure. That may go a long way towards explaining why we repeatedly believe government eavesdroppers when they ask that we trust them not to break the law, even though the historical record reveals consistent illegality.[115]

Of course, if we remain ignorant, we can still be injured in the sense that our private information is revealed. But here, the distinction between "innocent" and "guilty" targets of surveillance complicates the picture. Those that believe themselves to be fundamentally "innocent" may view the privacy deprivations that accompany excessive surveillance as relatively harmless. Some people undoubtedly view the civil rights of criminals as less worthy than those of "innocent" people. Of course, under a totalitarian regime, there may well be few who count as "innocent." And criminals should

---

essential to combating modern criminals).

111. *See, e.g.*, Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting) (commenting that electronic surveillance is "more penetrating, more indiscriminate, more truly obnoxious to a free society" because it "makes the police omniscient; and police omniscience is one of the most effective tools of tyranny").

112. Edith Lapidus has suggested that the impetus for passage of the Wiretap Act was increased fear of organized crime. LAPIDUS, *supra* note 3, at 12-13, 205.

113. *See* DASH, *supra* note 1, at 9 (observing that "[a]lmost all the law professors, defense attorneys, public defenders, and civil liberties organizations pleaded ignorance of the subject" of wiretapping when questioned). Dash wrote that the confusing state of wiretapping law and the conflicting reports about its use during the 1950s meant that "although people read all about wiretapping, they actually know little or nothing about it." *Id.* at 5. In all of the jurisdictions that Dash studied in depth, he found that most local citizens seemed utterly unaware of the extent of illegal police surveillance. *See id.* at 121, 128, 144-45, 162, 217 (providing examples of communities who seemed to accept what turned out to be false denials of wiretapping by local police).

114. For eloquent statements of this concern, see United States v. United States Dist. Ct., 407 U.S. 297, 314 (1972) ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power . . . [f]or private dissent, no less than open public discourse, is essential to our free society."); United States v. White, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting) ("Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances."); *Lopez*, 373 U.S. at 470 (Brennan, J., dissenting) ("[F]reedom of speech is undermined where people fear to speak unconstrainedly in what they suppose to be the privacy of home and office.").

115. *See, e.g.*, 1967 PRESIDENT'S COMMISSION, *supra* note 39, at 470 (claiming that past abuses had been largely curtailed); *supra* note 113 and accompanying text.

not be considered guilty until they are tried under a system that respects their civil rights. At some level, the common sense intuition that all surveillance that uncovers criminal activity is justified conflicts with our commitment to due process.

Although Congress did not explicitly acknowledge any ambivalence towards electronic surveillance when it passed the Wiretap Act, the Senate Report complained that the prior legal regime had done little to stop illegal wiretapping.[116] The following elaborates on why there was so much illegal wiretapping prior to the Wiretap Act's passage and the Act's safeguards to prevent a recurrence.

1. Aggressive Interpretations and Judicial Review

Not all of the agents who wiretapped prior to the Wiretap Act intentionally broke the law. Some apparently viewed their surveillance as permitted.[117] It took years of litigation for the courts to reject almost all of the rationalizations offered for government wiretapping despite federal law explicitly prohibiting wiretapping from 1934 to 1968.[118] In particular, Section 605 of the Communications Act of 1934 provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[119] The Act also prohibited using intercepted information for personal use.[120] Although the Act might not seem ambiguous, state and federal prosecutors seized upon and arguably invented ambiguities to justify their wiretapping investigations.

For example, three years after the Communications Act took effect, in *Nardone v. United States* federal agents argued that the government was not explicitly prohibited from wiretapping by the Act, and thus prosecutors

---

116. S. REP. NO. 90-1097, at 67 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2156.

117. Rogers, *supra* note 81, at 794.

118. Successive attorneys general claimed the power to wiretap on behalf of the president to protect national security, which the courts did not deny. *See, e.g., id.* at 794-96 (reviewing that history). The Wiretap Act specifically excluded national security investigations from its purview. 18 U.S.C. § 2511(3) (1968) (repealed by the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, § 201(c), 92 Stat. 1796 (1978) (codified at 50 U.S.C. §§ 1801-1811 (2000)). *But see United States Dist. Ct.*, 407 U.S. at 324 (holding that the Wiretap Act did not grant the government unbridled power in domestic security surveillance). Today, investigations of foreign threats to national security largely proceed under FISA, which is significantly more permissive than the Wiretap Act. The USA PATRIOT Act expanded FISA's scope and further blurred the line between electronic surveillance for law enforcement purposes and for foreign intelligence purposes. The scope of foreign intelligence surveillance is critically important, but it is beyond the scope of this Article. *See generally* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1 (2000) (reviewing history); Peter P. Swire, *supra* note 17 (reviewing the history of and recent amendments to FISA).

119. Communications Act of 1934, ch. 652, 48 Stat. 1064, 1100 (codified at 47 U.S.C. § 605 (1958) (amended 1968)).

120. The Act provided that "no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect or meaning of the same or any part thereof, knowing that such information was so obtained, shall . . . use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto." *Id.*

could introduce government wiretap-derived evidence in court.[121] The government contended that though the Act made wiretapping by any "person" punishable by a fine and imprisonment, Congress did not intend to prohibit government wiretapping.[122] The government claimed that it was "improbable Congress intended to hamper and impede the activities of the government in the detection and punishment of crime."[123]

The Supreme Court disagreed and construed the Act's "plain words" and "clear language" to prohibit the government's recitation of the contents of wiretap evidence in a federal criminal prosecution.[124] The Court explained that "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty."[125] Thus interpreting the Act "to include within its sweep federal officers as well as others," the Court reversed the defendant's conviction.[126] Two years later, the Court clarified that evidence both directly and indirectly obtained by wiretapping was not admissible in court, relying on the "fruit of the poisonous tree" doctrine.[127] In the second *Nardone* decision, the Court reasoned that in forbidding "the acquisition of evidence in a certain way," the Communications Act meant "not merely [that] evidence so acquired shall not be used before the Court, but that it shall not be used at all."[128]

Despite this expansive language, federal agents interpreted the two *Nardone* decisions as merely prohibiting the introduction of wiretap-derived evidence and its fruits into federal court.[129] The government relied on the statute's admonition that "no person" shall "intercept . . . and divulge or publish" to permit federal agents to intercept communications and divulge them to each other.[130] The government maintained that federal agents who worked for a single agency constituted "one person," so information sharing by members of one agency did not count as divulging or publishing the information to another person.[131]

Despite criticism from contemporary commentators, the federal government persisted in this interpretation for decades. The argument was

---

121. Nardone v. United States, 302 U.S. 379, 380-82 (1937).
122. *Id.* at 381-82 (citing 47 U.S.C. § 501 that punished "wilful and knowing" violations of § 605).
123. *Id.* at 383; *see also id.* at 385 (Sutherland, J., dissenting) (doubting that Congress "intended to tie the hands of the government in its effort to protect the people against lawlessness of the most serious character").
124. *Id.* at 382.
125. *Id.* at 383.
126. *Id.* at 384.
127. Nardone v. United States, 308 U.S. 338, 338 (1939).
128. *Id.* at 340-41.
129. *See, e.g.*, DIFFIE & LANDAU, *supra* note 7, at 157-65 (reviewing government justifications for wiretapping during this period); Hennings, *supra* note 15, at 830-31 (summarizing the Department of Justice's arguments made during Congressional hearings).
130. 47 U.S.C. § 605 (2000).
131. *See* DASH, *supra* note 1, at 394 (discussing this interpretation); Williams, *supra* note 34, at 859-60.

called "the greatest legal fiction ever engaged in by the Federal Government,"[132] and "patently absurd."[133] After all, nothing in the statute suggested that an agency of the government could be considered one person. As for the Court, it never directly addressed the government's interpretation.[134] In 1968, it did find that the "federal law itself explicitly protects intercepted communications from divulgence, in court or any other place," however, that was in the context of wiretapping by state law enforcement agents.[135]

Shortly after the *Nardone* decisions, the Court clarified that the Communications Act applied to both interstate and intrastate telephone calls.[136] This holding, in combination with the Supremacy Clause, should have convinced state agents that their wiretapping was illegal. Yet, prior to the passage of the Wiretap Act, many state law enforcement agents contended *they* could wiretap notwithstanding the federal law.

Some state legislatures passed laws after 1934 specifically permitting wiretapping, thus encouraging state agents to believe that they could wiretap.[137] State courts ruled that state statutory and constitutional law, not federal statutory law, governed state wiretapping practices.[138] Finally, in 1957, the Supreme Court stated that Congress did not mean to allow state legislation that would contradict Section 605 of the Communications Act.[139] Even so, officials in New York continued to view its state statute permitting wiretapping as good law.[140]

Surprisingly, the Supreme Court countenanced, for a short time, the introduction of wiretap-derived evidence by state agents in state court, though it acknowledged such evidence would not be admissible in federal court.[141] In 1952, the Court followed the lead of a Texas statute and refused to exclude wiretap-derived evidence from a Texas state court trial, though it

---

132. CEDERBAUMS, *supra* note 12, at 14.

133. Williams, *supra* note 34, at 860-61; *see also* Hennings, *supra* note 15, at 832 (rejecting the argument). The Supreme Court later characterized its rejection of the government's argument as "unequivocal." Lee v. Florida, 392 U.S. 378, 382 (1968) (referring to Nardone v. United States, 302 U.S. 379, 382 (1939)).

134. Commentators questioned whether the statute necessarily meant to preclude interception only when combined with a divulgence or a publication. *See, e.g.*, LAPIDUS, *supra* note 3, at 11; Westin, *supra* note 49, at 169-71. The Supreme Court left the point open. *See* Benanti v. United States, 355 U.S. 96, 100 n.5 (1957) (leaving open the question of whether violations required both elements); Goldstein v. United States, 316 U.S. 114, 122 (1942) (declining to consider whether the Communications Act precluded use of wiretap-derived information by federal officers for obtaining evidence).

135. *Lee*, 392 U.S. at 385.

136. Weiss v. United States, 308 U.S. 321, 329 (1939) (explaining that the language of the Communications Act does not exclude intrastate communications).

137. *See* Berger v. New York, 388 U.S. 41, 48-49 (1967) (surveying state laws on electronic surveillance); DASH, *supra* note 1, at 35-160 (studying "permissive jurisdictions").

138. Of course federal constitutional law did not find electronic surveillance to implicate the Constitution until 1967. *See supra* Part II.C.2.

139. *See Benanti*, 355 U.S. at 105-06. The statement was arguably dicta, however, because the Court was considering whether wiretapped evidence could be introduced in federal court.

140. *See* 1967 PRESIDENT'S COMMISSION, *supra* note 39, at 472 (reporting that New York law enforcement officers working in areas other than New York City wiretapped and introduced the evidence gathered in court); DASH, *supra* note 1, at 4, 395; Hennings, *supra* note 15, at 826-28.

141. *See* Schwartz v. Texas, 344 U.S. 199, 203 (1952), *overruled by* Lee v. Florida, 392 U.S. 378 (1968).

recognized that the state agents violated federal law when they introduced the evidence.[142] Two days before the Wiretap Act's passage, the Court saw the error of its ways and overruled its prior decision. The Court held that state courts may not permit the introduction of wiretap-derived evidence, regardless of state law.[143]

Even when federal officials conceded the prohibition, they argued that state agents who violated the law could give illegally obtained information to federal agents.[144] However, in 1957 the Court reversed a decision permitting this practice,[145] holding that "evidence obtained by means forbidden by Section 605, whether by state or federal agents, is inadmissible in federal court."[146] In light of federal law prohibiting the practice, the Court's decision is not surprising. However, it is odd that for the twenty-three years preceding this decision, federal agents were able to introduce evidence obtained by wiretapping in federal court, so long as state agents conducted the surveillance.

In addition to complications that arose from the state and federal split, some law enforcement agencies used private entities to facilitate illegal wiretapping. Samuel Dash reported that in San Francisco private parties wiretapped pursuant to a deal: If caught, the wiretapper would not implicate the police, if the police agreed not to punish the wiretapper.[147] Wiretapping by private entities had long been a federal felony; but federal courts permitted the introduction of evidence obtained by a private wiretapper.[148] Similarly, phone company involvement in wiretapping blurred the lines between private and public wiretapping.

Taking into account the various appellate court decisions clarifying the 1934 law, by 1968 it should have been clear that wiretapping was entirely prohibited for law enforcement purposes. However, wiretapping persisted. The Wiretap Act explicitly covered all federal law enforcement agents, and mandated that states could pass their own laws patterned after the federal model.[149] The Act generally prohibited private surveillance and permitted few exceptions.[150]

---

142. *See* Schwartz, 344 U.S. at 201-02. Several states permitted the introduction of wiretap evidence into state court, even when it was illegal to wiretap under state law. *See, e.g.*, Silver, *supra* note 10, at 853 (discussing cases).

143. Lee v. Florida, 392 U.S. 378, 386-87 (1968).

144. It had also been a longstanding practice to admit into federal court evidence obtained in violation of state rather than federal law. *See, e.g.*, On Lee v. United States, 343 U.S. 747, 754-55 (1952); Olmstead v. United States, 277 U.S. 438, 468 (1928).

145. *See Benanti*, 355 U.S. at 99 (ruling out the use of evidence obtained in conformity with state law).

146. *Id.* at 100.

147. DASH, *supra* note 1, at 164.

148. *See* CEDERBAUMS, *supra* note 12, at 11 (discussing Burdeau v. McDowell, 256 U.S. 465 (1921) (permitting the admission in a criminal case of private papers unlawfully seized by a private citizen)).

149. 18 U.S.C. §§ 2515, 2516(2) (1968).

150. 18 U.S.C. § 2511 (1968). As mentioned, the Wiretap Act excluded national security investigations from its purview. *See supra* note 118. For an important recent study of wiretapping under state law, see Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L.J. 971. 983-85 (2003).

Additionally, the Wiretap Act provided several responses to the new aggressive interpretations that the inherent complexity of the Act might engender.[151] The involvement of a neutral judge at all stages of wiretapping investigations provided an important check on unlawful investigations. As discussed, a reviewing judge must agree with the applicant that the statute's extensive requirements are met before approving any order or extension.[152] The judge must approve of the length of any investigation, and may require periodic progress reports in order to make sure that it stays within proscribed limits.[153] After an investigation is completed, the judge determines where to keep records of the surveillance. The judge also decides to whom notice will be given, who will get a copy of the recorded information, and what exactly will be disclosed.[154]

Although some critics have complained that judges grant almost all wiretap applications, others explain that the need to meet strict requirements and to go through several levels of review means that questionable applications never appear before a judge.[155] Meanwhile, prosecutors have claimed that the need to impress a judge with the necessity of using wiretapping meaningfully limits the number of cases in which law enforcement even considers using electronic surveillance.[156]

Post-investigation review provides another important check on abusive practices and aggressive interpretations. The Wiretap Act explicitly provides that those injured by improper investigations can have the evidence and its fruits excluded from any proceedings against them.[157] This exclusionary remedy deters law enforcement officers from breaking the wiretap law.[158] Moreover, the judge has an opportunity to refine and clarify the Act's provisions when a defendant challenges government practices in a motion to suppress. Such opportunities arise often, as motions to suppress have been common.[159] One practical guide from the late seventies advised criminal defendants to accuse prosecutors of unlawful surveillance in nearly

---

151. As an example of a modern aggressive interpretation, the Third Circuit recently rejected an attempt by the government to require (by subpoena) an illegal private wiretapper to disclose the information she acquired to a grand jury. The government claimed that since it was not involved in the unlawful surveillance, it had "clean hands." The court applied 18 U.S.C. § 2515, which prevents the disclosure of unlawfully intercepted information in any proceeding. *See In re* Grand Jury, 111 F.3d 1066 (3d Cir. 1997).

152. *See* 18 U.S.C. §§ 2518(3), (5) (1993 & Supp. 2004); *see also supra* notes 97-101 and accompanying text.

153. *Id.* §§ 2518(5), (6) (1993 & Supp. 2004).

154. *Id.* § 2518(8) (1993).

155. *See* LAPIDUS, *supra* note 3, at 91, 118, 163; Hennings, *supra* note 15, at 819-20.

156. *See* LAPIDUS, *supra* note 3, at 163; Silver, *supra* note 10, at 840-41.

157. *See* 18 U.S.C. § 2510(11) (1993) (providing for a statutory exclusionary rule for any "aggrieved person," which includes "a person who was a party to any intercepted . . . communication or a person against whom the interception was directed"); *id.* § 2518(10) (1993 & Supp. 2004).

158. *See* Lee v. Florida, 392 U.S. 378, 386-87 (1968); *see also* LAPIDUS, *supra* note 3, at 163-67.

159. *See* LAPIDUS, *supra* note 3, at 165-70 (reporting that wiretapping suppression motions were often brought in the 1970s); *see also* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 77 (1997) ("Between 1985 and 1994, judges nationwide granted 138 suppression motions while denying 3,060 . . . .").

all criminal cases.[160] Further, as the next subpart discusses, the Act offered substantial incentives to bring civil cases, which further refines the Act's parameters.

2. *Underenforcement and New Remedies and Punishments*

We will never know the extent of illegal surveillance, but we do know that prior to the Wiretap Act agents conducted a significant number of wiretapping investigations even when it was illegal to do so. Law enforcement agents simply broke the law.[161] Despite the prevalence of illegal surveillance, the historical record reveals a surprising paucity of prosecutions. Federal prosecutors brought only a handful of cases against violators of the 1934 Communications Act, and all cases were against private parties rather than law enforcement agents. Even when confronted with flagrant violations, the Justice Department refrained from prosecuting state or federal agents.[162] Some contemporary commentators suggested that law enforcement agents felt little incentive to prosecute others for relying on the same strained interpretations of the law that the executive branch itself used.[163] The underenforcement of the federal law helps explain the paradox that several commentators viewed proposals to permit surveillance for the first time as opportunities to crack down on illegal wiretapping.

The Wiretap Act notably improved the 1934 law by enhancing penalties for unlawful surveillance and increasing incentives to bring suit. Violators of the Wiretap Act faced a significant fine and jail time. In addition, the Act gave standing to bring civil claims for damages against violators to any person whose communications were intercepted, disclosed, or used in violation of the Act.[164] In contrast, the Communications Act of 1934 had not clearly provided for civil claims.[165] Under the Wiretap Act, a victim could receive attorney's fees, punitive and actual damages, or statutory damages.[166] By expanding the ways to deter unlawful surveillance, Congress reduced the chance that the law would be flouted extensively.

---

160. *See* NATIONAL LAWYERS GUILD, *supra* note 44, at § 3-1.

161. *See supra* notes 12-15 and accompanying text.

162. *See Lee*, 392 U.S. at 386 n.12 ("Research has failed to uncover a single reported prosecution of a law enforcement officer for violation of § 605 since the statute was enacted."); LAPIDUS, *supra* note 3, at 42; *see also* 1967 PRESIDENT'S COMMISSION, *supra* note 39, at 472 ("[T]he lack of prosecutive action against violators has substantially reduced respect for the law.").

163. *See, e.g.*, Westin, *supra* note 49, at 169.

164. *See* 18 U.S.C. § 2518(10) (1993 & Supp. 2004). Note that standing under the Wiretap Act is considerably broader than standing under the Communications Act. *See* Goldstein v. United States, 316 U.S. 114, 121 (1942) (denying standing under § 605 to those who are not parties to the intercepted communications).

165. *See Lee*, 392 U.S. at 387 (Black, J., dissenting) (noting that the Act might imply some civil remedies); *see also* DASH, *supra* note 1, at 403-05 (describing hurdles to bringing civil claims under the Communications Act).

166. *See* 18 U.S.C. § 2520 (1993 & Supp. 2004).

3. Secret Practices and Reporting Obligations

As discussed, law enforcement benefits in several ways from the secrecy of its surveillance. The less people know about surveillance, the more information surveillance reveals and the less law enforcement needs to spend on counter-surveillance efforts. In fact, before the Wiretap Act, law enforcement agents took steps to keep public awareness of surveillance at a minimum, because disclosures of surveillance were often followed by calls for reform.[167] Nonetheless, by its very nature secret surveillance prevents the public from ensuring that surveillance is kept within appropriate limits.

