2005

Spyware and the Limits of Surveillance Law

Patricia L. Bellia
Notre Dame Law School, patricia.l.bellia.2@nd.edu

SPYWARE AND THE LIMITS OF SURVEILLANCE LAW

By Patricia L. Bellia†

TABLE OF CONTENTS

I. INTRODUCTION

Electronic surveillance law remains a weapon of choice for policy-makers, litigants, and commentators seeking to address the threats digital technology poses for privacy. The controversy over how best to respond to the "spyware" problem provides only the most recent illustration of that

---

† Lilly Endowment Associate Professor of Law, Notre Dame Law School. A.B. Harvard College, J.D. Yale Law School. I thank A.J. Bellia, Susan Freiwald, and Orin Kerr for helpful discussions. Jeannette Cox provided excellent research assistance.

phenomenon.[1] Federal surveillance statutes bar the unauthorized acquisition of electronic communications and related data in some circumstances.[2] Although there is much debate over how to define "spyware,"[3] that label encompasses at least some software that monitors a computer user's electronic communications. Surveillance statutes thus present an intuitive fit for responding to the regulatory challenges of spyware. Indeed, those who argue that no new federal legislation is needed to address the spyware problem rely in part on the opportunities that surveillance statutes and related doctrines provide for criminal prosecution and civil suits.[4]

A recent report issued by the staff of the Federal Trade Commission, for example, suggests that the Department of Justice "has statutory authority to prosecute distributors of software products, such as spyware, in cases where consumers' privacy or security is compromised."[5] That observation was based in part on testimony of Justice Department officials at a day-long FTC workshop held in April 2004. The Justice Department denied that the absence of specific spyware legislation had impeded law enforcement efforts in any way.[6] As one official noted, "we have in our

1. A recent report of the staff of the Federal Trade Commission provides a flavor of the debate. *See* FED'L TRADE COMM'N STAFF REPORT, SPYWARE WORKSHOP: MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE (2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarept.pdf [hereinafter FTC STAFF REPORT].

2. *See* 18 U.S.C. § 2511(1)(a) (2000) (prohibiting "intercept[ion]" of communications); *id.* § 2701(a) (barring one from gaining unauthorized access to facility of service provider and thereby "obtain[ing], alter[ing], or prevent[ing] authorized access" to communications in electronic storage).

3. *See, e.g.*, H.R. REP. NO. 109-32, at 10 (2005) (report of Committee on Energy and Commerce, noting that the committee "received testimony that spyware represents a range of software programs on a broad continuum from the most pernicious criminal activities on one end to the less threatening but still intrusive on the opposite end of the spectrum"); FTC STAFF REPORT, *supra* note 1, at 3 ("Panelists generally agreed that reaching an industry consensus on one definition [of spyware] has been elusive because of the technical complexity and dynamic nature of software.").

4. The Senate and the House have debated various spyware proposals over the last two years; most recently, the House overwhelmingly passed two dramatically different versions of spyware legislation in May of 2005. *See* Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), H.R. 29, 109th Cong. (2005); Internet Spyware (I-SPY) Prevention Act, H.R. 744, 109th Cong. (2005). Both bills were passed on May 23, 2005, H.R. 29 by a margin of 393-4 and H.R. 744 by a margin of 395-1. *See* 151 CONG. REC. H3744 (daily ed. May 23, 2005). For a discussion of disagreement over the need for new legislation, see FTC STAFF REPORT, *supra* note 1, at 22.

5. FTC STAFF REPORT, *supra* note 1, at 21.

6. *See* FED'L TRADE COMM'N WORKSHOP TRANSCRIPT: MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE 261 (Apr. 19, 2004), *available*

quiver a number of arrows that we can use in prosecution."[7] Justice Department officials testified at the FTC workshop that some forms of spyware, such as devices and software designed to capture keystrokes, could violate the principal federal electronic surveillance statute—Title III of the Omnibus Crime Control and Safe Streets Act of 1968—which prohibits the "intercept[ion]" of communications, including electronic communications.[8] Other commentators have suggested that spyware may also implicate a separate electronic surveillance statute limiting access to stored communications.[9]

As the debate on the need for new federal legislation proceeds, however, there is good reason to believe that federal electronic surveillance statutes can combat only the most extreme forms of spyware. Electronic surveillance law does not apply by any reasonable construction to most forms of spyware. Moreover, the overall record on application of surveillance law statutes to a variety of digital-age problems is in fact quite mixed. Courts have reached aggressive privacy-protective outcomes on very bad facts, but they have also let seemingly problematic practices pass unsanctioned.