It is not true that if we wait long enough, the extent of electronic surveillance will eventually come to light. Not all surveillance information makes it into court as evidence. Much of it is used merely to generate leads. More perniciously, law enforcement agents may use surveillance information for extortion. Several sources report that agents used surveillance to keep track of targets' illegal profits, so that agents would know how much kickback money to demand.[168] Surveillance has also been used in promoting public corruption and intimidating government critics.[169] Even requests made under the Freedom of Information Act will not uncover surveillance that has been classified.[170] In short, much surveillance proceeds without public awareness.

The Wiretap Act combats surveillance secrecy by providing for post-investigation notice to those affected by a wiretap investigation. Notice must be provided to anyone named in an application, as well as anyone else the reviewing judge deems appropriate.[171] Congress viewed the notice provision, in combination with civil remedies, as an important check on unlawful practices.[172]

In addition to notifying the targets of surveillance, the Act was intended to provide the public, including Congress, with an overall picture of wiretapping practices each year. To that end, prosecutors and judges involved in electronic surveillance investigations must submit detailed yearly reports on electronic surveillance practices.[173] These reports form the basis for the Report on Wiretapping, published each year. The report's statistics are designed to reveal the extent of wiretapping, its cost, and its effectiveness in combating crime.[174]

The information published is not always complete; nor is it straightforward to analyze. The reports exclude information about foreign intelligence

---

167. *See, e.g.*, DASH, *supra* note 1, at 99-100, 221-22, 251.
168. *See, e.g.*, LAPIDUS, *supra* note 3, at 130.
169. *See, e.g.*, DASH, *supra* note 1, at 56, 60, 123-28; SUMMERS, *supra* note 16; NATIONAL LAWYERS GUILD, *supra* note 44, 1-10.
170. *See* 28 C.F.R. § 16.7 (1999).
171. 18 U.S.C. §§ 2518 (8)(d), (9) (1993).
172. *See* S. REP. NO. 90-1097, at 105 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2194.
173. *See* 18 U.S.C. § 2519(2) (1993 & Supp. 2004).
174. *Id.* § 2519(3).

taps, and consensual taps that may proceed without court order. Obviously, the reports omit unauthorized wiretaps. Yet the reporting requirement permits at least a rough sense of the extent and nature of official law enforcement electronic surveillance by court order. In recent years, use of this surveillance has grown markedly.[175]

4. *Line Drawing and Reasonable Expectations of Privacy*

The tortured history of federal statutory regulation is not the only evidence of society's mixed feelings about wiretapping during the period preceding the Wiretap Act. Supreme Court Justices also exhibited ambivalence towards electronic surveillance. At the extremes, Justice Douglas repeatedly inveighed against the practice and Justice Black consistently defended it.[176] Other Justices took seemingly contradictory positions. For example, Justice Stewart wrote the majority decision in *Katz v. United States*[177] that extended constitutional protection to wiretapping and eavesdropping and Justice Harlan formulated the "reasonable expectation of privacy" test in a concurring opinion.[178] But six months earlier, in *Berger v. New York*, both Justices viewed the New York statute as constitutional on its face, disagreeing with the majority.[179] Moreover, both Justices authored opinions significantly curtailing the privacy protection of electronic surveillance.[180]

With that in mind, it should not be surprising that the decision credited with protecting a target's privacy granted rather anemic protection. In *Katz*, the Justices clearly intended to bring constitutional protection to telephone conversations, but the reasoning did not provide clear guidance for future cases. *Katz* established a constitutional floor under electronic surveillance practices, but that floor rested on a shaky foundation.

In *Katz*, the Court had to draw a line between those things a person says that are private under the Constitution and those statements that lack constitutional protection. The Court properly ruled out the "constitutionally pro-

---

175. *See, e.g.*, Dempsey, *supra* note 159, at 76-78.

176. *See, e.g.*, United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting); Katz v. United States, 389 U.S. 347, 364 (1967) (Black, J. dissenting); Berger v. New York, 388 U.S. 41, 71 (1967) (Black, J., dissenting); Osborn v. United States, 385 U.S. 323, 340-54 (1966) (Douglas, J., dissenting); On Lee v. United States, 343 U.S. 747, 762-65 (1952) (Douglas, J., dissenting).

177. 389 U.S. 347.

178. *See id.* at 360-62 (Harlan, J., concurring).

179. *See* 388 U.S. 41, 104-06 (Harlan, J., dissenting) (stating that "what the Court is doing is very wrong," and viewing the New York statute as likely in compliance with the federal constitution); *id.* at 68 (Stewart, J., concurring in result) (agreeing with Justices Black, Harlan, and White that the New York law is entirely constitutional).

180. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 303 (1966) (Stewart, J.) (denying protection to a defendant who trusted a government informant and forming the basis for later restrictions on communications privacy); Desist v. United States, 394 U.S. 244, 254 (1969) (Stewart, J.) (finding *Katz* to have prospective application only). Justice Harlan dissented and maintained that *Katz* should be applied retroactively. *See id.* at 256. But Harlan authored the *Lopez* decision, finding no constitutional search because the defendant assumed the risk that the person to whom he was speaking carried a hidden recording device. *See* Lopez v. United States, 373 U.S. 427 (1963).

tected area" test, which afforded a bright line, but an irrational one.[181] The Court could have distinguished between conversations heard by the naked ear, and those heard only with the aid of electronic surveillance. Thus any conversation a police officer could hear unaided would not be private, but those that required a wiretap or a bug would be constitutionally protected.[182] That approach would analogize information perceivable without surveillance to objects observable in plain view, and use a basic fairness argument to withhold protection: the police should not have to shield their senses from those things perceptible by others. At the same time, it would credit the view of those Justices who saw electronic surveillance as a "dirty business" which—if used at all—should be subject to Fourth Amendment protections.[183]

Unfortunately, the Supreme Court precluded the "presence of electronic surveillance" test in a line of cases beginning with *Goldman v. United States*[184] in 1942. Relying on *Olmstead v. United States*,[185] the Court found no constitutional significance in the fact that agents could hear the defendant's conversations only because they used a sensitive "detectaphone."[186] Ten years later in *On Lee v. United States*, a divided Court found no constitutional search when a government informant used electronic surveillance to transmit his conversations with the defendant to a Narcotics Bureau agent.[187] The majority saw no meaningful difference between the government agent listening to the conversation using an electronic receiver and hearing the conversation with his own ears.[188] Finally, a few years before *Katz*, in *Lopez v. United States*, a divided Court found no difference between an unaided undercover agent and one who carried a pocket wire recorder to record the incriminating conversation.[189] In each of these three cases, the Court found the defendant assumed the risk his information would be disclosed through the use of electronic aids.[190]

---

181. *Katz*, 389 U.S. at 351 (rejecting the test); *see supra* note 71 (discussing distinctions that flowed from that test).

182. *See* James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 437-44 (2002) (advocating a similar test).

183. *See, e.g.*, On Lee v. United States, 343 U.S. 747, 758-61 (1952) (Frankfurter, J., dissenting); Olmstead v. United States, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting).

184. Goldman v. United States, 316 U.S. 129, 135 (1942).

185. 277 U.S. at 438.

186. *See Goldman*, 316 U.S. at 135.

187. 343 U.S. 747, 747 (1952). Justice Burton recommended a hybrid version when he suggested protecting words that are picked up without warrant or consent in a constitutionally protected area and considered the defendant's words so obtained because the transmitter permitted the government agent to be present in the room without authorization. *See id.* at 766-67 (Burton, J., dissenting) (advocating the use of a "clearly ascertainable line").

188. *See id.* at 753-54.

189. *See* 373 U.S. 427, 439 (1963).

190. *See Lopez*, 373 U.S. at 439 (finding that the defendant took the risk that his statements would be recorded and admitted into evidence); *On Lee*, 343 U.S. at 753-54 (noting that the defendant "was talking confidently and indiscreetly with one he trusted, and he was overheard"); *Goldman*, 316 U.S. at 135 (rejecting the claim that "it is not to be assumed [that the defendant] takes the risk of someone's use of a delicate detector in the next room"); *see also* Hoffa v. United States, 385 U.S. 293, 303 (1966) (relying on the assumption of risk analysis from *Lopez*). *But see* United States v. White, 401 U.S. 745, 789-90

The *Katz* court could have rejected this line of cases and established the presence-of-surveillance standard as a substitute for the constitutionally-protected-area test.[191] However, it would have been awkward for Justice Harlan to do so since he wrote the majority opinion in *Goldman*.[192] Had the Court done this, there is little doubt that subsequent communications privacy cases would have been easier to decide and more protective of privacy. Any time law enforcement officers used electronic surveillance they would have to satisfy the Fourth Amendment requirements, whether they worked undercover or not. Though much can be said in favor of this approach, later cases made clear that the *Katz* court did not adopt it.[193]

Nonetheless, in *Katz*, Justice Stewart clearly recognized the need to distinguish private from unprotected statements. He wrote that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[194] On the other hand, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[195] By considering what the target seeks to preserve as private the Court recommended a subjective standard that focuses on the target's intent. At the same time, by rejecting claims for constitutional protection of information that is "knowingly exposed," the Court included an objective limit.[196] The Court recognized that clearly irrational claims to privacy, such as the claim that something yelled in a crowd is private, should be denied protection.[197]

But what about the considerable middle ground in which most claims present themselves? For example, Justice Stewart's test does little to address the informant wired for sound. If a target says something to a small group of people whom the target believes can be trusted, but one of those people turns out to be a government informant who transmits the information to others, the target has sought to preserve the information as private and cannot be said to have "knowingly expose[d] [it] to the public."[198] Yet the as-

---

(1971) (Harlan, J., dissenting) (advocating that *On Lee* be overruled because ordinary citizens should not have to bear the risk of unknown eavesdroppers in the absence of probable cause).

191. *See, e.g., White*, 401 U.S. at 755 (Brennan, J., concurring) (reaffirming his view that use of any electronic surveillance implicates the Fourth Amendment); *Lopez*, 343 U.S. at 450-53, 465-66 (Brennan, J., dissenting) (arguing that privacy requires that society not be considered to assume the risk of surreptitious electronic surveillance). Justice Douglas appeared to agree that only a presence-of-surveillance test would adequately protect society from becoming a police state. *See White*, 401 U.S. at 758-59 (Douglas, J., dissenting) (asserting the need for judicial supervision under the Fourth Amendment whenever electronic surveillance is used).

192. *See infra* note 206 (discussing Justice Harlan's attempt to draw a line between *Goldman* and *On Lee*).

193. Any doubt was removed by *White*, in which the majority (including Justice Stewart) refused to find a constitutional difference between "the electronically equipped and the unequipped agent." *White*, 401 U.S. at 752-53. The Court found that *Katz* overruled neither *On Lee* nor *Lopez* and affirmed the assumption of risk approach. *See id.* at 745, 749-52.

194. Katz v. United States, 389 U.S. 347, 351 (1967).

195. *Id.* at 351-52.

196. *See id.* at 351 (pointing out that Fourth Amendment protection is not invoked when one knowingly exposes information to the public).

197. *Id.* at 361 (Harlan, J., concurring).

198. *Id.* at 351; *see, e.g.*, United States v. White, 401 U.S. 745, 751-52 (1971) (conceding that indi-

sumption of the risk cases suggest that such information is not protected. Justice Stewart's test does not differentiate between these cases.

Justice Harlan's concurrence improves somewhat on Justice Stewart's test. The reasonable expectation of privacy test protects those things that the speaker subjectively views as private, when that subjective view is objectively reasonable. By concluding that it is not objectively reasonable for a target to view as private statements made to a government informant who is wired for sound, a court can use the reasonable expectation of privacy test to chart a course that protects the Katz's of the world, but not those who place mistaken trust in informants.

In order to protect Katz—who spoke his intercepted comments in a telephone booth—the Court had to find that it is *reasonable* for citizens to believe that statements uttered into a telephone are private.[199] The Court rejected the notion that telephone speakers assume the risk that their calls may be intercepted, even though those who speak to wired informants assume the risk that their statements may be recorded or transmitted. The Court reasoned that denying protection in *Katz* would "ignore the vital role that the public telephone has come to play in private communication."[200]

Although it is not altogether clear where the Court drew the line between protected and unprotected communications, it is clear that it did not treat the "fact of interceptibility" as the dividing line.[201] If it had, the Court would have reasoned that, because telephone calls may be intercepted, such interceptions do not implicate the Fourth Amendment.[202] This approach would have signified the death knell of communications' privacy. Even if it were limited to cases in which the participants knew of the possibility of interception, it would mean that telephone conversations would never be protected, because it was widely known at the time of *Katz* that telephone conversations could be intercepted.[203] While destructive of privacy, the fact-of-interceptibility approach would have provided a bright line; communica-

---

viduals generally do not know or suspect that their colleagues are carrying recorders or transmitters).

199. *See id.* at 352, 361.

200. *Id.* at 352.

201. I use the fact-of-interceptibility test as a special communications version of the principle that once information is disclosed to third parties, it is no longer private. *See, e.g., Antiterrorism Investigations and the Fourth Amendment After September 11, 2001: Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 108th Cong., 1st Sess. 12 (2003) [hereinafter *Antiterrorism Hearings*] (statement of Viet D. Dinh, Assistant Att'y Gen. for the Office of Legal Policy, Dep't of Justice) (arguing that *Smith* was based on this principle). The rule is subject to much criticism in all contexts, but it seems particularly faulty in the communications' context since making one's information interceptible is typically unavoidable.

202. In fact, the Court viewed the *Olmstead* case as relying on just that logic. *See* Goldman v. United States, 316 U.S. 129, 135 (1942) (describing *Olmstead's* reasoning: "[I]n using a telephone, the speaker projects his voice beyond the confines of his home or office and, therefore, assumes the risk that his message may be intercepted.").

203. *See, e.g.*, CEDERBAUMS, *supra* note 12, at 21-22 (discussing the practice at the time of *Katz*); AMERICAN BAR ASSOCIATION PROJECT ON MINIMUM STANDARDS FOR CRIMINAL JUSTICE, STANDARDS RELATING TO ELECTRONIC SURVEILLANCE APPENDIX E (Tentative Draft, 1968) [hereinafter 1968 ABA STANDARDS] (citing 60 general periodicals and 150 law review articles on electronic surveillance in the ten years prior to *Katz*).

tions either may or may not be interceptible, as a matter of fact. It would also have been more consistent with the assumption of risk cases.

Fortunately for privacy, the Court rejected the fact-of-interceptibility approach in *Katz*,[204] but settled for a fairly ambiguous test. As many have noted, the reasonable expectation of privacy test is circular.[205] It protects the privacy of those communications which it is reasonable to regard as private. Rather than using a bright-line test that considers the presence of surveillance or the fact that communications may be intercepted, the Court established that communications privacy depends on what a court views as reasonable. Notably, Justice Harlan later argued that it is not reasonable to view people as having assumed the risk that electronic surveillance will permit third parties to hear their conversations as they are spoken, but that view did not prevail.[206]

Whether or not *Katz* used the proper approach to communications privacy—and I think the presence-of-surveillance test would have been a better choice—the decision left courts in an awkward position. It required a normative judgment every time a court faced the inevitable questions that would arise about communications privacy.[207] Were all aspects of the telephone network vital? What about successors to the telephone network? What about other attributes of telephone calls besides their content?

In 1979, the Court had to confront the last of these questions when it considered whether the numbers dialed on a phone were protected under the Fourth Amendment.[208] At the time, dialed number registers recorded the telephone numbers of the target's outgoing calls on paper tape as they were dialed.[209] The most popular of such devices used pens to record the numbers and so were dubbed "pen registers."[210] The Wiretap Act did not cover pen registers because of their extremely limited output; they did not reveal any

---

204. *See Katz*, 389 U.S. at 352 ("One who occupies [a phone booth] . . . is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

205. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383-86 (1974).

206. *See* United States v. White, 401 U.S. 745, 776-77, 785 (1971) (Harlan, J., dissenting). Justice Harlan would permit the simultaneous *recording* of a conversation by a participant, which could later be played to third parties who would not otherwise be able to "hear" the conversation, but not simultaneous *transmission* of the recording to the third parties. *Id.*; *see also id.* at 787-88 (distinguishing between third-party bugging and single-party informer bugging). By permitting third parties to hear a conversation they could not otherwise hear through electronic surveillance, his test is not a presence-of-surveillance test. It also fails to create a bright line. For example, how much of a delay in receiving the information suffices to remove constitutional protection? *See id.* at 788 n.24 (attempting to distinguish the cases on the grounds that the informer who records rather than transmits may decide not to turn over the recording and recognizing that future distinctions based on the relationship between the investigator and suspect may arise).

207. Justice Harlan recognized this need: "The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement." *White*, 401 U.S. at 786 (Harlan, J., concurring); *see also* Amsterdam, *supra* note 205, at 403 ("The ultimate question, plainly, is a value judgment.").

208. Smith v. Maryland, 442 U.S. 735, 741-46 (1979).

209. *Id.* at 736 n.1 (defining "pen register").

210. *See* DASH, *supra* note 1, at 269, 323-25 (describing how a pen register operates).

information considered to be content, such as the identities of the parties or even the existence of the call, since they did not indicate if the call had succeeded.[211] Nonetheless, courts had generally held that pen register investigations required a warrant under the Fourth Amendment.[212]

In *Smith v. Maryland*,[213] the Court employed the fact-of-interceptibility test that *Katz* had rejected to deny Fourth Amendment protection of pen registers.[214] Because the phone company tracked the numbers people dialed to bill for calls, and because people knew that the phone company had that ability, the Court found it unreasonable to expect such information to be private.[215] The *Smith* court ignored the lesson of *Katz*: We do not lose privacy in communications merely because they may be intercepted. In denying Fourth Amendment protection to phone numbers, the Court also failed to make explicit any normative judgments. The majority did not reason that telephone numbers do not require privacy, that the numbers dialed are somehow less essential than phone calls, or that law enforcement interests trump the privacy interest in telephone numbers.[216] The dissenting justices in *Smith* (including Justice Stewart) argued that the Court should engage in that inquiry and that if it did, it would reach the opposite result.[217]

The problem with the reasonable expectation of privacy test is not that it tries to separate private from nonprivate information—that has to be done. The problem is that it invites courts to make a normative judgment that they seem to be uncomfortable making. In *Smith*, the Court substituted the fact-of-interceptibility test for a difficult normative judgment, likely because it was more comfortable with the former's objective approach. Unfortunately, the fact-of-interceptibility test not only contradicts *Katz*, it provides insufficient privacy protection to our communications systems. The cases that have followed *Smith* and applied the fact-of-interceptibility test to determine the privacy of modern communications have made that loss of privacy evident.[218]

---

211. *See* United States v. Dote, 371 F.2d 176 (7th Cir. 1966) (describing pen registers' operation), *cited in* S. REP. NO. 90-1097, at 88 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2178.

212. *See, e.g.*, United States v. King, 335 F. Supp. 523, 549 (S.D. Cal. 1971).

213. 442 U.S. 735 (1979).

214. *See* Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 564 (1990) (calling this the "disclosure principle" based on assumption of risk); Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1757-58, 1794-95 (1994) (criticizing the fact-based inquiry of *Smith* and like cases).

215. *Smith*, 442 U.S. at 742-44, 745 ("[P]etitioner voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record.").

216. As Justice Marshall pointed out, the majority recognized that in some cases a normative inquiry would be appropriate, see *Smith*, 442 U.S. at 740-41 n.5, but did not recognize that a normative inquiry is essential for all privacy inquiries. *See id.* at 749-52 (Marshall, J., dissenting). For an excellent critique of the reasoning in *Smith*, see Patricia L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375 (2004).

217. *See Smith*, 442 U.S. at 746-48 (Stewart, J., dissenting) (identifying the question as whether a telephone user is "entitled" to assume the numbers he dials are private).

218. *See infra* Part III.D.4 for a discussion of modern cases.

Congress failed to clarify this situation in the Wiretap Act. In establishing that telephone conversations were protected against interception no matter what, it obviated the need for the test in the wiretapping context. But the Wiretap Act incorporated the reasonable expectation of privacy test in the context of eavesdropping.[219] As for the online context, Congress has failed to make explicit its judgments about what should be private. The result, as we shall see, is the significant underprotection of modern communications.

E. Amendments to the Wiretap Act

In 1986, following *Smith*, Congress revised the definition of communications contents in the Wiretap Act to exclude information disclosing the "existence" of the call or the "identities" of the parties to it.[220] At the same time, Congress added a set of regulations designed to regulate pen registers. Those regulations were part of a comprehensive effort to update the Wiretap Act to handle new electronic communications. In the Electronic Communication Privacy Act ("ECPA"), Congress extended some of the wiretapping protections to electronic communications.[221] It bears clarifying that when Congress passed the ECPA in 1986, electronic communications were in their infancy. The World Wide Web would not be developed for several years, the text-based Internet was used mostly by academics, and a relatively small number of people used electronic mail.[222] To encourage further development of electronic communications, Congress added "electronic communication" to most occurrences of "wire" and "oral" communications in the Wiretap Act. The extension of protection was not complete, however. Most importantly, Congress declined to extend the statutory exclusionary

---

219. *See* 18 U.S.C. § 2510(2) (2000) (defining "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation"). The Eleventh Circuit has interpreted this provision to require that the speaker have "a reasonable expectation that [his] conversations will not be intercepted by a device." Walker v. Darby, 911 F.2d 1573, 1579 (11th Cir. 1990) (applying a reasonable expectation of noninterception test); *see also* Karen A. Springer, *In God We Trust; All Others Who Enter This Store Are Subject to Surveillance*, 48 FED. COMM. L.J. 187 (1995) (arguing that the reasonable expectation of noninterception is easier to establish than the reasonable expectation of privacy). Interestingly, the noninterception test seems akin to a presence-of-surveillance test. *See Walker*, 911 F.2d at 1579 ("But while Walker might have expected conversations uttered in a normal tone of voice to be overheard by those standing nearby, it is highly unlikely that he would have expected his conversations to be electronically intercepted and monitored in an office in another part of the building."). A subsequent court, however, claimed that it was not using a "capable of being intercepted" test, but instead considered whether the comments were "readily or practicably capable of being intercepted." *See* Wesley v. Hearst Corp., 806 F. Supp. 812, 815 (E.D. Wis. 1992) (precluding recovery when the "person should know . . . that the person's comments could be artificially detected without too much trouble").

220. *See* 18 U.S.C. § 2510(8) (defining "contents").

221. *See* H.R. REP. NO. 99-647, at 77 (1986); S. REP. NO. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3568. The ECPA established that states may pass laws that are "at least as restrictive" as the ECPA. *See id.* at 35. The ECPA is the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

222. *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003) (finding the ECPA "ill-suited to address modern forms of communication" because it "was written prior to the advent of the Internet and the World Wide Web") (quoting Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002)); *In re* Pharmatrak, Inc., 329 F.3d 9, 21 (1st Cir. 2003) (expressing the same concern).

rule to electronic communications.[223] Further, Congress divided the treatment of electronic communications into several categories based on what information was acquired and when it was acquired. Overall, the new privacy protections for electronic communications were both considerably weaker and significantly more complex than the protections in the original Wiretap Act. In fact, the two are related; the ECPA's complexity has weakened its ability to protect privacy.

Congress has significantly revised the ECPA and the Wiretap Act only twice since 1986. In 1994, the Communications Assistance for Law Enforcement Act ("CALEA") obliged communications service providers to ensure law enforcement's continued ability to wiretap newly evolving digital networks.[224] In 2001, the USA PATRIOT Act provided some new tools to law enforcement agents.[225] The amendments made minor changes to the standards and structure of the ECPA and the changes did not significantly impact communications privacy.[226]

III. ONLINE SURVEILLANCE

A. Background

1. The Appeal and Threat of Online Surveillance

Though analogous, electronic surveillance of the Internet, or online surveillance, appeals more to law enforcement and poses a greater threat to privacy than traditional wiretapping.[227] From the law enforcement perspective, online surveillance is safer, cheaper, and more powerful than traditional wiretapping.[228] The electronic medium affords more opportunities to acquire information than the telephone network. Law enforcement may choose several different places along the electronic network to obtain target data, including the internet provider's server. By contrast, prior to the Wiretap Act, live agents often had to install a traditional wiretap or set up a lis-

223. *See infra* notes 359-61 and accompanying text. Note that the statutory exclusionary rule in the Wiretap Act provides more protection than the constitutional exclusionary rule. *See* United States v. Koyomejian, 946 F.2d 1450, 1455 n.10 (9th Cir. 1992); SAMUEL DASH, THE INTRUDERS: UNREASONABLE SEARCHES AND SEIZURES FROM KING JOHN TO JOHN ASHCROFT 105-31 (2004) (describing the substantial erosion of the exclusionary rule under the Burger Court).

224. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001-10 (2000) and in scattered sections of 18 U.S.C.). *See generally* Susan Freiwald, *Uncertain Privacy: Communications Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996) (discussing the history and provisions of CALEA).

225. *See supra* note 26 and accompanying text; *see also infra* Part III.E.1 (discussing the impact of the USA PATRIOT Act).

226. In the following discussion, I will refer to the Wiretap Act when discussing wire communications (which include a human voice) and the ECPA when discussing electronic communications. Where significant, I will point out amendments to the ECPA either in the text or notes.

227. I use the term "online surveillance" intuitively in this section, but I will refine it in Part V.

228. *See* DIFFIE & LANDAU, *supra* note 7, at 116, 152-53 (comparing modern wiretapping techniques to traditional ones).

tening post in the physical vicinity of the target's phone.[229] If they wanted to conduct visual surveillance, which was common, they had no choice but to remain nearby.[230] Online surveillance, has largely, if not entirely, avoided the need to go to the target's premises. Recently developed software tools permit law enforcement agents to access target computers remotely by infecting the target's computer with a computer virus that sends information to the agents over the electronic networks.[231]

Online surveillance costs less and accomplishes more than traditional wiretapping. Technology grows cheaper and more powerful every year, so one can only imagine how much it has progressed in the thirty-five years since the Wiretap Act's passage. Large quantities of data may be gathered at minimal cost, either as it is produced or at some time later. Once law enforcement agencies develop the computerized systems they need to conduct online surveillance, software applications may be duplicated at a fraction of the cost. Agencies can use one of several private software packages that conduct surreptitious online listening.[232] Additional savings derive from the elimination of contemporaneous listening. With traditional wiretapping, the preferred practice was to have live agents listen to conversations as they were generated. This minimized the interception of non-incriminating conversations because agents stopped the tape at appropriate times.[233] In contrast, the consensus seems to be that after-the-fact filtering suffices when one must minimize electronic communications, so there is no need to have an agent monitor in real time.[234]

Traditional wiretapping perceives more than the human senses, and remembers forever by creating a detailed permanent record. Online surveillance does the same, but also perceives information people send over the Internet. Law enforcement can obtain large documents, pictures, sound files, or videos sent by a target. As phone calls increasingly travel the Internet, online surveillance captures those as well. Monitors usually identify the sender of information online, whether by e-mail address, IP address, or even a digital signature, whereas traditional wiretap investigators often encountered difficulties putting a name to a voice. Encrypted electronic data may make online information harder to use, but law enforcement currently pos-

---

229. *Id.* at 153.

230. Hidden video cameras were not viable. *See* United States v. Torres, 751 F.2d 875, 880-81 (7th Cir. 1984) (1985) ("The legislative history [of the Wiretap Act] does not refer to it, probably because television cameras in 1968 were too bulky and noisy to be installed and operated surreptitiously").

231. *See* Neal Hartzog, *The "Magic Lantern" Revealed: A Report on the FBI's New "Key Logging" Trojan and Analysis of its Possible Treatment in a Dynamic Legal Landscape*, 20 J. MARSHALL J. COMPUTER & INFO. L. 287 (2002).

232. *See* PRESTON GRALLA, HOW THE INTERNET WORKS 316-19 (7th ed. 2004) (describing use by government monitors of commercial monitoring tools); *see also* John Schwartz, *AOL to Add Spyware Detection to Service*, N.Y. TIMES, Jan. 6, 2004 at C7 (describing feature that will remove "hidden tools that can monitor Web surfers' online habits for marketing purposes").

233. *See* LAPIDUS, *supra* note 3, at 127-28.

234. *See, e.g.*, S. REP. NO. 99-541, at 31 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3585; Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994). *But see infra* note 491 (discussing problems with after-the-fact filtering).

sesses powerful techniques to decode encryption.[235] Also, encryption has not yet become popular.[236] When and if it does, law enforcement representatives will likely renew their efforts to gain access to deciphered text.[237]

It would be surprising if online surveillance were less effective than traditional wiretapping, because the former offers cheaper, richer, and more reliable information with less risk. Although the very quantity of information online may make it almost unusable, to the extent that law enforcement agents focus their efforts on a particular person who spends time online, online surveillance will surely be more effective than traditional wiretapping. At the end of the day, law enforcement's interest in using online surveillance must surely surpass its interest in traditional wiretaps.

Even if online surveillance posed the same threat to privacy as traditional wiretapping, its increased appeal to law enforcement agents would increase that threat. Historically, law enforcement has responded to the lure of traditional wiretapping by engaging in unauthorized surveillance. The increased appeal of online surveillance means that we must be alert for even more unauthorized online surveillance.

In addition, those factors that make online surveillance more privacy-intrusive than traditional wiretapping add to its appeal as a tool for law enforcement. One may learn much more about a typical American by looking at her online activities than merely by listening to her telephone conversations. Anyone who spends time online creates a rich and detailed personal digital dossier.[238] At the same time, much of the information about us online is "private" in the sense that we intend for only a limited number of people to see it. The question remains: How much does the law protect our online privacy?

B. Complexity Becomes Chaos on the Internet

1. The Practices and Stages of Online Surveillance

Recall that the overlap between the two traditional forms of electronic surveillance, wiretapping and bugging, made regulation complicated. For online surveillance, the problems multiply. Though the current nature and extent of online surveillance remains unknown, we do know there are significantly more than two practices. Electronic communications may be acquired as they travel across the communications network or after they have come to rest. Agents may track online movements on the World Wide Web, either in real time or by obtaining electronic logs. A few years ago, the FBI

235. *See generally* DIFFIE & LANDAU, *supra* note 7; David J. Phillips, *Cryptography, Secrets and the Structuring of Trust*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, *supra* note 28, at 243.

236. *See supra* note 7.

237. For an overview and analysis of past efforts, see A. Michael Froomkin, *The Metaphor is Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

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

announced a filtering program, dubbed "Carnivore," that grabs Internet traffic as it passes over a server.[239] Details about how the system works remain sketchy.[240] Similarly, the FBI has used a key logger system to record a defendant's keystrokes and obtain his encryption passcode, but has classified information about the system's functionality.[241] Also, details remain elusive about the government's capacity to use computer viruses to install secret monitoring systems from remote locations.[242] Even the most up-to-date and comprehensive statute would have a hard time contending with all these practices.

Unfortunately, the ECPA is neither up-to-date nor comprehensive. Several of its important definitions have not been revised since 1986. Its provisions fail to mention the World Wide Web or the Internet, even after recent amendments.[243] It is so confusing and intricate that it is nearly impossible to determine which provisions apply to which practices, and the Department of Justice, both the enforcer and subject of the Act, has not clarified matters. Instead, the government has argued, with some success, that several of the new online surveillance practices are either immune from regulation or that their regulation depends critically on how the agents choose to configure them.[244]

To obtain some appreciation for the complexity of online surveillance law, consider the stages of online surveillance. Just as traditional telephone calls could be intercepted, disclosed, used for leads, and brought into court, the same may be done with electronic communications. But in 1968, unless recorded by the wiretapper, telephone calls existed only while their participants conversed.[245] Electronic mail, by contrast, exists in several discrete stages in several different physical locations.

An e-mail comes into being when its author composes it on her own computer. She may send it immediately or she may send it later. To be sent, the e-mail is broken up into packets that travel over the electronic network, but those packets may be reconstituted at several intermediate points along

---

239. *See The "Carnivore" Controversy: Electronic Surveillance and Privacy in a Digital Age: Hearing Before the Senate Comm. On the Judiciary,* 106th Cong., 1st Sess. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation); E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions,* 6 VA. J.L. & TECH. 10 (2001).

240. *The Fourth Amendment and Carnivore: Hearing Before the Subcomm. on the Constitution of the House Judiciary Comm.*, 106th Cong., 1st Sess. (2000) (statement of Barry Steinhardt, Associate Director of the ACLU) (describing Carnivore as "a black box into which flows all of a service providers communications traffic. The service provider knows what goes in, but it has no way of knowing what the FBI takes out.").

241. *See* United States v. Scarfo, 180 F. Supp. 2d 572, 576-77 (D.N.J. 2001); *see also id.* (affidavit of Randall S. Murch) (Oct. 4th, 2001) (describing the functionality of KLS in general terms).

242. *See* Hartzog, *supra* note 231.

243. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

244. *See infra* Part III.D-E.

245. *See* H.R. REP. NO. 99-647, at 17 (1986) (noting that when the Wiretap Act was passed, "the contents of a traditional telephone call disappeared once the words transmitted were spoken and there were no records kept").

the way to the recipient.[246] The e-mail makes a temporary stop when it arrives at the recipient's computer server. Once there, the e-mail waits until the recipient downloads it to his local computer. It may take a while before the recipient actually reads the email. Long periods of time may pass before the recipient deletes the email. After deletion, the e-mail may rest in a temporary file on the recipient's computer. Even after that file is deleted, the message may be recoverable from a backup file or from the computer's memory.

The content and character of the e-mail does not change as it travels through these various stages.[247] Nonetheless, prosecutors have seized upon this complexity to argue that the law varies dramatically depending on the point at which they obtain the electronic information. Some of those arguments seem to be invited by ECPA's text and structure; others seem quite aggressive. In the next subpart, I describe how the ECPA segregates its protections. I address law enforcement's interpretations in Part III.D.1.

2. *Communications, Communication Attributes, and Web Browsing*

In this discussion, I use the ECPA's legal categories, though I give them my own descriptive terms. In the next sections, I critique the current legal framework and raise questions about the categories themselves, not the least of which is that they are too confusing. For now, I provide a brief description of the relevant terms.

I will use the term "dynamic content interceptions" to refer to investigations that acquire the contents of electronic communications in real-time. "Dynamic" describes the process by which information is acquired; a dynamic interception grabs communications as they are in transit across the electronic networks. What "contents" includes is somewhat uncertain, which I will discuss. As distinct from content interceptions, I will use the term "dynamic attribute acquisitions" to refer to the real-time acquisition of all of the information available about an electronic communication, other than its contents.[248] I use the term "communication attributes" to refer to non-content information associated with a communication.[249]

The communication attributes of a traditional telephone call include the telephone number dialed and the telephone number of the party who dialed the call. In addition, they include whether or not the call succeeded, its duration, and its physical location. In the electronic context, communication attributes include electronic addressing information, the size of the communication, and its duration. Other information, such as attachments and sub-

246. *See* GRALLA, *supra* note 232, at 92-95.

247. *See infra* Part V.

248. I use the term "acquisitions" for all but dynamic content interceptions. As I will discuss, "interception" is a term of art under the ECPA.

249. *See* Freiwald, *supra* note 224, at 953-60 (defining and describing communication attributes). Some use the term "transactional data" for communication attributes, but that term may confuse different types of information.

ject lines, seem to be content, but the line between communications contents and attributes is blurry.[250] I will also refer to dynamic attribute acquisitions as "pen register investigations," because pen registers traditionally acquired such communication attributes as the telephone numbers dialed, and because that is the convention.[251]

In addition to distinguishing between contents and attributes, the ECPA distinguishes between electronic information acquired in real-time, as discussed, and information acquired out of electronic storage. What counts as "electronic storage" has been disputed in various cases, but generally a communication may be acquired from electronic storage after it has come to rest and is no longer "in transmission."[252] I will refer to the acquisition of the contents of communications in storage as "stored content acquisitions" and the acquisition of communication attributes in storage as "stored attribute acquisitions." I will use a fifth category, "web traffic data," to cover information about online activities that does not seem to fit into the other categories. The following discussion briefly describes the ECPA's protection for each category.

a. Dynamic Content Interceptions

The ECPA adapted traditional wiretapping regulations to the online context by adding the term "electronic communications" to almost every occurrence in the text of the Wiretap Act of "wire communications" and "oral communications." The statute defines "electronic communications" broadly, but it drafted the definition with electronic mail as it existed in 1986 in mind.[253]

Those techniques of online surveillance that "intercept" the content of electronic communications receive almost the same treatment as wiretaps and electronic bugs. The most significant difference is the absence of a statutory exclusionary rule for electronic communications.[254] Agents who conduct dynamic content interceptions must generally satisfy all of the requirements that pertain to traditional surveillance, including the need to

---

250. *See id.* at 956-57; *see also* Part III.E (discussing this ambiguity).

251. I use the term "investigations" for pen registers rather than "acquisitions" because pen registers refer to the investigative tool rather than the data acquired.

252. *See* H.R. REP. NO. 99-647, at 65. As did the House Judiciary Committee in 2000, I view electronic storage as encompassing electronic communications after they have been read, so long as they are retained by the electronic service provider or by another third party. *See infra* note 327. I find unpersuasive and counter-intuitive the interpretation that holds that an e-mail cannot be stored on an electronic service provider after it has been read. *See infra* notes 322-23 and accompanying text.

253. *See id.* at 34; 18 U.S.C. § 2510(12) (2000) (defining electronic communications as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system," but excluding wire and oral communications).

254. *See* 18 U.S.C. § 2518(10)(a), (c) (2000); *see also infra* note 361 and accompanying text (discussing remedies). In addition, the list of government officials who could request surveillance of electronic communications and the list of predicate offenses were both broader than for traditional wiretapping and bugging. *See* H.R. REP. NO. 99-647, at 51.

obtain a "super-warrant" court order. They must establish a high level of probable cause, demonstrate that surveillance is essentially a last resort, minimize the acquisition of innocent communications, and provide progress reports to the judge who grants the application.[255] In short, the ECPA vigorously protects the privacy of electronic communications from unauthorized dynamic interceptions.

The ECPA strictly limits what information qualifies for this high level of wiretap-like protection in two ways. First, the dynamic content interception provisions apply only when a law enforcement agent *intercepts* the information while it is in transmission. The protections for communications acquired out of storage are significantly less protective, as I will discuss. Second, the wiretap-like protections apply only to interceptions of the *contents* of electronic communications.[256] In the context of traditional wiretapping, there is not much besides the contents of communications to be acquired.[257] But in the online context, communication attributes convey rich information. As the next subpart discusses, the dividing line between contents and attributes assumes critical importance because the protection for communication attributes is much weaker than for contents.

b. Dynamic Attribute Acquisitions (Pen Register Investigations)

Dynamic attribute acquisitions receive the lowest level of protection under the ECPA. Although the tools used may be quite similar, the legal treatment of dynamic attribute acquisitions could not differ more from the treatment of dynamic content interceptions.[258] Government agents must obtain a court order to collect attributes dynamically, but courts have interpreted the provision to mandate rubber stamp approvals with no meaningful review of applications.[259] Unlike with wiretaps, law enforcement agents have no responsibility to acquire attributes dynamically as a last resort, to minimize the acquisition of innocent information, or even to establish probable cause. No remedies exist for victims of dynamic attribute interceptions.[260] To the extent that the provisions give rights at all, they do not seem to be enforceable.

---

255. *See* 18 U.S.C. §§ 2511, 2516, 2518 (2000 & Supp. I 2001).

256. "Intercept" is defined as the "acquisition of the contents" of communications. *Id.* § 2510(4). The original Wiretap Act had the same definition, but it applied a broader definition of content. *See supra* note 76 and accompanying text.

257. *See, e.g.*, Berger v. United States, 388 U.S. 41, 99-100 (1967) (Harlan, J., dissenting) (noting that the court order permitted the interception of "conversations"); Goldman v. United States, 316 U.S. 129, 133-34 (1942) (recognizing that the "message itself" is protected as it travels over phone lines).

258. *See infra* note 347 (suggesting that law enforcement agents use the same tools for both); *see also In re* United States, 10 F.3d 931, 936 (2d Cir. 1993) ("There is a sharp contrast between the stringent controls over wiretap orders (including the severity of punishment enforcing them) and the much less onerous conditions for obtaining pen register and trap and trace authorization.").

259. *See infra* note 358 and accompanying text.