The difficulty with efforts to apply surveillance law statutes to new privacy problems is that our federal electronic surveillance statutes are emphatically not comprehensive data privacy statutes. They may wrongly be perceived as such, particularly by victims of spyware and related privacy threats. The mismatch between the statutes and the goal of protecting online privacy has created a body of confused—even incoherent—case law. To that extent, it diverts attention from important policy questions, including whether Congress should consider legislative solutions tailored

---

at http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf (comments of Mark Eckenwiler, Deputy Chief, Computer Crime and Intellectual Property Section, Department of Justice) [hereinafter FTC WORKSHOP TRANSCRIPT].

7. *Id.*

8. 18 U.S.C. § 2511(1)(a) (2000); *see* FTC WORKSHOP TRANSCRIPT, *supra* note 6, at 260 (comments of Mark Eckenwiler). Justice Department testimony also focused on various prongs of the federal computer crime statute, known as the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2000 & Supp. II 2002). *See* FTC WORKSHOP TRANSCRIPT, *supra* note 6, at 259-60 (comments of Mark Eckenwiler). CFAA claims often go hand-in-hand with claims under the surveillance statutes, but because the CFAA is not technically a surveillance statute, I discuss it only briefly. *See infra* note 168 and accompanying text.

9. 18 U.S.C. §§ 2701-2709, 2711-2712 (2000 & Supp. II 2002); *see* FTC STAFF REPORT, *supra* note 1, at 35 n.206 (citing 18 U.S.C. §§ 2701-2711); CENTER FOR DEMOCRACY & TECHNOLOGY, GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM 10 n.12 (Nov. 2003), *available at* http://www.cdt.org/privacy/031100spyware.pdf (citing 18 U.S.C. §§ 2701-2712).

to specific privacy threats (such as spyware) or whether broader data privacy statutes are necessary or appropriate. In other words, we might be better off if courts and commentators would simply make surveillance law's limits plain.

This Article uses the difficulties of applying electronic surveillance law statutes to spyware to illustrate the broader limits of surveillance law. Part II provides an overview of the electronic surveillance framework. Part III considers the interpretive issues that have arisen and that are likely to arise as litigants and courts seek to apply the federal statutes to various types of spyware. Current case law suggests that electronic surveillance statutes are likely to constrain only the most egregious forms of spyware—and there may even be some difficulties in surveillance law performing that limited task. Efforts to use surveillance law to create more privacy-sensitive industry practices are likely to fail altogether.

The constructions of the law that I offer in Part III may be controversial, partly because surveillance law is sufficiently unstable that there is room for courts to adopt approaches that are more privacy-protective. In Part IV, I consider whether courts *should* use surveillance law to respond more aggressively to privacy challenges such as spyware. Drawing upon case law from other contexts, I show that there are good reasons to be wary of using surveillance law as a vehicle for addressing various information privacy problems. Indeed, if electronic surveillance cases were to plainly expose the limits of surveillance law, they would generate a more fruitful legislative debate about the propriety of true data privacy legislation, whether broadly or narrowly conceived.

II. UNDERSTANDING THE ELECTRONIC SURVEILLANCE LAW FRAMEWORK

In this Part, I introduce three statutes that form the federal electronic surveillance law framework:[10] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (also known as "Title III" or the "Wiretap

10. The electronic surveillance landscape also includes another important statute: the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C.A. §§ 1801-1863 (West 2000 & Supp. 2005). That statute authorizes surveillance to gather "foreign intelligence information," defined in part to include information that relates to the ability of the United States to protect against an attack or other hostile acts by a foreign power. *Id.* § 1801(e). Because I am primarily concerned with legal authorities that constrain private parties' conduct, I do not discuss FISA, which regulates only conduct undertaken "under color of law." *See id.* § 1809(a). For further discussion of FISA, see Patricia L. Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. (forthcoming 2005).

Act");[11] the segment of the Electronic Communications Privacy Act (ECPA) limiting access to stored communications (also known as the "Stored Communications Act (SCA)");[12] and the provisions governing the use of "pen registers" and "trap and trace devices"—that is, devices designed to acquire source and destination information associated with communications.[13]

Before exploring the electronic surveillance framework, it is useful to define "electronic surveillance" and to discuss one shortcoming of that phrase. By "electronic surveillance," I mean techniques that historically have involved the use of certain electronic or mechanical *devices* to acquire the contents of communications and identifying data associated with them. The term "electronic" in "electronic surveillance," then, refers to the technique used in the surveillance, not to the type of communication acquired through the technique. Wiretapping (attaching a device to a telephone wire to acquire the contents of a telephone communication) and eavesdropping (installing a device to transmit or record a conversation) are two electronic surveillance techniques. The Wiretap Act, the principal modern federal surveillance statute, was originally designed to regulate those techniques. As discussed below, technological developments necessitated an expansion of the Wiretap Act to encompass more modern methods of communication.

The phrase "electronic surveillance" is also something of a misnomer. The term "surveillance" is ordinarily used to describe the *government's* acquisition of information about its citizens. Indeed, all three of the federal statutes discussed below were primarily passed in response to, or designed to take account of, Supreme Court decisions addressing the legality under the Fourth Amendment of government surveillance activities. Each statute, however, also regulates *private* conduct. For purposes of understanding

---

11. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, §§ 801-804, 82 Stat. 197, 211-23 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000 & Supp. II 2002)). I dislike the term "Wiretap Act," because the statute covers not only "wiretapping"—that is, acquisition of the contents of wire communications through use of an electronic or mechanical device—but also the acquisition of oral and electronic communications. It is nevertheless difficult to avoid using it, because it appears in many of the cases that I discuss. When describing provisions of the statute under which government officials seek court authorization to conduct surveillance activities, however, I generally refer to "Title III" orders, in keeping with government practice.

12. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 201-202, 100 Stat. 1848, 1860-68 (codified as amended at 18 U.S.C. §§ 2701-2709, 2711-2712 (2000 & Supp. II 2002)).

13. *See id.* § 301, 100 Stat. at 1868-73 (codified as amended at 18 U.S.C. §§ 3121-3127 (2000 & Supp. II 2002)).

how, if at all, surveillance statutes constrain the distribution or use of spyware, we are primarily interested in the scope of the statutory prohibitions on private conduct. Because each statute to some extent accommodated a Supreme Court decision addressing government surveillance activities, however, it is impossible to understand the structure and terminology of each statute without understanding the Fourth Amendment limitations on government conduct.

I discuss the Wiretap Act, the Stored Communications Act, and the pen register and trap and trace provisions in turn. With respect to each statute, I identify the key interpretive issues that are likely to arise in attempts to apply the statute to the spyware problem.

A. The Wiretap Act

In adopting the Wiretap Act in 1968, Congress prohibited the "intercept[ion]" of certain communications.[14] Although the statute was the product of several years of legislative efforts to regulate wiretapping and eavesdropping activities,[15] two cases decided by the Supreme Court in 1967 provided the immediate impetus for the statute's passage.

In 1928, the Supreme Court held in *Olmstead v. United States*[16] that the government's use of a wiretapping device would not violate the Fourth Amendment unless government agents trespassed onto private property to install the device.[17] Congress responded in 1934 by outlawing wiretapping by private or governmental entities,[18] but these proscriptions were widely disregarded.[19] More than three decades later, as Congress weighed various statutory proposals to revise the prohibition on wiretapping and to add a prohibition on eavesdropping, the Supreme Court decided two key cases that would shape the legislative effort. First, in *Berger v. New York*,[20] the Court invalidated a New York statute setting forth requirements under

14. 18 U.S.C. § 2511(1)(a) (2000).