260. The possibility of a fine and a one-year prison sentence exists for offenders, but there are no published prosecutions. *See* 18 U.S.C. § 3121(d) (2000).

The ECPA regulates dynamic attribute acquisitions under a section devoted to pen registers.[261] In contrast to the other provisions, which focus on the type of information acquired, the pen register provisions pertain to a particular investigative tool, the pen register—creating significant uncertainty. Notably, it was unclear whether the pen register provisions regulated the acquisition of electronic addressing information when the statutory language did not so provide.[262] In fact, when Congress drafted the ECPA, it clearly understood that pen registers obtained merely the telephone numbers dialed on the target's traditional telephone.[263] Although the USA PATRIOT Act clarified that pen registers could gather "dialing, routing, addressing, or signaling information" of "electronic communication[s]," much remained unclear.[264]

c. *Stored Content Acquisitions*

By 1986, emerging technologies permitted the digital storage of communications, presenting new opportunities for privacy deprivations.[265] Congress accorded stored voice mail recordings the same protections against interception that they would enjoy if they were intercepted during transmission. Congress accomplished this by extending the ECPA's definition of a wire communication to include such communications in "electronic storage."[266] If Congress had similarly defined electronic communications to include such communications in storage—so that interceptions of both would be subject to the wiretap-like protections—it would have created a much simpler and more privacy-protective statute.

Instead, the ECPA protects electronic communications in storage according to a complicated scheme.[267] It defines "electronic storage" as "(A) any temporary, intermediate storage of a[n] . . . electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[268] This definition has not been updated since 1986, but it appears that Congress meant storage under part A

261. Pub. L. No. 99-508, § 301, 100 Stat. 1848, 1868-73 (1986) (codified as amended at 18 U.S.C. §§ 3121-27 (2000 & Supp. I 2001)).

262. *See, e.g.*, H.R. No. 106-932, at 13 n.10 (2000) (noting that at that time government investigators used the pen register provisions to obtain e-mail addressing information, and declining to take a position in the debate over whether the statute gave them that authority).

263. *See, e.g.*, S. REP. NO. 99-541, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3564; 18 U.S.C. 3127(3) (Supp. I 2001).

264. 18 U.S.C. § 3127(3); *see infra* Parts III.D.1., III.E.

265. *See* H.R. REP. NO. 99-647, at 18, 22; S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3557.

266. *See* S. REP. NO. 99-541, at 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3566; H.R. REP. NO. 99-647, at 67-68; *infra* note 400 and accompanying text (discussing how the USA PATRIOT ACT removed electronic storage from the definition of wire communications).

267. *See* Stored Wired and Electronic Communications and Transactional Records Access, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701-11 (2000 & Supp. I 2001)).

268. 18 U.S.C. § 2510(17) (2000 & Supp. I 2001).

to include the period of time after an electronic mail message has been delivered to the recipient, but before the recipient has read it. Part B would include electronic mail that has been read and that stays either on the user's system or on a backup of that system.[269]

As it does for dynamic investigations, the ECPA differentiates stored electronic contents from stored electronic attributes. With regard to the former, the provisions are further divided into two categories: stored content obtained within 180 days or less from when it is received ("short-term storage") and stored content obtained thereafter ("long-term storage").[270] According to the legislative history, Congress analogized the short-term storage of electronic contents to a safety-deposit box, but it viewed contents in long-term storage as similar to business records held by third parties.[271] Congress regarded contents in short-term storage as likely protected by the Fourth Amendment, and so it imposed a warrant requirement on their acquisition. [272] Congress did not impose, however, any of the super-warrant requirements of the Wiretap Act on such acquisitions.

Because third party business records had been denied constitutional protection, Congress provided for substantially less protection for contents obtained from long-term storage.[273] Specifically, to obtain electronic communications contents from long-term storage, law enforcement officers may use a subpoena or a court order if they provide notice to the target, or a warrant with no need to provide notice. The court order may issue upon a finding that is much easier to satisfy than probable cause.[274] The next subpart discusses the protections of electronic communication attributes in storage.

d. Stored Attribute Acquisitions

The ECPA permits the government to obtain stored attribute information whenever the government satisfies the court order requirement for long-term storage or obtains a warrant.[275] In addition, the government may acquire a subset of stored attributes, considered to be basic subscriber in-

269. *See* H.R. REP. NO. 99-647, at 63 (e-mail "held in storage until the addressee requests it"); *id.* at 72 (a system may maintain a "backup copy" after the subscriber has read the message and discarded or deleted it). As I will discuss, the Justice Department sees electronic storage as much more limited, a view with which I strongly disagree. *See infra* notes 318-29 and accompanying text.

270. *See* 18 U.S.C. § 2703(a). The Justice Department views these provisions as even more complicated. *See infra* notes 317-22 and accompanying text. The House Judiciary Committee would have extended the period of short-term storage requiring a warrant to one year. *See* H.R. No. 106-932, at 15 (2000).

271. *See* H.R. REP. NO. 99-647, at 23 n.41 (1986).

272. *See id.* at 67-68; ("[T]he general rule [requiring a warrant] applies to electronic communications which have been in electronic storage for 180 days or less."); 18 U.S.C. § 2703(a).

273. The House Report referred to *United States v. Miller*, 425 U.S. 435 (1976), for this reasoning, though it also noted that Congress had overruled *Miller* by statute and thereby protected the privacy of the banking records at issue in *Miller*. *See* H.R. REP. NO. 99-647, at 23, 73 (1986).

274. *See infra* notes 352-53 and accompanying text (discussing the court order and warrant requirements).

275. 18 U.S.C. § 2703(c)(1)(B). *See infra* note 353 and accompanying text; S. REP. NO. 99-541, at 38-39 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3592-93.

formation, by presenting a simple subpoena without ever giving notice to the target.[276] Information about an electronic service provider account receives this low level of protection.[277] The scheme is confusing, because it is not entirely clear what information may be obtained at each of the different levels.[278] The ECPA does not distinguish between attributes in short- and long-term storage.

e. Web Traffic Data

As mentioned, the USA PATRIOT Act amendments clarified that pen registers may be used online to obtain the "to" and "from" information from electronic mails.[279] But they failed to specify what else, if anything, a modern pen register may acquire. Much of the information online does not constitute e-mail addressing information. I use the term "web traffic data" to refer to the information that we generate when we use the World Wide Web.[280] For example, we enter search terms into online search engines, we fill out forms to register for websites or buy products online, and we almost constantly request web pages and information within web pages.[281] While the definition of electronic communication may well be broad enough to encompass all or much of this information, the newly revised definition of pen registers is not.[282] It is hard to see how web traffic data constitutes the "dialing, routing, addressing, or signaling information" of "electronic communication[s]."[283] If it does not, the courts will have to figure out what type of protection to provide. I will return to that issue.[284]

---

276. *Id.* § 2703(c)(2). Government may use a court order or warrant as well. *Id.* § 2703(c)(1). Government agents never need to provide notice when they acquire stored attributes. *See infra* Part III.D.3.

277. The original list included the user's "name, address, . . . telephone toll billing records, telephone number or other subscriber number or identity, . . . length of service[,] . . . and the types of services." 18 U.S.C. § 2703(c)(1)(C). The USA PATRIOT Act added "records of session times and durations"; "instrument number, . . . including any temporarily assigned network address"; and "means and source of payment for such service." *Id.* § 2703(c)(2) (as amended 2001).

278. For example, it is unclear what "records of session times and durations" includes and whether that information must be segregated from system log files.

279. The Justice Department explains that dialing, routing, addressing and signaling information includes "IP addresses and port numbers" as well. Mark Eckenwiler, U.S. DEP'T OF JUSTICE, *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001*, 701 PLI/PAT 1227, 1234 (2002) [hereinafter *DOJ Field Guidance*].

280. Others have referred to this data as "click stream data." *See, e.g.*, Jerry Berman & Dierdre Mulligan, *Privacy in a Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 558 (1999) ("Transactional data, click stream data, or 'mouse-droppings,' can provide a 'profile' of an individual's online life.").

281. *See, e.g.*, *In re* Pharmatrak, Inc., 329 F.3d 9, 13 (1st Cir. 2003) (describing a marketing tool that recorded "the webpages a user viewed at clients' websites; how long the user spent on each webpage; the visitor's path through the site (including her points of entry and exit); the visitor's IP address . . . and . . . the webpage the user viewed immediately before arriving at the client's site"); *see generally* Kang, *supra* note 28.

282. *See, e.g.*, Konop v. Hawaiian Airlines, 302 F.3d 868, 876 (9th Cir. 2002) (finding a website to be an electronic communication), *cert. denied*, 537 U.S. 1193 (2003).

283. 18 U.S.C. § 3127(3) (Supp. I 2001). Paul Taylor, *Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks*, 6 VA. J.L. & TECH. 4, 17-19 (noting that embedded URL's and search terms might be included, even though they convey private information).

284. *See infra* Part III.E.2 (discussing the ambiguous legal status of this information).

Even after recent amendments, the law of online surveillance remains remarkably chaotic.[285] To the extent that the law is clear, however, it offers significantly reduced protection for the privacy of online information.

C. *Online Surveillance Unbounded*

1. *All-purpose Online Surveillance*

Recall that in the compromise that yielded the Wiretap Act, wiretapping was permitted only for serious crimes and those that typified organized crime activities.[286] Congress reached a different compromise when it passed the ECPA. Dynamic content interceptions, the most highly restricted practice, may proceed for the investigation of any federal felony.[287] The ECPA places no restrictions on the crimes that may justify the other types of online surveillance. Stored communication acquisitions and pen register investigations may be used to pursue any "ongoing criminal investigation."[288] The law does not require that law enforcement be investigating a felony, let alone a particularly serious one. It makes little sense to place fewer restrictions on online surveillance than on traditional wiretapping, given the greater threat to privacy it poses.[289]

2. *The Constitutional Requirements Revisited*

In contrast to the Supreme Court's extensive guidance on the constitutional requirements for traditional electronic surveillance, the Court has never addressed the constitutionality of online surveillance. The House Report on the ECPA describes Fourth Amendment protection of e-mail as "speculative" in light of the lack of cases. The Report considers it "likely, however, that the courts would find . . . [some] 'reasonable expectation of privacy'" in e-mail, and require "some kind" of warrant.[290]

The lower federal courts have not squarely addressed the constitutionality of online surveillance either. As of this writing, *United States v. Max-*

---

285. *See Konop*, 302 F.3d at 874 ("We observe that until Congress brings the laws in line with modern technology, protection of the Internet . . . will remain a confusing and uncertain area of the law."); United States v. Councilman, 373 F.3d 197, 203-04 (1st Cir. 2004) ("Moreover, at this juncture, . . . the [privacy] protection may have been eviscerated by the realities of modern technology."), *reh'g en banc granted, opinion withdrawn by,* 385 F.3d 793 (1st Cir. 2004).

286. *See* S. REP. NO. 90-1097, at 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153 (explaining that the predicate crimes were limited to "specified types of serious crimes" to protect privacy, one of two purposes of the Wiretap Act).

287. 18 U.S.C. § 2516(3) (2000). Any attorney for the government may authorize such interceptions, while only certain Justice Department officials may authorize wiretaps. *See id.* § 2516(1), (3).

288. 18 U.S.C. §§ 2703(d), 3123(a) (2000 & Supp. I 2001).

289. *See infra* Part V (discussing how to link online surveillance practices to offline analogues).

290. H.R. REP. NO. 99-647, at 22 (1986). On the other hand, the Senate report noted that electronic communications stored by third parties "may be subject to no constitutional privacy protection." *See* S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

well[291] persists as the only decision to hold that government searches of e-mail implicate the Fourth Amendment, and it lacks precedential value because it is a military case. In *Maxwell*, the Court of Appeals for the Armed Forces affirmed limited constitutional protection for the content of e-mail messages and analogized e-mails to telephone calls and sealed letters.[292] A few other cases suggest in dicta that the Fourth Amendment protects the contents of e-mail, but none has granted a suppression remedy to a victim of an unauthorized e-mail interception.[293]

Meanwhile, several lower courts have denied suppression remedies to victims of potentially unlawful online surveillance. These cases have identified categories of online information that affirmatively lack constitutional protection. For example, a federal district court excluded chat room conversations from constitutional protection.[294] In other cases, courts have denied constitutional protection to online communication attributes, such as the user's e-mail address and other identifying information, including passwords. The courts reasoned that users forfeit any privacy interest in such information when they voluntarily give the information to their electronic service providers.[295]

With the lack of a constitutional baseline from the Supreme Court, it has been up to Congress to regulate online surveillance. Because the ECPA is both out-of-date and ambiguous, those regulations require much interpretation. The next subpart considers those interpretations.

D. Ambivalence Becomes Hostility in the Online Environment

Extensive disregard for the prohibition against wiretapping prior to the Wiretap Act signified deep ambivalence about how to regulate traditional electronic surveillance. Continued violations of the Wiretap Act, notwithstanding its efforts to rein in unauthorized surveillance, suggest that ambiva-

---

291. *See* United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996). For a case stating that *Maxwell* has "little or no precedential value," see United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000), *cert. denied*, 531 U.S. 1099 (2001).

292. *Maxwell*, 45 M.J. at 417-18. The protection was limited in the sense that it seemed to depend on such factors as Maxwell's contractual relationship with America Online and its policy not to read subscriber's e-mails. *See also* Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (finding system operator's disclaimer of privacy to defeat reasonable expectation of privacy in e-mail); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (finding the same for a government employee); United States v. Monroe, 52 M.J. 326 (C.A.A.F. 2000).

293. *See, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997); Commonwealth v. Proetto, 771 A.2d 823, 830-31 (Pa. Super. Ct. 2001).

294. *See Charbonneau*, 979 F. Supp. at 1185. The court noted in dicta that e-mail messages lose Fourth Amendment protection once they are received or forwarded. *Id.* at 1184; *accord Guest*, 255 F.3d at 334-35.

295. *See, e.g., Guest*, 255 F.3d at 335-36 (denying the suppression of passwords, names, addresses, and birthdates because they were provided to a third party); *Hambrick*, 55 F. Supp. 2d at 508 (denying suppression of e-mail address, name, billing address, credit card number, and IP connection information despite invalid subpoena); *Kennedy*, 81 F. Supp. 2d at 1110 (denying suppression of subscriber information obtained by invalid court order). See *infra* Part III.D.4 for a critique of this reasoning.

lence persists.[296] When we maintain a sizeable gap between official proscriptions and actual practices, our commitment to strict regulation of wiretapping seems unsteady.

One does not need to look to a gap between proscription and practice to perceive significant ambivalence about whether to restrict law enforcement access to private online data. The law itself gives government agents considerable leeway. On their face, the ECPA provisions for online surveillance permit significantly more information to be disclosed with significantly fewer restrictions than the Wiretap Act.

But the real blow to online privacy has been delivered by the executive branch, which has promulgated interpretations of the ECPA that substantially limit its protection of online privacy. The government has taken advantage of the statute's ambiguity and complexity, and Congress has largely failed to clarify or simplify the law. Bills to increase online privacy gained momentum but not passage prior to the tragic events of September 11, 2001.[297] Instead, the Justice Department promoted the two substantive amendments that have actually made it into law.[298] The public has remained disengaged, no doubt due in part to the statute's complexity, which defeats attempts to make sense of it.[299]

Government's efforts to limit the ECPA's protections both in court and in Congress evidence not ambivalence, but outright hostility towards online privacy. In Part V, I take up the question of whether that characterizes society's views as well. First, I briefly review some of the government's aggressive statutory interpretations and how, in contrast to those courts that rejected narrow interpretations of the proscription against wiretapping, modern courts have mostly accepted the government's narrow view of the ECPA.

1. Aggressive Interpretations and Judicial Review

a. Limiting the Scope of the Dynamic Content Protections

Because the law restricts dynamic content interceptions so much more rigorously than stored content acquisitions, courts have been forced to di-

---

296. *See supra* note 20 and accompanying text.

297. *See, e.g.*, Electronic Communications Privacy Act of 2000, H.R. 5018, 106th Cong. (2000) *reprinted in* H.R. No. 106-932, at 2-7 (2000); Enhancement of Privacy and Public Safety in Cyberspace Act, S. 3083, 106th Cong. (2000); *see also Antiterrorism Hearings*, *supra* note 201, at 21 (statement of James X. Dempsey) (describing proposed privacy bills).

298. *See Antiterrorism Hearings*, *supra* note 201, at 3 (statement of Rep. Nadler) (recalling that the USA PATRIOT Act "was drafted in secret over a weekend by representatives of the Department of Justice and the House leadership."); Freiwald, *supra* note 224 (discussing the Justice Department's promotion of CALEA).

299. Those of us who teach online privacy watch law students struggle mightily with the ECPA's provisions and cases interpreting them. Mention of a "pen register," in particular, provokes an eyes-glazing-over response. Activist groups who support online privacy, such as the ACLU, the Electronic Privacy Information Center, and the Electronic Frontier Foundation, have done an admirable job trying to educate the public.

vine the line between the two practices. In particular, they have had to decide when an electronic communication comes to rest in electronic storage after being "in transmission." The answer has significant repercussions; the smaller the dynamic interception category, the less favorably the privacy of online communications compares to the privacy accorded traditional telephone calls.

A key question has been whether an e-mail is conceptually "in transmission" and therefore capable of interception until its intended recipient retrieves it, or whether, instead, an e-mail is no longer "in transmission" once it comes to rest on the recipient's server. Congress gives little guidance on the matter.[300] In 1994, in *Steve Jackson Games, Inc. v. United States Secret Service*, the Fifth Circuit considered what remedy to give innocent users of an electronic bulletin board whose e-mail messages had been read by Secret Service agents without any legal authority.[301] The Fifth Circuit accepted the government's argument that an e-mail may be intercepted only when a law enforcement agent acquires it "contemporaneous[ly] with . . . transmission."[302] Although the agents had read and even deleted the e-mails before the recipients had retrieved them, they had not done so "contemporaneously" with the e-mails' transmission. The Court refused to find a violation of the dynamic content interception provisions.[303]

Courts have generally adopted the Fifth Circuit's approach.[304] Several have considered the implication. By merely waiting perhaps a nano-second for an e-mail to reach its destination, law enforcement monitors may easily avoid the super-warrant requirements for dynamic content interceptions.[305] Privacy of online communications therefore depends heavily on the agents' timing, rather than on meaningful differences in either the information acquired or the intrusiveness of the procedures. A panel of the Ninth Circuit recognized the anomaly in a 2001 decision involving unauthorized access to

---

300. Although the House report suggested that an e-mail waiting on the server to be read by its recipient would be considered to be in electronic storage for the purposes of a different provision, it also considered voice mail to be in electronic storage, which meant it could be both in storage and interceptible. *See* H.R. REP. NO. 99-647, at 63 (1986); *see also supra* note 266 (discussing ECPA treatment of voice mail); *infra* notes 400-02 and accompanying text (discussing amendments to voice mail provision).

301. 36 F.3d 457, 460 (5th Cir. 1994).

302. *Id.*

303. *See id.* at 463. The agents had apparently never heard of the ECPA, four years after its passage. Though the agents persistently denied that they had read or deleted the 162 e-mails, the trial court chose not to believe them. *See id.* at 459. Note that the court found the Secret Service in violation of the provisions pertaining to unauthorized access to electronic communications, 18 U.S.C. § 2701, rather than 18 U.S.C. § 2703, which pertains to procedures for requiring a service provider to disclose electronic communications contents in storage. *See id.* at 462-63.

304. *See* Fraser v. Nationwide Mut. Ins., 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission.").