15. *See* AMERICAN BAR ASS'N PROJECT ON MINIMUM STANDARDS FOR CRIMINAL JUSTICE, STANDARDS RELATING TO ELECTRONIC SURVEILLANCE app. E (Tentative Draft, 1968) (cataloguing congressional hearings); S. REP. NO. 90-1097, at 134 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2223 (individual views of Sen. Long and Sen. Hart) (noting that Congress had debated bills addressing wiretapping and eavesdropping activities for forty years).

16. 277 U.S. 438 (1928).

17. *Id.* at 466.

18. Act of June 19, 1934, ch. 652, § 605, 48 Stat. 1103 (codified as amended at 47 U.S.C. § 605 (2000)).

19. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 12 (2004).

20. 388 U.S. 41 (1967).

which a judge could authorize law enforcement officials to use listening devices. Because the case involved a listening device that had been placed in an office after a "trespassory intrusion," the Court applied the Fourth Amendment notwithstanding its conclusion in *Olmstead*.[21] The Fourth Amendment requirements identified in *Berger* ultimately provided a blueprint for federal legislation.[22] Second, in *Katz v. United States*,[23] the Court abandoned its prior focus on trespass as the trigger for applicability of the Fourth Amendment. The *Katz* Court held that the Fourth Amendment does not simply protect against government intrusions into physical areas in which an individual has a property interest: "[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[24] Because the government's activities "in electronically listening to and recording [Katz's] words violated the privacy upon which he justifiably relied while using the telephone booth," the government's conduct amounted to a search.[25]

These two decisions brought a new sense of urgency to the legislative debate, because they essentially outlawed all wiretapping and eavesdropping activities by federal and state officials not conducted in conformity with the Fourth Amendment requirements outlined in *Berger*. The Wiretap Act reflected Congress's attempt to broadly regulate electronic surveillance by outlawing such activities by both private parties and government officials and excepting certain law enforcement conduct from the prohibition.[26]

The Wiretap Act provides for criminal penalties and civil damages against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept" any covered communication.[27] To "intercept" a communication is to use "any electronic, mechanical, or other device" to acquire its contents.[28] As passed in 1968, the Wiretap Act covered "wire communications," defined

21. *Id.* at 44.

22. *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1389-90 (2004); Freiwald, *supra* note 19, at 25.

23. 389 U.S. 347 (1967).

24. *Id.* at 353.

25. *Id.*

26. *See* 18 U.S.C. § 2511(1)(a) (2000) (outlawing interception by "any person"); *id.* § 2518 (setting forth procedures for government officials to request court authorization for electronic surveillance activities).

27. *Id.* § 2511(1)(a).

28. *Id.* § 2510(4).

to include a communication "made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection,"[29] and "oral communications," defined to include a communication "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[30] In 1986, in ECPA,[31] Congress extended the Wiretap Act's coverage to "electronic communications," defined in part 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 that affects interstate or foreign commerce."[32]

As will become clear, the Wiretap Act presents a number of difficult interpretive issues. First, the statute defines the term "intercept" to include the "aural or other acquisition of the contents of a communication"[33]—but the definition does not specify whether acquisition of a communication must occur contemporaneously with its transmission in order to qualify as an interception, or whether acquisition of stored communications would also qualify. That issue is among the most frequently litigated under the Wiretap Act, both with respect to government and private conduct,[34] and is likely to arise in the spyware context as well. Second, in addition to permitting authorized government conduct, the Wiretap Act exempts conduct undertaken with the "consent" of a party to the intercepted communication.[35] The consent exception essentially preserves a line of cases pre-

29. 18 U.S.C. § 2510(1) (2000 & Supp. II 2002). When Congress revised the Wiretap Act in 1986 by passing ECPA, it distinguished wire communications from electronic communications by amending the wire communication definition to refer to an "aural transfer," a term further defined as a transfer "containing the human voice." 18 U.S.C. § 2510(18) (2000). In addition, ECPA altered the wire communication definition to include "any electronic storage of such communication." *Id.* § 2510(1). That portion of the definition was excised by the USA Patriot Act. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 209, 115 Stat. 272, 283 [hereinafter USA PATRIOT Act]. For further discussion, see *infra* notes 198-206, 290-293 and accompanying text.

30. 18 U.S.C. § 2510(2) (2000).

31. Pub. L. No. 99-508, § 101, 100 Stat. 1848, 1848 (1986).

32. 18 U.S.C. § 2510(12).

33. *Id.* § 2510(4).

34. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); Wesley Coll. v. Pitts, 974 F. Supp. 375, 388 (D. Del. 1997); Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996); United States v. Reyes, 922 F. Supp. 818, 837 (S.D.N.Y. 1996); *see also infra* notes 183-189, 194-229, 281-293 and accompanying text.

35. 18 U.S.C. § 2511(2)(c), (d) (2000).

dating the Wiretap Act's passage in which the Supreme Court upheld the introduction into evidence of communications recorded or transmitted to the government by an undercover agent or informant.[36] The Court reaffirmed these cases after its decision in *Katz*, concluding that the Fourth Amendment does not prevent a party to a conversation from revealing its contents to the government, because a defendant has no "constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police."[37] The Wiretap Act permits a person "acting under color of law" to intercept a communication where the person is a party to the communication or another party has given prior consent.[38] In the case of purely private conduct, the Act permits a person to intercept a communication where the person is a party or where a party has given prior consent, so long as the communication is not intercepted "for the purpose of committing any criminal or tortious act."[39]

Each of these interpretive issues—what it means to "intercept" a communication and when an interception is consensual and thus not unlawful—will present challenges for the application of the Wiretap Act to spyware. I discuss these issues further in Part III.

B. The Stored Communications Act

As previously noted, the Wiretap Act initially prohibited only the interception of wire and oral communications. The extension of the Wiretap Act to electronic communications in 1986 was part of a larger effort to update surveillance law to account for the increasing use of electronic communications.

In particular, Congress recognized that systems allowing for the transmission and receipt of electronic communications necessarily involved the *storage* of such communications.[40] During hearings on how

36. *See, e.g.*, Osborn v. United States, 385 U.S. 323 (1966) (admitting recording taped by government informant and concluding that case involved "not . . . surreptitious surveillance of a private conversation by an outsider, but . . . the use by one party of a device to make an accurate record of a conversation"); Hoffa v. United States, 385 U.S. 293, 302 (1966) (declining to suppress government informant's testimony because Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"); Lopez v. United States, 373 U.S. 427, 439 (1963) (holding that evidence derived from a conversation recorded by a government agent was admissible).

37. United States v. White, 401 U.S. 745, 749 (1971) (plurality opinion); *see* United States v. Caceres, 440 U.S. 741, 750-51 (1979) (following *White*).

38. 18 U.S.C. § 2511(2)(c) (2000).

39. *Id.* § 2511(2)(d).

40. *See, e.g.*, S. REP. NO. 99-541, at 8 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3562 (describing e-mail systems); H.R. REP. NO. 99-647, at 22 (1986) (same).

Congress should update surveillance law, industry representatives emphasized that the development of electronic communication services necessarily depended upon Congress providing a degree of statutory protection for stored communications.[41] Quite apart from the need to protect stored communications against intrusions by private parties, Supreme Court case law cast doubt upon whether stored communications were entitled to any Fourth Amendment protection against government acquisition.[42]

In *United States v. Miller*,[43] the Supreme Court weighed a defendant's Fourth Amendment challenge to the government's use of a subpoena to obtain certain records from the defendant's banks. The defendant moved to suppress the records on the ground that the Fourth Amendment required a search warrant. The Court held that because the defendant had voluntarily conveyed the items in question—including checks, financial statements, and deposit slips—to the banks, he had no legitimate expectation of privacy in the documents' contents.[44]

A broad reading of *Miller* would suggest that users storing electronic communications with service providers similarly surrender Fourth Amendment protection, because they have voluntarily conveyed those communications to a third party. As I have argued elsewhere, there are compelling reasons to reject this broad reading.[45] *Miller* nevertheless pro-