305. *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003) (describing the interception of emails as nearly impossible under this approach) (quoting Jarrod J. White, *E-mail @Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1083 (1997)), *cert. denied*, 538 U.S. 1051 (2003); *Fraser*, 352 F.3d at 114 ("While Congress's definition of 'intercept' does not appear to fit with its intent to extend protection to electronic communications, it is for Congress to cover the bases untouched.").

information stored on a private web page.[306] The panel held that an "intercept" under the ECPA means the acquisition of the contents of a communication whether in transit or from electronic storage and that the lesser protections for stored communications apply only when a person obtains unauthorized access to communications but does not obtain their contents.[307] According to the panel, "[a]n electronic communication in storage is no more or less private than an electronic communication in transmission. Distinguishing between the two for purposes of protection from interception is 'irrational' and 'an unsupportable result given Congress' emphasis of individual privacy rights during passage of the ECPA."[308] The panel's decision was subsequently withdrawn, and a new panel issued a decision that followed *Steve Jackson Games* and required a statutory intercept to be contemporaneous with the e-mail's transmission.[309] The original panel's laudable attempt to make sense of the statute and give appreciable scope to the category of highly regulated dynamic content interceptions ended in failure.[310]

Another court has promoted an interpretation of the ECPA that could eviscerate the dynamic content protections. In early 2003, a Massachusetts federal district court, in *United States* v. *Councilman*, held that an e-mail cannot be intercepted when it rests on a computer server along its transmission path.[311] The court reasoned that even communications obtained during the "ephemeral" moment they are stored in a "momentary 'hop' along the path from sender to receiver" are "in storage" rather than "in transit." The court recognized that electronic communications traveling the Internet may "constantly" be in storage and in transit "simultaneously" but opted to apply the weaker in-storage provisions nonetheless.[312] The First Circuit affirmed the lower court's decision and its expansive reading of electronic storage.[313]

---

306. *See* Konop v. Hawaiian Airlines, 236 F.3d 1035, 1035 (9th Cir. 2001).

307. *See id.* at 1045-48 (considering when to apply 18 U.S.C. § 2701 instead of 18 U.S.C. § 2511), *withdrawn*, 262 F.3d 972 (9th Cir. 2001).

308. *Id.* at 1045 (quoting Thomas Greenberg, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 248-49 (1994)). The panel "believe[d] that Congress intended the ECPA to eliminate distinctions between protection of private communications based on arbitrary features of the technology used for transmission." *Id.* at 1046.

309. *See* Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003).

310. *See id.* at 892 (Reinhardt, J., dissenting) ("[R]eading the Wiretap Act to prohibit interception of 'stored electronic communications' provides a more coherent construction of the Act and is more consistent with the text of the statute as well as with the Congressional intent . . . .").

311. 245 F. Supp. 2d 319, 321 (D. Mass. 2003), *aff'd*, 373 F.3d 197 (1st Cir. 2004). *reh'g en banc granted, opinion withdrawn by,* 385 F.3d 793 (1st Cir. 2004).

312. *See id.* The court noted that the rule of lenity influenced its choice; it was considering a criminal action against a private individual. A court considering the actions of government could well make the opposite choice. However, the court noted that the government had pressed for the court's interpretation in an earlier case. *See id.*

313. *See* United States v. Councilman, 373 F.3d 197, 203 (1st Cir. 2004) (finding e-mails "accessed . . . as they were being transmitted and in real time" to be acquired out of electronic storage and therefore not intercepted), *reh'g en banc granted, opinion withdrawn by,* 385 F.3d 793 (1st Cir. 2004).

If other courts follow suit, there will be no cases in which the privacy-protective provisions for dynamic content interceptions apply.[314]

In addition to shrinking the category of dynamic content interceptions, which substantially reduces online privacy, the contemporaneity standard has generated other odd results. For example, one court concluded that a government agent's installation of a key stroke logger system ("KLS") to obtain a target's password was not a dynamic content interception. Though the device recorded the target's keystrokes contemporaneously with his typing them, the court accepted the FBI agents' claim that they had configured the device to operate only when the target's modem was turned off.[315] Strangely, the court implied that the KLS was wholly unregulated due to the way the FBI had installed it.[316]

b. Minimizing the Protections for Stored Communications

Government monitors have an incentive to reduce the number of investigations that require a warrant, because warrants are harder to obtain than either subpoenas or the statutory court orders available to access stored communications in the ECPA.[317] One way to do so is to expand the definition of long-term storage at the expense of short-term storage, since the former does not require a warrant, while the latter does. Justice Department training materials currently assert that once a recipient retrieves and opens an e-mail, any acquisition of that e-mail's contents—no matter when it occurs—falls under the long-term storage protections.[318] The Justice Department's interpretation erodes online privacy by permitting agents to obtain almost all e-mail messages without ever obtaining a warrant.

Though a complete analysis of the Justice Department's approach is beyond the scope of this Article, it is clearly quite aggressive. It rests on a strained reading of a statutory term designed to cover practices in 1986 that are no longer applicable.[319] It asserts, illogically, that a computer morphs

---

314. *See Konop*, 302 F.3d at 878 n.6 (recognizing that "if the term 'intercept' does not apply to the *en-route* storage of electronic communications, the Wiretap Act's prohibition against 'intercepting' electronic communications would have virtually no effect.").

315. United States v. Scarfo, 180 F. Supp. 2d 572, 581-83 (D.N.J. 2001). The defendant received only a short summary of how the device worked because the government successfully claimed the information was classified. *See also id.* (affidavit of Randall S. Murch) (Oct. 4th, 2001) (providing a general description of KLS).

316. The court found no violation of the stored communication protections because "the F.B.I. [did not] 'install or operate any KLS component which would search for or record any fixed data stored within the computer.'" *Id.* at 581.

317. *See* COMPUTER CRIME AND INTELL. PROP. SEC., CRIM. DIV., U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELEC. EVIDENCE IN CRIM. INVESTIGATIONS 54-56 (2002) [hereinafter DOJ SEARCH MANUAL].

318. *Id.* at 56-58. For simplicity, I will say that the recipient has "read" an e-mail when he retrieves it and opens it, but the three acts may well be distinct.

319. The Justice Department argues that once retrieved, an e-mail rests on a "remote computing service," which, in 1986, described off-site time-sharing services used to conserve electronic storage. The training materials recognize that the technology described is outmoded. *Id.*; 18 U.S.C. § 2511; H.R. REP. NO. 99-647, at 64 (1986); S. REP. NO. 99-541, at 45 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555,

from one type of service into another type when an e-mail is read, just for that e-mail. The approach conflicts with the ECPA's legislative history, which indicates that the government would need warrants for e-mails stored 180 days or less, because Congress viewed such information as constitutionally protected.[320] It conflicts with the reasoning of a recent case, in which the Sixth Circuit accepted that electronic contents stored for a short time may not be acquired without a warrant.[321] Finally, the approach contrasts with a clarification provided by the House Judiciary committee in a report accompanying a 2000 bill. The report indicates that the protection for e-mails in storage should not vary based on whether the e-mails are read or accessed.[322]

Again drawing upon the outmoded statutory term that no court has ever defined, the Justice Department further teaches that an e-mail, once read, falls entirely out of the ECPA's protections if it resides on a service that does not offer e-mail to the general public.[323] In other words, the Justice Department claims that users of e-mail provided by private employers, such as companies and universities, have absolutely no protection from government demands for their e-mail messages once the messages have been read. This would mean that a large proportion of e-mails in existence today are completely unprotected.[324] This interpretation directly conflicts with Congress' stated intent to protect the contents of e-mails after they have been read, and, in fact, even after they have been discarded or deleted.[325] The

---

3599. *See also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1559-64, 1593-96 (2004) (discussing the background to the ECPA's treatment of stored e-mails).

320. *See, e.g.*, H.R. REP. NO. 99-647, at 69 ("The only contents which can be sought using the court order option are, of course, those stored for more than 180 days."); *id.* at 68 ("The general rule [requiring a warrant] applies to electronic communications which have been in electronic storage for 180 days or less."); *id.* at 23 n.41.

321. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 339 (6th Cir. 2001) (reading the ECPA to "provide[] that the government may have access to the contents of electronic communications that have been stored 180 days or less only by using a warrant").

322. *See* H.R. REP. NO. 106-932, at 12-15 (2000) (noting that the approved bill "clarifies that an electronic communication in 'electronic storage' enjoys the protections provided to such communications regardless of whether or not the communication has been 'opened' or otherwise accessed by the intended recipient"). The approved bill would have extended the warrant requirement from e-mails stored 180 days to one year. *Id.*

323. The ECPA defines a "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). The Justice Department argues that read e-mails cannot be on remote computing services if their electronic service provider does not serve the public, and they cannot be on an electronic communication system once read. DOJ SEARCH MANUAL, *supra* note 317, at 57-58, 66-67.

324. DOJ SEARCH MANUAL, *supra* note 317, at 57-58, 66-67.

325. *See* H.R. REP. NO. 99-647, at 65 (1986) (stating that communications stored "for re-access at a later time" after having been received, "should continue to be covered by" the stored content protections); *id.* at 72. The Ninth Circuit recently rejected the government's argument, made as amicus curaie, that opened e-mail may no longer be considered to be in electronic storage. Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004). Though the court did not "lightly conclude that the government's reading is erroneous," it held that "prior access is irrelevant to whether the messages at issue were in electronic storage." *Id.* at 1077. The issue was whether a private party had violated the provisions on access to stored communications without authorization, 18 U.S.C. § 2701, rather than the stored contents provisions I have been discussing. *Id.* at 1071. *See also* Fraser v. Nationwide Mut. Ins., 352 F.3d 107, 114 (3d

very fact that the ECPA provides specific procedures for accessing communications stored for more than 180 days conflicts with the government's interpretation.[326] Finally, the House Judiciary report from 2000 offers absolutely no support for such an outrageous interpretation.[327]

According to the Justice Department, e-mails are entitled to the short-term storage protections for stored content acquisitions only when they are sitting on a server waiting to be retrieved.[328] Once they are retrieved—even if it is immediately after they arrive—they are subject to the long-term storage protections if they reside on a public system, but to no protections at all if they reside on a private system.[329] Were it not for the history of outlandish interpretations of restrictions on wiretapping, these arguments would be hard to believe.[330] Unfortunately, Congress has not managed to reassert that the ECPA is designed to protect privacy rather than eliminate it.

c. *Immunizing the Government from Stored Attribute Claims*

Recall that the protections for stored attributes are even weaker than those for stored content. Many stored attributes may be acquired with a subpoena that can be obtained without a judge's involvement. For the more protected attributes, Congress provided a relatively easy-to-obtain court order.[331] As though these provisions were not weak enough, in 1996, the Fourth Circuit found that police officers faced no liability when they used an admittedly invalid subpoena.[332] The court examined the statutory text and concluded that it regulated only the conduct of the service providers and not government actors.[333] Given the expansive good faith defense for service providers, it is hard to imagine how stored records would ever be protected under the Fourth Circuit's approach.[334]

The USA PATRIOT Act amendments rephrased the statutory language, which recently encouraged one district court to reject the Fourth Circuit's approach and to impose liability on the government for failure to comply

---

Cir. 2003) (assuming the same approach without deciding it).

326. *See* H.R. REP. NO. 99-647, at 39 (explaining that definitions of "storage" are not intended to be limiting); 18 U.S.C. § 2703(b) (describing procedures that apply when the government acquires electronic contents after 180 days).

327. While the 2000 House Judiciary report did not discuss remote computer services, nothing in it suggests that e-mail on private services would cease to be covered once read. Quite the contrary, the drafters appeared to view e-mails on internet service providers, or "other third parties," as entirely covered by the ECPA's protections. *See* H.R. REP. NO. 106-932, at 12 (2000). Had the committee members viewed this interpretation as credible, it seems likely that they would have at least mentioned it.

328. DOJ SEARCH MANUAL, *supra* note 317, at 57-58.

329. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

330. *See supra* Part II.D.1.

331. 18 U.S.C. § 2703 (1993 & Supp. 2004).

332. Tucker v. Waddell, 83 F.3d 688, 693 (4th Cir. 1996) (interpreting 18 U.S.C. § 2703(c)).

333. *Id.*

334. *See* 18 U.S.C. § 2703(e) (immunizing service providers who provide information "in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification").

with the stored attribute requirements.[335] If other courts agree, the stored attribute protections may not be completely toothless. That would certainly be more consistent with Congress' intent in the ECPA to regulate both public and private conduct and to protect the privacy of stored information.[336] Nevertheless, the Fourth Circuit's approach, affirmed in dicta by the Sixth Circuit, stands as a stark example of how little privacy the courts are willing to read into the ECPA.[337]

d. Expanding the Scope of Pen Register Investigations

The history of the pen register provisions is replete with aggressive interpretations. As discussed, Congress based the pen register provisions on the 1979 *Smith v. Maryland* decision, which found that pen register surveillance does not constitute a search under the Fourth Amendment.[338] The pen register in *Smith* recorded the telephone numbers dialed on a traditional phone.[339] The ECPA reflected the pen register's technical limitations in its terminology and legislative history.[340]

Nonetheless, during the period after the ECPA's passage and before the USA PATRIOT Act, government monitors argued that surveillance obtaining *any* non-content information needs to satisfy only the minimal requirements of the pen register provisions. Courts treated increasingly sophisticated devices as pen registers, notwithstanding the ability of the devices to obtain rich electronic communication attributes, and notwithstanding that the devices lacked resemblance to the pen registers Congress considered when it passed the ECPA. Such devices could incorporate hardware and software and reveal communications' participants, duration, and location.[341] Nonetheless, the devices were subjected to the minimally demanding pen register provisions of the ECPA.

The USA PATRIOT Act amendments clarified that "pen registers" could intercept electronic addressing information and thereby accepted the notion that sophisticated devices—like Carnivore—would be subject to the pen register provisions.[342] Unfortunately, Congress did not match the power

---

335. Freedman v. Am. Online, 303 F. Supp. 2d 121, 126 (D. Conn. 2004). Apparently, the provisions were changed for unrelated reasons. Those amendments are scheduled to sunset at the end of 2005. *DOJ Field Guidance*, *supra* note 279, at 1232-33.

336. *See, e.g.*, H.R. REP. NO. 99-647, at 74 (1986); *Freedman*, 303 F. Supp. 2d at 126-27 (discussing Congressional intent to protect privacy).

337. *See* Guest v. Leis, 255 F.3d 325, 339 (6th Cir. 2001).

338. Smith v. Maryland, 442 U.S. 735, 745 (1979).

339. *Id.* at 737.

340. *See* 18 U.S.C. § 3127(3) (1986), *amended by* 18 U.S.C. § 3127 (1993 & Supp. 2004) (defining the term "pen register"); *see also* S. REP. NO. 99-541, at 49 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3603 (stating that pen registers "record only the telephone numbers dialed").

341. *See* Freiwald, *supra* note 224, at 982-89 (reviewing the "Evolution of the Pen Register from Mechanical Device to Computer System"); *see also* Schneier, *supra* note 57, at 77 (discussing how much addressing information reveals).

342. 18 U.S.C. § 3127 (1993 & Supp. 2004). Unlike other parts of the USA PATRIOT Act, the pen register provisions do not sunset in 2005.

of the new devices with any additional restrictions, except that when a government agent uses a Carnivore-type device, she must provide a report to the judge who approved it.[343] As it now stands, much online information may be obtained by satisfying the pen register provisions.[344] Those requirements are so limited that one court suggested that they were designed merely to gather statistics rather than to protect privacy.[345]

It seems absurd to use regulations designed for a device that recorded the numbers dialed by a telephone on a paper tape for systems that may electronically collect all Internet-based data.[346] Moreover, online privacy rests in the technical choices of government monitors. The government has interpreted the pen register provisions to authorize devices that can record contents, so long as they are not configured to do so when they are used.[347] Similarly, although the language is ambiguous, the ECPA seems to require that government monitors use "technology" to assure that pen registers do not gather content only if that technology is "reasonably available."[348] The bottom line seems to be that the government may lawfully obtain much online information merely by meeting the pen register requirements. As I next discuss, the ECPA's minimal control mechanisms do little to ensure that government agents comply with the law.

e. Judicial Review of Online Surveillance

The Wiretap Act required judges to be actively involved in electronic surveillance investigations. Historically, judges have rejected many of law enforcement's most aggressive interpretations of the law. This is not the case in the online context, where courts have seemed inclined to accept statutory constructions that narrow privacy protections.[349] But even if a modern court were inclined to rein in online surveillance, it would have few opportunities to do so.

---

343. *Id.* § 3123(a)(3).

344. In a related context, the D.C. Circuit has rejected the government's argument that "call-identifying information" under CALEA includes all numbers dialed, even after a call has been connected. The court recognized that such numbers include passwords, codes, prescription numbers, and other content and faulted the FCC for not considering privacy when it accepted the government's claim. United States Telecom Ass'n. v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000).

345. *See In re* Order Authorizing Installation of Pen Register, 846 F. Supp. 1555, 1559-60 n.5 (M.D. Fla. 1994).

346. *See supra* notes 239-40 and accompanying text.

347. *See* 147 CONG. REC. S10372 (daily ed. Oct. 9, 2001) (statement of Sen. Leahy) (stating that current pen registers do obtain content).

348. 18 U.S.C. § 3121(c) (Supp. 2004); *see also* 147 CONG. REC. S10372 (daily ed. Oct. 9, 2001) (statement of Sen. Leahy) ("Perhaps, if there were meaningful judicial review and accountability, the FBI would take the statutory direction more seriously and actually implement it.") (referring to 18 U.S.C. § 3121(c)); *Antiterrorism Hearings*, *supra* note 201, at 13 (statement of Viet D. Dinh) (explaining that law enforcement must minimize the possible collection of content by a pen register "to the extent feasible with reasonably available technology" (quoting a May 24, 2002 memorandum from the Deputy Attorney General to field officers instructing them on how to avoid collecting data inadvertently)).

349. *See infra* Part III.D.1.

As a matter of pre-investigation review, only dynamic content interceptions maintain the super-warrant procedural requirements. Under those requirements, would-be government monitors have to establish a tight locus between the proposed surveillance and the commission of an enumerated crime, and they must use surveillance only as a last resort. Further, judges may oversee ongoing investigations to ensure that agents comply with the minimization requirements and limit the duration of the investigations.[350] Courts play a much more limited role in approving the other types of online surveillance investigations. The minimization and duration requirements do not apply to other types of online surveillance, and no provision is made for ongoing judicial oversight.[351]

If government monitors satisfy the standard warrant requirement to conduct a stored contents acquisition, they may search for mere evidence and fruits of a crime.[352] The court order requirement for stored information is not rigorous: agents must merely "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought . . . [is] relevant and material to an ongoing criminal investigation."[353] Subpoenas may be easily obtained on a standard of mere relevance.

For pen register surveillance, courts are to approve requests "if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained . . . is relevant to an ongoing criminal investigation."[354] It is not clear whether courts are even supposed to review pen register applications. On one hand, the ECPA requires the court to "find" that the attorney has made the proper certification,[355] and the Senate report indicates that a court "must first be satisfied that the information sought is relevant" before it issues an order.[356] On the other hand, the same report explains that the "provision does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only to review the completeness of the certification submitted."[357] Government attorneys have convinced courts that they should act as human rubber stamps when presented with a pen register application.[358]

---

350. *See supra* Part II.C.2.

351. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 463 (3d Cir. 1994) (suggesting that the possibility of key-word searching obviates the need to minimize acquisition of stored contents).

352. FED. R. CRIM. P. 41(c) (2000).

353. 18 U.S.C. § 2703(d) (Supp. 2004). Originally, the court order requirement was easier to satisfy, but it was amended to its present form in 1994. *See supra* note 224.

354. 18 U.S.C. § 3123(a)(1) (Supp. 2004).

355. *Id.*

356. S. REP. NO. 99-541, at 47 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3601. The Report also describes the need for the judge to make the "same judicial findings" before granting any pen register extensions. *Id.*

357. S. REP. NO. 99-541, at 47 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3601. The same ambiguous language appears in the House Report. *See* H.R. REP. NO. 99-647, at 77 (1986).

358. *Antiterrorism Hearings*, *supra* note 201, at 15 (statement of James X. Dempsey) (explaining that, in pen register investigations, the "judge, really, just becomes a rubber stamp"); *see, e.g.*, United States v. Hallmark, 911 F.2d 399 (10th Cir. 1990) (upholding a lack of review and finding against a separation of powers challenge). *But see* United States v. Doe, No. 91-10260, 1992 WL 138173 (9th Cir.

As for post-investigation review, all forms of online surveillance, including dynamic content interceptions, lack the statutory suppression remedy that Congress provided for traditional surveillance in the Wiretap Act.[359] Although there is no doubt that Congress intended to deprive victims of unlawful online surveillance of a suppression remedy, it is not clear why. The omission is not aligned with a major goal of the ECPA—to ensure the privacy of electronic communications and extend all of the Wiretap Act's protections to the new media.[360] The Senate report reveals only that the omission was the "result of discussions with the Justice Department."[361]

While the ECPA provides that defendants may still have a constitutional right to a suppression remedy, defendants have lost all motions to suppress online surveillance information based on the Fourth Amendment, with the exception of one military case.[362] The consistent failure of such claims likely explains why relatively few are brought. But without suppression hearings, courts have few opportunities to delineate permissible practices.[363] Moreover, without the prospect of a suppression remedy, few victims of unlawful surveillance have sufficient incentive to bring a case, no matter how egregious the privacy violation.

2. *Underenforcement and New Remedies and Punishments*

In the absence of a suppression remedy, law enforcement agents face few negative repercussions if they fail to adhere to the ECPA's requirements. If government agents conduct unlawful dynamic content interceptions, they face fines or imprisonment for up to five years when they cannot mount a good faith defense.[364] However, no published opinions discuss any convictions of law enforcement personnel for violations of these provi-

---

1992) (holding that the district court can conduct limited inquiry in pen register orders).

359. *See* Steve Jackson Games, 36 F.3d at 461 n.6 (discussing the ECPA and its legislative history).

360. *See* H.R. REP. NO. 99-647, at 17-19; S. REP. NO. 99-541, at 20 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3574.

361. *See* S. REP. NO. 99-541, at 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577; Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393, 409-11 (1997) (describing Justice Department opposition to the suppression remedy and congressional acquiescence due to the need for its support). Apparently, the ECPA proponents' original plan was to provide all of the protections of the Wiretap Act to electronic communications. *See* Mulligan, *supra* note 319, at 1582.

362. *See supra* Part III.C.2. Those cases that have been brought have concerned allegations of online child pornography, as did all the cases discussed in Part III.C.2. Child pornography defendants may well escape conviction if they can have the online evidence suppressed, so they have had a significant incentive to bring such suits. Unfortunately for privacy rights, they do not make sympathetic defendants. *See infra* Part III.D.4.

363. *See* Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Law*, 54 HASTINGS L.J. 805, 806, 825, 837 (2003).

364. 18 U.S.C. §§ 2511(4), 2520(d).

sions.[365] Agents who violate the stored communication provisions do not face criminal charges, although they could face administrative discipline.[366]

Victims of unlawful dynamic content interceptions may recover civil damages of as much as $10,000 from government agents.[367] Victims of stored communications violations may recover statutory damages of no less than $1,000 against willful violators.[368] Perpetrators may always raise a statutory good faith defense.[369] It is evident that the amounts for statutory damages will not cover the costs of most lawsuits. Moreover, the punishments for privacy violators pale in comparison to the punishment meted out against hackers, who may be fined up to $250,000 and imprisoned for five years for a first offense.[370]

Victims of unauthorized pen register investigations have no civil recourse.[371] In light of the refusal by courts to grant a suppression remedy to victims of unlawful pen register surveillance, there appears to be no meaningful regulation of pen register investigations.[372] The ECPA provides for the possibility of a fine and a misdemeanor criminal charge for knowing violators, but there are no known cases that have been brought against government agents for violating the pen register provisions.[373]

3. *Secret Practices and Reporting Obligations*

Two mechanisms combat the secrecy that necessarily attends electronic surveillance. The first is notice to the target, who can then challenge the asserted activity. Dynamic content interceptions track the provisions of the Wiretap Act that require targets to be notified soon after the surveillance investigation is complete.[374] But the other online surveillance investigations have much more limited notice requirements.

---

365. Research discloses no published opinions pertaining to prosecutions of government violators of the ECPA provisions.

366. 18 U.S.C. § 2707(d). Government entities may be subject to criminal penalties for accessing stored records if their actions constitute a violation of 18 U.S.C. § 2701, which prohibits unauthorized access.

367. 18 U.S.C. § 2520(c)(2)(B). Attorney's fees, costs and punitive damages are also available. *Id.* § 2520(b). The USA PATRIOT Act precludes claims against "the United States," except for willful violations. Recovery of $10,000 and costs are allowed, but no jury trial, attorney's fees, or punitive damages. *Id.* § 2712(a)-(b). Administrative discipline of federal agents may be pursued in some cases. *Id.* §§ 2520(f), 2712(c).

368. 18 U.S.C. § 2707(c). *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 459, 460 n.5 (5th Cir. 1994) (awarding $1,000 damages for violation of unauthorized access provisions). Punitive damages may be awarded when the violation was willful or intentional. 18 U.S.C. § 2707(c).

369. *See, e.g.*, Davis v. Gracey, 111 F.3d 1472, 1482-84 (10th Cir. 1997) (granting a good faith defense to police officers who conducted unauthorized seizure of stored e-mails).

370. *See* 18 U.S.C. § 2701(b)(1) (2000); H.R. REP. NO. 99-647, at 63 (1986).

371. *See* H.R. REP. NO. 99-647, at 76 (noting that the absence of a civil cause of action was "purposeful").

372. *See* United States v. Thompson, 936 F.2d 1249 (11th Cir. 1991) (refusing to exclude improperly obtained pen register information), *cert. denied*, 502 U.S. 1075 (1992).

373. 18 U.S.C. § 3121(d).

374. *See id.* § 2518(8)(d).

Targets must receive prior notice when the government uses a subpoena or a court order to obtain their stored communication contents. But when the government obtains a warrant, it need not provide notice before it obtains stored communications contents in long-term storage.[375] As for short-term stored communications contents—those for which agents must obtain a warrant—the statute is silent on notice, and the cases are divided on whether it is required.[376] Even when prior notice is required before accessing stored communications, it may be delayed if necessary to the investigation.[377] Although the ECPA permits targets to contest the acquisition of their stored electronic information,[378] many targets may never learn of the investigation or may learn of it too late to stop it, even when they have sufficient grounds to halt the investigation.

The ECPA explicitly excuses the government from providing notice to targets of stored attributes acquisitions.[379] Similarly, nothing in the ECPA requires that targets ever be notified of pen register surveillance. In fact, the orders for both types of investigations typically specify that service providers who learn of them or assist in them must never alert the target.[380]

The other mechanism that combats secrecy is notice to the community in the form of published reports to Congress. Dynamic content interceptions must be reported in the same manner as traditional wiretaps and electronic surveillance.[381] Pen register investigations must also be reported, but the reports are much more limited. They list only the number of pen registers used by the Department of Justice agencies, and they lack any information on the effectiveness of the investigations.[382] No reports are required about the acquisition of stored information.

4. Line Drawing and Reasonable Expectations of Privacy

As I have discussed, Congress drafted the ECPA with little constitutional guidance. It relied on two Supreme Court cases when it regulated online surveillance.[383] One, *United States v. Miller*, withheld constitutional

---

375. *See id.* § 2703(b).

376. *See id.* § 2703(a). *Compare* Guest v. Leis, 255 F.3d 325, 339 n.7 (6th Cir. 2001) (dispensing with notice) *with* Steve Jackson Games, Inc. v. United States Secret Serv., 816 F. Supp. 432, 443 (W.D. Tex. 1993) (requiring prior notice), *aff'd*, 36 F.3d 457 (5th Cir. 1994).

377. *See* 18 U.S.C. § 2705 (2000).

378. *See id.* § 2704 (providing a process for customer challenges to stored content acquisitions); H.R. REP. NO. 99-647, at 70 (1986).

379. *See* 18 U.S.C. § 2703(c)(3) (2001); H.R. REP. NO. 99-647, at 69.

380. *See id.* § 3123(d) (providing for no disclosure to the target "unless or until otherwise ordered by the court"); *id.* § 2705(a)(6)(b) (providing for a similar gag order regarding stored information).

381. *See id.* § 2519.

382. *Compare id.* § 3126 (listing the requirements for pen register reports), *with* 18 U.S.C. § 2519 (listing the requirements for dynamic content interceptions). In 2000, the pen register reporting provision was amended to require some details on the nature of the investigations, such as their length, what offenses were investigated, and which agency and agent applied for the order. Pub. L. No. 106-197, § 3, 114 Stat. 247 (2000). Prior to that, the law required merely the number of pen register applications each year to be reported. *See* 18 U.S.C. § 3126 (1986).

383. *See supra* notes 273, 290.

protection from financial records compiled by banks.[384] The other, *Smith v. Maryland*, denied Fourth Amendment protection to the telephone numbers dialed by a target and acquired by a mechanical pen register.[385] The Court in both of these decisions used the fact-of-interceptibility analysis to reason that if it is possible for information to be acquired by others, its acquisition is acceptable.[386] The Court avoided normative analysis and failed to consider how much privacy the law *should* actually grant to information. If the law treats information as private, then it will not be acceptable to acquire it, even when it possible to do so.[387]

Modern lower courts have failed to establish constitutional protections for online communications. This failure has certainly contributed to the lack of online privacy. Instead, when they have addressed the constitutional issues, lower courts have engaged in a fact-of-interceptibility analysis. For example, the Sixth Circuit found that a disclaimer of privacy posted on a computer bulletin board defeated users' claims to a reasonable expectation of privacy in their e-mails.[388] The court did not consider that the disclaimer might be ineffective to deprive users of their privacy rights.[389] In the same decision, the court rejected a reasonable expectation of privacy in online subscriber information, because the users had revealed it to a third party.[390] The other courts that have rejected a reasonable expectation of privacy in communication attributes have relied on the same reasoning.[391] Even in *Maxwell,* the only case so far to find a reasonable expectation of privacy online, the military court's finding was contingent on the fact that America Online was a private system, and it contractually bound itself not to read its users' e-mails.[392] Another court concluded that a child pornography defendant lacked a reasonable expectation of privacy in his subscriber information because he had knowingly turned it over to his electronic service provider.[393] Of course, telephone calls are revealed to the phone company, yet

384. 425 U.S. 435, 435 (1976).

385. 442 U.S. 735, 735 (1979).

386. *See supra* notes 213-17 and accompanying text (discussing *Smith*); *Miller*, 425 U.S. at 435 (reasoning that bank customers have no legitimate expectation of privacy in bank records because they were turned over to third parties), *overruled by* Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3421 (2000). In *Miller*, the information was not technically intercepted, but the reasoning is similar.

387. *See supra* note 218 and accompanying text; *see also* Bellia, *supra* note 216, at 1397-1409 (arguing that the Court conflated two different lines of Fourth Amendment cases in *Smith* and *Miller*).

388. *See Guest*, 255 F.3d at 333 (involving child pornography).

389. *Cf.* Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979) (explaining that a "normative inquiry" to determine privacy "would be proper" in a case in which the government merely announced that there was no privacy).

390. *See Guest*, 255 F.3d at 335 (relying on the *Miller* reasoning).

391. *See, e.g.*, United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); United States v. Hambrick, 55 F. Supp. 2d 504, 507-09 (W.D. Va. 1999).

392. *See* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996). Also, the *Maxwell* court viewed as significant that, at that time, AOL kept e-mails on its private system rather than sending them over the Internet. The court viewed e-mails sent over the Internet as "less secure" because they "must pass through a series of computers in order to reach the intended recipient." *Id.*

393. The *Hambrick* court recognized the need to make "a value judgment" about "how much privacy we should have as a society," before concluding that Hambrick had none. *See Hambrick*, 55 F. Supp. 2d

courts have not questioned that wiretapping phone calls violates reasonable expectations of privacy.

Modern courts have avoided the normative inquiry into how essential the Internet has become in our lives. Additionally, courts have avoided answering the question of whether our electronic communications should be subject to view by all simply because they may be subject to view by some.[394] I have suggested that the courts have avoided normative analyses because they are not comfortable with engaging in such value judgments explicitly. Deciding what should and should not be private may seem like a job better suited to the legislature. Unfortunately, it seems as though Congress is not willing to take the job, as it has neither clarified the ECPA nor ruled out interpretations that gut its privacy protections.[395]

If courts had engaged in the normative analysis that the reasonable expectations test requires, the context in which the claims had been made would not favor privacy interests. Almost all of the cases addressing the constitutional regulation of online surveillance have been brought by men eventually convicted of online child pornography and related offenses.[396] While child pornographers represent the worst side of the Internet and some of the most reprehensible members of society, they have been fighting for the privacy rights of all of us. Many judges would likely hesitate to grant online privacy rights when the immediate effect would be to free a sexual abuser of children.[397] However, the current failure to recognize most online privacy claims hurts many more people than just child sexual predators.

E. Unresolved Questions

1. The Impact of the USA PATRIOT Act

Passage of the USA PATRIOT Act brought renewed interest to American civil liberties because its provisions make significant changes to the way we handle terrorism investigations.[398] Much of the USA PATRIOT Act, however, has little to do with electronic surveillance, and the changes it

---

at 506. The court reasoned that the lack of any restriction in the ECPA on service providers' ability to share subscriber information with non-governmental third parties counseled against finding the information to be constitutionally protected. *See id.* at 507.

394. *See* Katz v. United States, 389 U.S. 347, 352 (1967) (basing its holding on the "vital role that the public telephone has come to play").

395. However, Congress made a move in the right direction in 2000. *See supra* note 297.

396. *See supra* note 362. Because most evidence of online child pornography derives from online surveillance, these defendants have much at stake in attempting to suppress the fruits of online surveillance.

397. Over the history of wiretapping, defendants prosecuted for gambling or prohibition violations fared better in their constitutional claims than those accused of more violent crimes. *See, e.g.*, CEDERBAUMS, *supra* note 12, at 19 (suggesting that the Court's refusal to apply retroactively *Katz'* protections reflected its concern with the seriousness of the crime alleged).

398. *See generally* THE WAR ON OUR FREEDOMS: CIVIL LIBERTIES IN AN AGE OF TERRORISM (Richard C. Leone & Greg Anrig, Jr. eds., 2003) (collecting essays on the impact of the USA PATRIOT Act).

makes to online surveillance are not dramatic.[399] The USA PATRIOT Act left almost all of the statutory definitions unchanged, and did not alter the structure of the online surveillance laws. It did not change the paucity of remedies or the lack of involvement of a judge in most online surveillance. It did not address most of the aggressive interpretations asserted by law enforcement. All of the changes it made, however, reduced online privacy.

The USA PATRIOT Act amended the definition of voice communications so that it would no longer include such communications when in electronic storage.[400] The legislative history suggests that the change was designed to reduce the privacy of voice mail by ensuring that it may not be "intercepted"; voice mail messages may be retrieved only out of electronic storage, and therefore subject to the weaker stored communications rules.[401] The other effect of the change was to remove one of the strongest arguments in favor of treating the acquisition of an e-mail message as an "interception" even after the e-mail had come to rest. If voice mail could be subject to the stronger protections accorded dynamic content interceptions, then it seemed irrational not to extend the same protection to e-mail. The amendment may well reduce the privacy protection of both voice mail and e-mail by removing the disparity in treatment.[402]

The USA PATRIOT Act reduced the privacy of stored records by adding more items to the list of attributes that may be obtained with a mere subpoena. Prior to the change, those items presumably could be obtained only upon presentation of a court order or a warrant, both of which are harder to obtain. In addition, the USA PATRIOT Act facilitated law enforcement's access to private computer systems by providing new mechanisms for service providers to disclose information voluntarily or invite agents to monitor their systems.[403]

Probably the most significant changes were made to the pen register provisions.[404] As mentioned, the USA PATRIOT Act changed the statutory definition to clarify that the pen register provisions would apply to devices or processes that obtained electronic addressing information. The change permits law enforcement agents to use Carnivore-type filtering packages

---

399. *See DOJ Field Guidance, supra* note 279; *see generally* Cindy Cohn, *EFF Analysis of the Provisions of the USA PATRIOT Act that Relate to Online Activities* 1201 (PLI Intellectual Property, Handbook Series No. G-701, 2002).

400. *See* 18 U.S.C. 2510(1) (Supp. I 2001).

401. *See* H.R. REP. NO. 107-236(I), at 158-59 (2001); *supra* notes 266, 300 and accompanying text.

402. *See* Konop v. Hawaiian Airlines, 302 F.3d 868, 878 (9th Cir. 2002) (reasoning that the amendment reduces the privacy of voice mail and supports a narrow construction of "intercept" to exclude the possibility of intercepting communications in electronic storage). However, according to Judge Reinhardt, there are other reasons to extend the interception protections to e-mail. *See id.* at 886-92 (Reinhardt, J., dissenting).

403. *See supra* note 399.

404. *See generally* Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 Geo. Wash. L. Rev. 1145 (2004) (describing negotiations over language including numerous discussions about the pen register provisions). The USA PATRIOT Act provided for nationwide pen register orders under which one order may be issued and then used to acquire information anywhere in the United States. *See* 18 U.S.C. § 3123(a)(1) (Supp. I 2001).

whenever they submit to a court for rubber-stamping an application that purports to demonstrate the relevance of the information sought.[405] The Act added a requirement that law enforcement agents who use Carnivore must report on that use to the judge who approves the order, but it did not specify what the judge should do with the report. The information is to be submitted under seal, and no provision is made for its disclosure to Congress or to the target, or for any repercussions to flow from its content.[406]

Several of the provisions just described are scheduled to sunset and thereby cease to be effective on December 31, 2005.[407] It is not clear whether the sunset provision will be repealed or delayed, although there have already been proposals for both.[408] But, the changes to the pen register provisions and the stored record provisions are permanent and will not be changed except by new legislation.

2. *A Third Category?*

The ECPA treats communication contents as substantially more deserving of protection than communication attributes, which are available largely by subpoena or by non-demanding court orders.[409] Only acquisition of contents ever requires a warrant, or even a super-warrant in some cases.[410] As I have discussed, the number of times either type of warrant is required may be few indeed. The USA PATRIOT Act did not reduce the significance of the divide between content and attributes.

As important as the line between contents and attributes is, it remains fuzzy. Clearly the communicative message within an e-mail (and now voice mail) must be classified as contents and electronic addressing information must be attributes. Other than that, nothing is clear. The Justice Department indicates in its training materials that the contents of actual files and the subject line of e-mails count as contents, but nothing in the statute guarantees either conclusion.[411] In fact, the content of "contents" seems to be a matter of mystery. In a recent publication devoted to explaining the USA PATRIOT Act's impact on electronic surveillance, the Justice Department author explains that "[a]gents and prosecutors with questions about whether a particular type of information constitutes content should contact the . . . Computer Crime and Intellectual Property Section . . . ."[412]

---

405. *Id.* § 3123(a)(2).
406. *See id.* § 3123(a)(3), (B); *supra* Part III.D.3.
407. Pub. L. No. 107-56, § 224, 115 Stat. 272, 295 (2001).
408. *See, e.g.*, S. 2476, 108th Cong. (2004).
409. *See supra* notes 259, 275-78 and accompanying text.
410. *See supra* note 255 and accompanying text.
411. *See* DOJ SEARCH MANUAL, *supra* note 317, at 59; *see also* Kerr, *supra* note 103, at 645-47 (acknowledging the ambiguity of "contents" under the statute).
412. *See DOJ Field Guidance*, *supra* note 279, at 1234. Curiously, the article directs the inquiring prosecutor to contact the DOJ Section which purports to be the author of the publication. *See id; see also* DOJ SEARCH MANUAL, *supra* note 317, at 112 (directing prosecutors or agents to contact the same group if they encounter "debate about the distinction between addressing information and content").

Perhaps the government has avoided public statements about the actual boundary between contents and attributes because of concern about how the public might react to learning that online information has so little privacy.[413] The Justice Department apparently views *all* information that is not contents as available under the weak attribute regulations. Its training manual describes the stored attributes protections as "a catch-all category that includes all records that are not contents."[414] Similarly, its field guidance memo claims that "pen register and trap and trace devices may obtain any non-content information."[415] If that is true, then the government may obtain detailed information that reveals people's online activities after obtaining a subpoena or a court order that is either a rubber stamp or which uses a simple relevance test.[416] The training materials specify that detailed log files revealing a "person's entire online profile" may be obtained under the anemic attribute protections.[417]

The government currently claims that what I have called web traffic data, or records of all that we do online, receive only the weak protection accorded communication attributes.[418] The only way to avoid that result would be if there were a third category of information, perhaps less protected than contents, but more protected than attributes. However, when questioned, a high level Justice Department official denied the existence of a third category of online information, stating that the Justice Department views all online information as either contents, which is narrowly defined, or as readily-available attributes.[419]

Besides having dire consequences for privacy on the Internet, the insistence that online information falls into only two categories derives from two historical artifacts. First, when lawmakers stressed the need to protect the *contents* of communications in the years leading up to the Wiretap Act, they intended to rebut arguments that communication contents were too intangi-

---

413. *See* Swire, *supra* note 17, at n.13 (suggesting this possibility); *see also* 147 CONG. REC. S10372 (daily ed. Oct. 9, 2001) (statement of Sen. Leahy) ("[T]he FBI and Justice Department are short-sighted in their refusal to define" the terms "content," "routing," and "addressing" in the USA PATRIOT Act.); Howell, *supra* note 404, at 1197 (discussion the administration's refusal to define terms).

414. DOJ SEARCH MANUAL, *supra* note 317, at 91.

415. *DOJ Field Guidance*, *supra* note 279, at 1234. Historically, trap and trace devices obtained the numbers of those who dialed a particular phone, rather than the numbers that telephone dialed. Their modern incarnation is Caller-ID.

416. *See supra* Part III.B.2.

417. *See* DOJ SEARCH MANUAL, *supra* note 317, at 59-60 (explaining that "detailed internet address of sites accessed" and a "person's entire online profile" may be obtained).

418. *Id.* at 63.

419. The Chairman of the Subcommittee on the Constitution of the House Judiciary Committee submitted the following written questions to Assistant Attorney General Viet Dinh: "[I]s it your understanding that all non-'content' information is 'dialing, routing, addressing, and signaling' information [under the pen register provisions] . . . ? Or is there a third category of information . . . ? If there is such a third category of information, what statutory provisions or Department rules and procedures govern its collection by the Department of Justice?" He received the following answers: "The Department of Justice interprets the phrase 'dialing, routing, addressing, and signaling information' . . . as complementary to the term 'contents' . . . . Further, we do not believe that there exists a third category of information which is not comprehended by either 'contents' or 'dialing, routing, addressing, and signaling information.'" *Antiterrorism Hearings*, *supra* note 201, at 63-64.

ble to warrant protection. The Supreme Court had previously specified that communication contents were protected, though intangible. The Court had focused on the contents of communications because that is what wiretapping revealed, not to distinguish them from less protected attributes.[420]

By the same token, support for just two categories cannot be found in the original Wiretap Act. The 1968 Act did not distinguish protected contents from less-protected attributes. Rather, the Act defined "contents" so broadly that it included the identity of the parties and the mere existence of the communication, both of which are now considered attributes.[421] The notion that information counts as either contents or non-contents is a modern, aggressive interpretation.

The government claims that support for this distinction can be found in *Smith v. Maryland*, but overreads that case.[422] *Smith* denied Fourth Amendment protection to the telephone numbers dialed, but it had nothing to say about a huge range of attributes; in fact, the pen register it considered recorded numbers on a paper tape, and did not even reveal whether the call went through, let alone how long it lasted or any of the other attributes now available.[423] Certainly the Court did not consider, in 1979, the constitutional status of web traffic data.[424] Though *Smith* supports the denial of constitutional protection for telephone numbers, it in no way supports the dichotomy between contents and non-contents that the Justice Department urges.

The truth is that the current categories of the ECPA do not cover web traffic data.[425] At least one other category of protection is needed. Search terms entered, web-pages visited, and items viewed are neither message contents nor their to/from information.[426]

When the Justice Department does recognize a third category, it is the category of online information utterly unprotected by the ECPA.[427] As discussed, the Justice Department views e-mails that have been opened on a system that does not offer e-mail services to the public as falling entirely

---

420. *See supra* Part II.B.2; note 257 and accompanying text.

421. *See supra* note 76 and accompanying text.

422. Viet Dinh, the Justice Department Official credited with designing the USA PATRIOT Act amendments, told Congress: "Of course, the Supreme Court has long held that non-content information is not protected by the Fourth Amendment." *Antiterrorism Hearings*, *supra* note 201, at 7.

423. *See* Smith v. Maryland, 442 U.S. 735, 736 n.1, 741-42 (1979); United States v. New York Telephone Co., 434 U.S. 159, 167 (1977).

424. *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 508-10 (S.D.N.Y. 2004) (rejecting the extension of *Smith* to internet records and hypothesizing a different result in *Smith* if the pen register had gathered online data).

425. *But cf. In re* Pharmatrak, Inc., 329 F.3d 9, 18 (1st Cir. 2003) (finding possible interception when online tracker obtained the contents of completed online forms as they were transmitted, and finding the definition of "contents" to include "personally identifiable information such as a party's name, date of birth, and medical condition").

426. *See* Dempsey, *supra* note 159, at 83 ("[T]ransactional data has evolved into a third, hybrid type, providing detailed information about a person's habits of association and commerce.").

427. If the ECPA offered no protection, then there would be the possibility of common law protection, but tort claims regarding online privacy have not fared well. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Penn. 1996) (finding no reasonable expectation of privacy by an employee on an employer's computer).

outside of the ECPA's protection.[428] In that vein, Professor Orin Kerr, who worked for the Justice Department and helped them formulate their online surveillance policies, has written that online information which is neither contents, nor dialing, routing, addressing, and signaling information is unprotected by the surveillance laws.[429] Courts have found information such as electronic cookies and other files stored on personal computers to be outside the protections of the ECPA.[430] Considered in that light, treating web traffic data as communication attributes may be preferable to the alternative of no protection.[431]

The government ignores a much better way to handle surveillance practices not covered by the ECPA when it argues that they are unregulated. Courts could follow the lead of the appellate courts who adopted the core requirements of the original Wiretap Act to cover video surveillance. Starting in 1984, federal appellate courts considered which legal requirements pertained to the use by government agents of secret video surveillance when the Wiretap Act failed to mention this practice. All federal appellate courts to consider the question, including the courts of seven circuits, determined (largely by analogy) that in those contexts in which the subjects of video surveillance entertain a reasonable expectation of privacy, they must be accorded the core protections of the Wiretap Act.[432] After finding constitutional searches in secret government videotapings of homes, offices, hotel rooms, public restroom stalls, and even yards visible to the public, the circuit courts found several provisions of the Wiretap Act to satisfy the constitutional requirements for the video surveillance.[433] The courts required that video surveillance be used only as a last resort, that agents minimize the interception of non-incriminating images, and that applications satisfy the

428. *See supra* notes 323-29 and accompanying text.

429. Kerr, *supra* note 103, at 645-47. *But see* Swire, *supra* note 17, at n.13 (disagreeing with Kerr on the ground that the Constitution might have protected some of the information). Kerr worked in the Computer Crime and Intellectual Property Section ("CCIPS") of the DOJ and contributed to the proposals that became the USA PATRIOT Act amendments. He is also credited with the analysis and organization of the CCIPS training manual on online surveillance. *See* DOJ SEARCH MANUAL, *supra* note 317, at 5.

430. *See* United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) (finding no protection under the stored contents provisions for files grabbed by a hacker and calling that failure a "legislative hiatus in the current laws purporting to protect privacy in electronic communications"); *In re* Doubleclick, Inc., 154 F. Supp. 2d 497, 511-13 (S.D.N.Y. 2001) (deciding that "cookie identification numbers" are not in electronic storage and therefore are not covered by the ECPA because they reside on individual users' computers).

431. On that basis, Professor Kerr argues that the USA PATRIOT Act amendments that extended use of pen registers to the Internet actually improved privacy. *See* Kerr, *supra* note 103.

432. *See, e.g.*, United States v. Torres, 751 F.2d 875 (7th Cir. 1984); United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987); United States v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990). Unlike the other circuits, the Ninth Circuit did not extend the Wiretap Act provisions by analogy, but rather found that they literally applied to video surveillance because the Wiretap Act was designed to be inclusive. *See* United States v. Koyomejian, 946 F.2d 1450, 1453-54 (9th Cir. 1992).

433. *See* Kent Greenfield, *Cameras in Teddy Bears: Electronic Visual Surveillance and the Fourth Amendment*, 58 U. CHI. L. REV. 1045, 1057 (1991).

particularity requirements.[434] Though Congress omitted video surveillance from the ECPA, the House Report accompanying the Act spoke approvingly of the appellate courts' approach.[435]

There are still other ways to regulate surveillance practices that are not clearly covered by the ECPA. One is to apply a simple warrant requirement, which the Supreme Court did for a pen register investigation in 1977, two years before *Smith v. Maryland* and during a period when the Wiretap Act did not cover pen registers.[436] The Court assumed—without holding—that the Fourth Amendment governed pen registers, and therefore found a simple warrant to be adequate, even though the warrant regulations did not mention pen registers.[437]

Moreover, one could treat surveillance techniques that do not fit within the parameters of the ECPA as wholly prohibited until authorized by Congress. In the case just mentioned, three justices dissented on the ground that pen register investigations were wholly prohibited in the absence of Congressional authorization.[438] In the video surveillance cases, the defendants claimed that the practice was entirely prohibited, the government claimed it was utterly unregulated, and the Courts chose a middle ground of imposing the super-warrant requirements.[439]

Something must be done about web traffic data. But treating it as unprotected, or protected by the minimal requirements of the pen register or stored attribute provisions, is the wrong choice.[440] In fact, as I argue next, there is no reason in principle not to accord web traffic data the same high protection as that accorded to the content of telephone calls under the Wiretap Act.[441]

---

434. *See, e.g.*, *Torres*, 751 F.2d at 883-84; *Biasucci*, 786 F.2d at 510; *Cuevas-Sanchez*, 821 F.2d at 251-52. In *Cuevas-Sanchez*, the Fifth Circuit called the government's argument "sophistry" when it claimed that the videotaping did not violate the target's reasonable expectation of privacy in his fenced backyard, because a person looking over the fence or a lineman on the power pole could have observed the same things. *Id.* at 250. The court reasoned that if the scene were truly visible without surveillance, then the government would not have been able to justify the use of such an intrusive technique. *See id.*

435. *See* H.R. REP. NO. 99-647, at 18, 18 n.11 (1986) (approving of this approach as an effort to provide "legal protection against the unreasonable use of newer surveillance techniques"); *see also id.* at 36 (approving of the court-derived rules).

436. *See* United States v. New York Tel. Co., 434 U.S. 159, 165-68 (1977).

437. *Id.* at 165 n.7, 167-70; *see also* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1298-1303 (2004) (advocating a warrant requirement for pen registers).

438. *Id.* at 178-87 (Stevens, J., dissenting). The ECPA authorized pen registers in 1986. Similarly, Congress considered the possibility that the lack of statutory guidance on surveillance of electronic communications could "expose law enforcement officers to liability and . . . endanger the admissibility of evidence." S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

439. *See* United States v. Koyomejian, 946 F.2d 1450, 1453-54 (9th Cir. 1992) (reviewing the three choices).

440. *See, e.g.*, Peter P. Swire, *Administration Proposal Hits the Right Issues but Goes Too Far*, Brookings Terrorism Project Website, *available at* www.peterswire.net (Oct. 3, 2001) (advocating that instead of the vague language in the USA PATRIOT Act, Congress should follow the recommendation of James X. Dempsey and clarify that search terms, URL's, and other transactional information may not be acquired under pen register authorization).

441. *Accord* Gavin Skok, *Establishing A Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61 (1999-2000) (arguing that instead of applying a reasonable expectation of privacy test to web traffic data, courts should recognize that warrantless searches of such

IV. REMEMBERING THE LESSONS OF THE WIRETAP ACT

I have argued that the Wiretap Act did a better job regulating traditional electronic surveillance than the ECPA does regulating online surveillance. In particular, I have argued that the Wiretap Act adopted sensible approaches to handling the challenges of electronic surveillance, approaches that the ECPA largely lacks. Three counter arguments present themselves. One is that the balance lawmakers have struck for online surveillance under current law, though it favors the government over privacy, is better than the one struck in 1968. The second is that there are meaningful differences between traditional telephones and the Internet that counsel against online privacy. The third is that while online privacy may be important, we should sacrifice it now to protect security. I address those arguments in this Part, starting with an evaluation of the balance struck in 1968.

A. The Wiretap Act in History

A solid case can be made that the Wiretap Act represents a superior piece of legislation due to the context in which it was enacted. Congress passed the Wiretap Act at the height of social concern about electronic surveillance and with the engagement of the public and all branches of government. While it was pending, leaders of the executive branch, including the President and the Attorney General, made public statements about electronic surveillance.[442] In 1967, a presidential commission presented a lengthy and divided report to Congress on the issue.[443] That same year, the Supreme Court weighed in with two comprehensive decisions that gave considerable guidance on the constitutional prerequisites for electronic surveillance;[444] that is not to mention the hundreds of cases during the prior thirty-four years in which federal and state courts opined on electronic surveillance practices. Even state legislatures experimented with electronic surveillance legislation during the preceding decades, with some prohibiting it, some permitting it, and some taking positions in the middle.[445]

The provisions of the Wiretap Act were thoroughly vetted. During the years leading up to the Wiretap Act, Congress considered numerous bills and held extensive hearings on electronic surveillance.[446] During the year

---

data violate the Fourth Amendment's fundamental prohibition on general warrants).

442. *See supra* note 82.

443. *See* 1967 PRESIDENT'S COMMISSION, *supra* note 39. The Commission report generated substantial commentary as well. *See, e.g.*, THE CHALLENGE OF CRIME IN A FREE SOCIETY: PERSPECTIVES ON THE REPORT OF THE PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND THE ADMINISTRATION OF JUSTICE (Leonard W. Levy ed., 1971).

444. *See, e.g.*, United States v. Donovan, 429 U.S. 413, 426-27 (1977) (detailing the history of the Wiretap Act and its drafters' efforts to reflect Supreme Court guidance).

445. *See generally* DASH, *supra* note 1 (studying each type of jurisdiction).

446. A national lawyer's group documented nine congressional hearings in the ten years preceding the Wiretap Act, with several hearings spanning several hundred pages of testimony. *See* 1968 ABA STANDARDS, *supra* note 203, app. E (collecting relevant sources); *see also* LAPIDUS, *supra* note 3, at 11 (reporting that there were at least sixteen sets of hearings in Congress about electronic surveillance

prior to the Wiretap Act's passage, Congress heard from hundreds of witnesses and debated an administration-supported alternative bill that would have permitted electronic surveillance only in national security investigations.[447] Numerous law review and popular articles canvassed the issues.[448] One can hardly imagine Congress having had more input. The 1968 Wiretap Act, though not perfect, represented our lawmaking system's best effort to address an issue of crucial social significance.

The ECPA's pedigree bears little resemblance to that of the Wiretap Act. Although there were a few hearings, there was nothing like the social engagement informing the Wiretap Act.[449] The public was largely unaware of the privacy implications of developing technologies, and groups advocating online privacy had yet to be born.[450] Congress drafted the ECPA in 1986, several years before the World Wide Web appeared and the Internet became popular.[451] The law arrived before courts had even considered online surveillance.

The subsequent substantive amendments did not improve on this process. There was relatively little public involvement in the passage of CALEA, which was instigated by the Justice Department amid fears that new digital technologies would hinder surveillance.[452] The USA PATRIOT Act was passed just six weeks after the September 11 attacks, during a period in which legislators were literally shut out of their offices due to anthrax attacks.[453] Commentators have complained about the limited deliberation that preceded the USA PATRIOT Act, which was passed despite the fact that members of Congress did not have a chance to view the actual text.[454] In short, the current law on electronic surveillance does not reflect the considered deliberative process that produced the Wiretap Act. Given the signficant flaws in the modern law, it is time to draw lessons from the earlier legislation.

---

between 1934 and 1967).

447. Ten days of hearings were held during 1967, with 41 witnesses testifying. Prior to that there had been 35 days of hearings with over 200 witnesses testifying. *See* S. REP. NO. 90-1097, at 134 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2222, 2223 (individual views of Sen. Long and Sen. Hart).

448. Many articles about the debate over electronic surveillance appeared in both law reviews and popular periodicals during the decade or so preceding the Wiretap Act. *See supra* note 203.

449. The ECPA's legislative history discloses a few days of hearings in the years leading up to the ECPA. H.R. REP. NO. 99-647, at 28 (1986); S. REP. NO. 99-541, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3558.

450. The online privacy groups were just beginning to be politically active in 1994. *See* Freiwald, *supra* note 224, at 1008-10.

451. *See supra* note 222.

452. *See* Freiwald, *supra* note 224, at 975-89, 1007-19.

453. *See* Howell, *supra* note 404, at 1162-63, 1175-76.

454. *See Antiterrorism Hearings*, *supra* note 201, at 3 (statement of Rep. Nadler) ("Members had to vote on a multi-hundred page bill, with no one having had a chance to even read the bill, except for staffs. The bill was available an hour in advance. People had to vote based on summaries."); *see also* Howell, *supra* note 404 (describing the intense pressure from the administration to pass a law quickly).

B. Privacy on the Internet

Under current Justice Department interpretations, most online surveillance today proceeds without meaningful judicial review. Given its appeal to law enforcement, the lack of both formal and practical regulation of government monitoring of our online lives should provoke substantial concern. In fact, because it provides little protection from unjustified online surveillance by the government, the current system is untenable.[455]

On the other hand, if for some reason privacy is inappropriate on the Internet, then the current chaotic system may be maintained. Though few say it outright, some judges and commentators seem to view the Internet as a forum where privacy has no place. The notion that we have no expectation of privacy online, either because we know that communications are easily monitored or because we voluntarily involve third parties in our communications, reflects that view.[456]

The most significant problem with the claim that we have no expectation of privacy online is that it does not match up with our behavior and our feelings. Available evidence does not suggest that we have abandoned the notion of privacy online and assumed the risk that all we say may be recorded and reviewed by government agents. Instead, people seem to be of the same two minds they were in the 1950s. They worry about the possibility of monitoring, but then they dismiss the concerns and proceed without thinking about it.[457] The use of passwords and the fact that many people access the Internet from the privacy of their homes or offices may encourage them to believe that what they do online is their own business. It seems clear that Internet users want and expect some privacy in their online communications.[458]

The government contributes to the belief in online privacy. In fact, some statements made by executive branch officials to the public and Congress seem to be affirmatively misleading. For example, officials consistently reaffirm that the law exerts meaningful limits on online surveillance because it requires that agents justify their surveillance before a reviewing court.[459]

---

455. State and local agencies may lack resources and technological sophistication for extensive monitoring, but not federal agencies. Kennedy and Swire, *supra* note 150, at 983-85 (expressing concern about several states' agents' lack of training and sophistication regarding electronic surveillance as compared to federal agents).

456. Professor Orin Kerr has been the most vocal proponent of this view, though he does claim to recognize some limited privacy rights in online information. *See, e.g.*, Kerr, *supra* note 363, at 811-14.

457. *See supra* notes 6, 7; Schwartz, *supra* note 19, at 1645-46 (describing these behaviors).

458. *Information Privacy Hearings*, *supra* note 6, at 5 (testimony of Lee Rainie) (reporting that most Internet users feel anonymous online, and "[i]f they could craft a Golden Rule for the Internet, it would be: 'Nobody should know what I do on the Web or anything else about me unless I say so'").

459. Assistant Attorney General Viet Dinh told Congress that "law enforcement must get court approval before installing a pen register. And now, as before, law enforcement must show that the information sought is relevant to an ongoing investigation." *Antiterrorism Hearings*, *supra* note 201, at 13. The statement implies that judges may refuse to approve the application if a proper showing is not made, which conflicts with the Justice Department's training material. DOJ SEARCH MANUAL, *supra* note 317,

A public education campaign that informes citizens of their actual lack of online privacy would help with the problem of mismatched perceptions, but it is not the answer. If the public were made fully aware of the possibility of extensive government monitoring, they would undoubtedly curb their online activities.[460] If we inhibit our speech and our political activities because we believe we are open to view, then we will have lost much. The Internet has received due praise as a great boon to participatory democracy, and if it becomes a realization of Orwell's big brother surveillance state instead, that will be a great loss.[461]

The central normative question concerns whether the Internet should be as private as the traditional telephone network. Let me briefly suggest some reasons why it should. Internet communications increasingly replace telephone calls, as people make their calls using Voice Over IP technology.[462] There is no reason that using the Internet protocol should reduce the privacy protection for traditional telephone calls, but it likely would under current law.[463] Apart from that, we reveal more of ourselves online than on the telephone, because we are more clearly identified with our internet activities via our password-protected accounts. We transmit much richer information online than offline; in addition to conversations, we send pictures, videos, songs, and long documents. We also create records of our activities when we shop, read, play, organize, and date online. We cannot do everything online that we can offline, but we can do most things, and some things we can do online only. The drafters of the Wiretap Act were concerned about the privacy of information over traditional telephone lines; we should be dramatically more concerned about the privacy of our online information. If the online world is to be more than a mere high-tech shopping center, we must not let it turn into a forum open to government view.[464]

C. Privacy in the Modern Age

Some might claim that neither the Internet nor traditional telephone calls should be private today. They would say that in our modern era, the value of privacy itself has dramatically decreased, as we have become accustomed to living our lives subject to the watchful eyes of others. With the near ubiquity of video cameras that watch us in public, of affinity cards that

---

at 59 (stating that judges "will authorize" applications with the required elements, without conducting "an 'independent judicial inquiry'").

460. *See supra* note 114.

461. *See, e.g.*, Reno v. ACLU, 521 U.S. 844, 850 (1997).

462. *See, e.g.*, Daniel Roth, *Catch Us if You Can*, FORTUNE, Feb. 9, 2004, at 65 (describing current plans to replace all telephone calls with internet-based calls); Peter P. Swire, Katz *is Dead, Long Live* Katz, 102 MICH. L. REV. 904 (2004) (predicting that there will be no practical difference between wiretapping and stored records searching when telephone calls take place over the Internet).

463. Wire communications are limited to "aural" transfers. 18 U.S.C. § 2510(1) (Supp. I 2001).

464. *See* Skok, *supra* note 441, at 86 (coming to the same normative conclusion); *see also* Schwartz, *supra* note 19, at 1674-75 (worrying about the impact of a lack of privacy on the democratic potential of the Internet).

remember our purchases, of intelligent vehicle traffic systems that track our travels, and of electronic monitors in the workplace that record our keystrokes, perhaps the idea of privacy has become antiquated, and rightly so.[465] This perspective would recommend applying the weak protections of the ECPA to telephone calls rather than extending the strong protections of the Wiretap Act to the Internet.

It is beyond the scope of this Article to justify the need for privacy, one of the most cherished of the protections that the Bill of Rights affords.[466] But I will briefly take up the argument that privacy must yield to the dangers posed by modern terrorism. Most importantly, fear does not yield the careful thinking that should guide legal policy. For example, the fear that privacy must be reduced or there will be blood on our hands when another terrorist attack occurs generates high emotion rather than reasoned deliberation.[467] Short-lived emotional reactions should not guide legislation designed to last. It seems clear that the terrorist threat will plague us for the foreseeable future. Realigning our rights to contend with terrorism must work in the long-term rather than be a short-term fix.[468]

We feel palpably the threat from terrorism today, but this is not the first time our country has feared attack. In World War II, we lived in fear of saboteurs, and sustained a brutal attack on Pearl Harbor.[469] Nonetheless, the law that made wiretapping illegal for all purposes persisted through that period. Subsequent to the war, we grew concerned about infiltration from communists and about nuclear attack, and yet we maintained our wiretapping prohibition.[470] Even post-September 11, few have suggested that we do away with our wiretapping restrictions for the telephone network.

Moreover, just as the balance between privacy and law enforcement must be carefully analyzed, so must the perceived trade-off between privacy and security from terrorism.[471] As a threshold matter, it is likely that most, if

---

465. Interestingly, two high-tech entrepreneurs, Scott McNealy and Larry Ellison have been vocal proponents of this perspective. *See, e.g.*, ROSEN, *supra* note 5, at 111-29.

466. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("[The framers] sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."). For some sources that may well convince non-believers to value privacy see TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, *supra* note 28; WESTIN, *supra* note 15; and Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

467. Attorney General Ashcroft told lawmakers that "blood would be on their hands" if another terrorist attack occurred before they passed the version of the USA PATRIOT Act he promoted. James A. Barnes et al., *Justice: From the Ashes of 9/11: Big Bad John*, 35 NAT'L J. 4, 255 (Jan. 25, 2003).

468. *See generally* PHILIP B. HEYMANN, TERRORISM FREEDOM AND SECURITY: WINNING WITHOUT WAR (2003) (arguing that a war metaphor conveys a false sense of a short-term situation).

469. Several authors have argued that Americans have reacted disproportionately and irrationally to the risk of terrorism after 9/11. *See, e.g.*, SCHNEIER, *supra* note 57, at 246-51; ROSEN, *supra* note 5, at 8, 34; Cass R. Sunstein, *Probability Neglect: Emotions, Worst Cases, and Law*, 112 YALE L.J. 61, 100 (2002).

470. *See* Rotenberg, *supra* note 60, at 1135.

471. *See supra* notes 57-60 and accompanying text; *see also* Doe v. Ashcroft, 334 F. Supp. 2d 471, 508-10 (S.D.N.Y. 2004) (rejecting the government's use in terrorism investigations of National Security Letters without judicial review).

not all, terrorism investigations would be unaffected by any changes making online surveillance law more consistent with wiretapping law. Much of the surveillance to protect against threats to national security proceeds under the Foreign Intelligence Surveillance Act of 1978 ("FISA"), rather than the Wiretap Act and the ECPA.[472] As for law enforcement surveillance, even the Wiretap Act incorporates an emergency provision that suspends the need for judicial review for a short period when necessary.[473] Those provisions have always been part of electronic surveillance law.[474] Moreover, the Wiretap Act permits extensive surveillance of those who are suspected of serious crimes.[475] Requiring a law enforcement agent to make her case to a judge before rooting through our electronic information does not mean making the information inaccessible. It is hard to imagine that law enforcement investigators would not have sufficient justification to conduct electronic surveillance of those it suspects of terrorist activities. The question is whether they can search through the electronic information of those they have no reason to suspect of illegal activity, in the hopes of finding a needle in a haystack.[476]

The lack of privacy for online information derives from complex and outdated provisions, aggressive interpretations by law enforcement, and the lack of an engaged public, Congress, and judiciary. Because differences in the medium and the modern age do not justify the weak protection for online privacy, we should build on the lessons of the Wiretap Act in the context of online surveillance.

V. FROM WIRETAPPING TO VIDEO SURVEILLANCE TO ONLINE SURVEILLANCE

Before they extended the Wiretap Act's protections to the video surveillance context, appellate courts identified the chief constitutional infirmities of electronic surveillance: it is intrusive, it is continuous, it is indiscrimi-

472. Under the USA PATRIOT Act, foreign surveillance investigations no longer need to satisfy the Wiretap Act or the ECPA, they are governed entirely by FISA. *See* 18 U.S.C. § 2511(2)(f) (1993 & Supp. I 2004); *supra* note 118. Also, the stored records provisions have a special provision authorizing special procedures for release of information to the FBI for foreign intelligence investigations. 18 U.S.C. § 2709 (1993 & Supp. I 2004).

473. 18 U.S.C. § 2518(7) (1993) (defining emergency situations as involving the danger of death or serious physical injury, organized crime conspiracies, or conspiracies that threaten national security); 18 U.S.C. § 3125 (providing for emergency pen registers) (1993 & Supp. I 2004). Both provisions permit law enforcement to use wiretaps or pen registers for 48 hours before obtaining a court order, provided that they would otherwise qualify for a court order. The USA PATRIOT Act added provisions that permit service providers to disclose stored communications in the event of an emergency. 18 U.S.C. § 2702(b)(8), (c)(4) (Supp. I 2004).

474. *See* 18 U.S.C. § 2518(7) (1968) (providing a similar form of the emergency provision, except lacking coverage of emergencies that pose a danger of death or serious physical injury). By the same token, the changes proposed in the wake of the September 11 attacks were proposals that the FBI had long wanted, rather than a response to the new threat. *See* SCHNEIER, *supra* note 57, at 250-51.

475. 18 U.S.C. § 2516 (1993 & Supp. I 2004).

476. *See* SCHNEIER, *supra* note 57, at 162-63, 243-51 (describing massive data mining schemes as vastly wasteful, unproductive, and threatening to privacy and safety).

nate, and it is hidden.[477] The courts considered video surveillance to be even more in need of restriction than wiretaps, because it engages more of the senses than wiretaps. While wiretaps uncover conversations, video surveillance reveals the actions—even facial expressions—of its targets.[478] By "continuous," the courts meant that, in comparison to a one-shot search, video surveillance collects information over a period of time.[479] Video surveillance is "indiscriminate" in the sense that, again unlike a traditional search and like wiretapping, video surveillance does not merely disclose the target's incriminating information, but also the target's non-incriminating information, as well as information about those innocent parties for whom there is no probable cause to suspect wrongdoing.[480] The "hidden" nature of video surveillance needs no further elaboration, except that the inability to hide video cameras effectively prior to 1968 likely explains why Congress omitted video surveillance from the Wiretap Act.[481] By the mid-1980s video cameras could be hidden from view.[482] With all those features in common with wiretaps, the appellate courts agreed to extend the significant restrictions in the Wiretap Act to protect against abuse of video surveillance by government agents.[483]

Dynamic content interceptions online clearly share those privacy-invading features. They reveal intrusively, continuously, and in a hidden manner all of the target's online correspondence.[484] They are indiscriminate, particularly if the investigation seeks e-mails sent to the target as well as e-mails sent by him. The significant parallels among wiretapping, video surveillance and dynamic content interceptions demonstrate the irrationality of the current weaker protections for electronic communications, especially the lack of a statutory exclusionary rule for victims of unlawful online surveillance.[485] Government agents should have to satisfy the same strict standards when they obtain electronic communications as they do when obtaining telephone communications.[486] In addition, the current stringent limitations

---

477. *See* United States v. Torres, 751 F.2d 875, 882-84; United States v. Koyomejian, 946 F.2d 1450, 1457 (9th Cir. 1992); United States v. Taketa, 923 F. 2d 665, 677 (9th Cir. 1991) (finding warrantless government video surveillance to be "exceptionally intrusive" and finding that "the silent, unblinking lens of the camera was intrusive in a way that no temporary search . . . could have been").

478. *See, e.g.*, *Torres*, 751 F.2d at 891 (Cudahy, J., concurring).

479. *Id.* at 884-85.

480. *Id.*

481. *See supra* note 230.

482. *See Torres*, 751 F.2d at 877 (describing the use of television cameras in the homes of suspected terrorists in 1983).

483. *See, e.g.*, Greenfield, *supra* note 433; Ric Simmons, *Can* Winston *Save Us From Big Brother? The Need for Judicial Consistency in Regulating Hyper-Instrusive Searches*, 55 RUTGERS L. REV. 547, 556-64 (2003).

484. *See, e.g.*, 1968 ABA STANDARDS, *supra* note 203, at 4 (finding modern forms of electronic surveillance to be more intrusive than traditional forms).

485. *See, e.g.*, Kerr, *supra* note 363 (advocating the availability of a statutory suppression remedy for electronic communications); Leib, *supra* note 361, at 410-11 (advocating the same and describing the concurring views of the drafters of the ECPA who eventually yielded to Justice Department demands that electronic communications be easier to obtain).

486. If Congress extends the Wiretap Act protections to online surveillance it should also consider proposals to improve on those provisions. *See generally*, LAPIDUS, *supra* note 3, at 6 (quoting a reporter

on what counts as dynamic content interceptions are indefensible. Just as we retain law enforcement powers in the wake of new technological developments, we must retain the protections against abuse of those powers.[487] Otherwise, we permit technology to be a one-way ratchet that enhances law enforcement power at the expense of privacy.[488]

A dynamic content interception is not the only type of online surveillance that shares the features of wiretapping and video surveillance. E-mails that have been retrieved by their recipient and saved present an intrusive view into an online life.[489] When monitors gain access to stored e-mails, they effectively conduct continuous surveillance for the period that the correspondence spans. Online surveillance of stored e-mails can be at least as hidden as wiretapping, if not more. Finally, it seems at least as likely that acquisition of stored e-mails will be indiscriminate in the sense that it discloses information about innocent people or innocent activities. Overall, extending the protections of the Wiretap Act to stored communications seems justified.[490] By the same token, while digital technology offers the capacity to filter information, that capacity suggests that a minimization obligation would be easy to meet, not that it should not be imposed.[491]

Of course, a dividing line between information that is private and information open to the public needs to be maintained in the Internet context. At the same time, considerable thought must be given to how to handle the role of non-government third parties in conducting online surveillance. Although service providers gather extensive records of online activities in the course of their businesses, those records take on a very different hue in the hands of government monitors. To the extent they offer an alternative to

---

who claimed the Wiretap Act allowed "too many people to listen in on too many conversations for too long a time in too many types of cases"); *see also id.* at 208-20 (proposing changes to clarify the Wiretap Act and to strengthen its privacy protections); Dempsey, *supra* note 159, at 75-77, 111-15 (describing erosion of Wiretap Act protections over time and recommending specific improvements).

487. Congress justified both CALEA and the USA PATRIOT Act as necessary to prevent new technology from eroding law enforcement surveillance.

488. I do not address here the issue of which institution—the judiciary or the Congress—is better suited to update the laws pertaining to online surveillance. Similarly, I do not resolve whether such changes are constitutionally required or policy choices. If the former, then the courts would have to confront how to define a reasonable expectation of privacy online, or, better, abandon that inquiry and engage in a more direct normative assessment of privacy online. *See supra* Parts II.D.4 and III.D.4 (critiquing the reasonable expectation of privacy test); *see also* Freiwald, *What a Comparative Institutional Analysis of Online Surveillance Reveals* (symposium draft 2004) (discussing the question of institutional choice).

489. *See* Konop v. Hawaiian Airlines, 302 F.3d 868, 890 (9th Cir. 2002) (Reinhardt, J., dissenting) (recognizing that electronic service providers "have possession and control over large amounts of stored electronic communications" and are "an obvious source for law enforcement authorities who seek to obtain the contents of electronic communications").

490. *Cf.* Dempsey, *supra* note 159, at 88 (questioning the minimal protection for communications in storage); Berman and Mulligan, *supra* note 280, at 569-71; Mulligan, *supra* note 319.

491. *See* Dempsey, *supra* note 159, at 87 (recommending that service providers filter electronic communications before providing them to law enforcement agents); *see also* Downes, *supra* note 75, at 266-69 (arguing that giving law enforcement agents discretion to filter electronic communications violates the constitutional ban on general warrants).

actual monitoring, third party records should not provide an end run around surveillance restrictions.[492]

Many would question whether the wiretapping analogy extends to communication attributes, either stored or seized dynamically, because the cases tell us that their acquisition is not intrusive. However, that analysis has relied on the fact of interceptibility, which is the wrong approach because it assumes voluntariness where there is none and permits developing technology to erode privacy.[493] As a normative matter, communication attributes, especially rich electronic attributes, deserve substantially more privacy protection than they now receive.[494] The acquisition of attributes is intrusive, and it certainly matches the other characteristics of being continuous, hidden, and indiscriminate. In fact, web traffic surveillance, or monitoring that discloses one's online movements, seems to represent a hybrid of telephone and video surveillance and shares all the privacy-invading features of both.[495]

Government surveillance of electronic information raises the same concerns that motivated the enhanced protections for both wiretapping and videotaping. Online surveillance should merit the same restrictive regulations as those more low-tech techniques. The significant exception would be subscriber information that does not reveal activities over a period of time—a lower level of protection for that information seems justified.

It has long been understood that the current framework for protecting the privacy of online information is woefully inadequate. Members of Congress have clearly recognized the need to reform some of the most egregious problems with the protection of online communications. For example, a year before the September 11 attacks, the House Judiciary Committee approved "The Electronic Communications Privacy Act of 2000."[496] If passed, the law would have made the suppression remedy available for unlawful interceptions of electronic communications and unlawful acquisi-

---

492. *See supra* Part II.D.1 (discussing use of private entities to circumvent legal prohibitions against wiretapping). For an example, see United States v. Allen, 53 M.J. 402, 404-10 (U.S. C.A.A.F. 2000). The military court found no statutory or constitutional problem when an ISP "freely and voluntarily" disclosed to the government the (child pornographer) defendant's "multiple page listing of online services accessed." *Id.* at 410, 405. Instead of requiring a warrant or ECPA court order, the ISP had merely asked for a "lawyer request." *Id.* at 404.

493. *See* Bellia, *supra* note 216 (severely criticizing the reasoning behind depriving online information of privacy because third parties may access it); *Cf.* Mulligan, *supra* note 319 (criticizing the rule in the context of stored records).

494. *See* Solove, *supra* note 437, at 1298-1303 (advocating that a warrant be required for almost all electronic surveillance); Dempsey, *supra* note 159, at 113-14 (advocating that the standard for judicial review be more rigorous); *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1607-08 (1997) (advocating a normative finding of privacy in online communications).

495. *See, e.g.*, Kang, *supra* note 28, at 1195-99 (analogizing travels through cyberspace to activities in a physical place, but with cyberspace activities yielding more personal data); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439 (2003) (critiquing the analogy of cyberspace to a physical place); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521 (2003) (same).

496. H.R. 5018, 106th Cong. (2000); *see also* Howell, *supra* note 404 (describing similar proposals promoted by Senator Leahy).

tions of stored contents and substantially increased the judicial review of pen register applications.[497] The law would also have ruled out some of the most aggressive interpretations of the ECPA by clarifying that e-mail retains the same protections even after being read.[498] Though the proposed law would not have brought all forms of electronic communications up to the level of the Wiretap Act, it would have substantially reduced the disparity in treatment.

In the wake of September 11, few politicians were willing to support any measures that could be interpreted as inhibiting our ability to keep ourselves safe.[499] I have already discussed ways in which the public's fears have been somewhat irrational. In fact, we have no reason to believe that rationalizing surveillance law by extending the protections of the Wiretap Act to all electronic information—stored or not, content or attributes—would inhibit law enforcement's efforts to keep us safe.[500] Before we are convinced otherwise, we should see specific cases in which fishing through the data of those not suspected of terrorist activity yields useful data that is worth the cost in resources and privacy. The experts tell us that such fishing expeditions will be fruitless.[501] History tells us that providing the government with broad surveillance powers could have a drastic impact on our freedoms and democracy.[502]

VI. CONCLUSION

The current legal framework for online surveillance ignores the lessons learned in the context of the Wiretap Act. Namely, the allure of electronic surveillance to law enforcement and its threat to privacy requires a comprehensive and workable framework that strictly limits government's ability to surveil and that affords myriad opportunities for oversight by members of the judiciary, Congress, and the public. As interpreted, and particularly as advocated by the Justice Department, the ECPA reduces to almost zero the number of investigations that will be accorded wiretap-like restrictions. Even then, victims of unlawful online surveillance lack a statutory suppres-

497. *See* H.R. REP. NO. 106-932, at 7-8 (2000). Rather than acting as a rubber stamp, judges would have approved of pen register investigations only when they found "specific and articulable facts reasonably indicat[ing] that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use is relevant to the investigation of that crime." *Id.* at 3. The law would have provided after-the-fact notice to pen register targets. *Id.* at 8.

498. *See* H.R. REP. NO. 106-932, at 8. It would have also required detailed reporting to Congress on stored record acquisitions and substantially increased the remedies available for violations of the stored communication provisions. *See id.* at 12-18.

499. *But see* Howell, *supra* note 404 (describing legislators' rejection of some of the most outrageous demands by the Administration during negotiations over the USA PATRIOT Act).

500. Of course it would limit law enforcement's ability to conduct online surveillance, but that would be by design. However, Justice Department officials testified in 2000 that they would have no problem accepting the substantial increase in judicial review of pen register applications proposed in the 2000 bill. *See* H.R. REP. NO. 106-932, at 14.

501. *See* SCHNEIER, *supra* note 57, at 567.

502. *See supra* notes 17-19.

sion remedy. Most online surveillance proceeds without the involvement of the judiciary, and without meaningful remedies for abuse. The statutory framework persists in an outdated and nearly incomprehensible form. It leaves significant questions unanswered about the scope of governmental powers to surveil, even after the USA PATRIOT Act.

Unless we are convinced that there should be no privacy on the Internet, or that there should be no privacy in our modern era, the system of online surveillance law warrants revision. The similarities among online surveillance, video surveillance, and traditional electronic surveillance suggest that the legal framework that protects the privacy of telephones and private spaces should be extended to protect the privacy of the Internet.