---

41. *See, e.g.*, S. REP. NO. 99-541, at 5, *as reprinted in* 1986 U.S.C.C.A.N. at 3559 (noting that gap in statutory protection "may unnecessarily discourage potential customers from using innovative communications systems" and "discourage American businesses from development of new innovative forms of telecommunications and computer technology"); H.R. REP. NO. 99-647, at 19 (noting that absence of legal protection for "may unnecessarily discourage potential customers from using such systems, and encourage unauthorized users to obtain access to communications to which they are not a party"); *see also Electronic Communication Privacy: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights and Trademarks, Senate Comm. on the Judiciary*, 99th Cong., 1st Sess. 121-22 (1987) (testimony of Philip M. Walker on behalf of e-mail industry noting vulnerability of communications while stored in provider's systems).

42. Indeed, the committee reports on ECPA reflected conflicting views on whether the Fourth Amendment protected stored communications. *Compare* S. REP. NO. 99-451, at 3, *as reprinted in* 1986 U.S.C.C.A.N. at 3557 (suggesting that communications in the hands of a third party "may be subject to no constitutional privacy protection"), *with* H.R. REP. NO. 99-647, at 22 ("It appears likely . . . that the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required.").

43. 425 U.S. 435 (1976).

44. *Id.* at 440.

45. *See* Bellia, *supra* note 22, at 1397-1412. The reasoning underlying *Miller* is questionable. In particular, *Miller* conflates two distinct lines of Supreme Court cases. *Id.* at 1397-1400. In the first line of cases, the Supreme Court rejected defendants' claims that the government could not acquire business records turned over to third parties with-

vided the foundation for some of ECPA's provisions regulating acquisition of stored communications, also known as the Stored Communications Act (SCA).[46] Like the Wiretap Act, the SCA prohibits all parties from gaining access to certain kinds of communications,[47] but also identifies a range of circumstances in which law enforcement officials are authorized to do so.[48] Although the government access provisions require law en-

---

out a search warrant, finding a subpoena adequate. *See, e.g.*, Couch v. United States, 409 U.S. 322, 335 (1973); Oklahoma Press Pub'g Co. v. Walling, 327 U.S. 186, 208 (1946). In those cases, the Court's reasoning relied not only on the fact that the records were provided to a third party, but on the *nature of the records* involved. *See, e.g.*, *Couch*, 409 U.S. at 335 (rejecting taxpayer's challenge to summons requiring accountant to surrender taxpayer's records and concluding that "there can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return"). In the second line of cases, the Supreme Court rejected claims that the Fourth Amendment prohibits the government from introducing into evidence communications revealed, recorded, or transmitted to the government by a government informant or undercover agent who is a party to the communications. *See supra* notes 36-37 (citing cases). In those cases, the Court essentially concluded that one who converses with another *assumes the risk* that the conversation will be revealed to law enforcement officials, thus eliminating any possible expectation of privacy. *See, e.g.*, United States v. White, 401 U.S. 745, 749 (1971) (plurality opinion) (noting that the *Katz* court did not "indicate in any way that defendant has a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police").

Miller was a business records case. In relying on the government informant cases, however, the *Miller* Court introduced an assumption-of-risk analysis not previously prominent in the business records cases. *See* Bellia, *supra* note 22, at 1402. Even if *Miller*'s analysis is correct, there are other reasons not to use the *Miller* framework in evaluating whether a user has an expectation of privacy in communications the user conveys to a service provider. The circumstances in *Miller* differ significantly from the circumstances involved when a subscriber relies on a service provider to transmit and store communications. First, *Miller* involved negotiable instruments rather than personal communications. Second, in *Miller*, the defendant's purpose in conveying the records to the bank—for the bank to complete certain transactions—made the substance of the records independently relevant to the bank. An e-mail subscriber's purpose in conveying the contents of a communication to a service provider is simply to have the provider transmit the communication. The contents of the communications are of no relevance to the service provider. *See id.* at 1403-05.

46. *See, e.g.*, S. REP. NO. 99-541, at 3, *as reprinted in* 1986 U.S.C.C.A.N. at 3557 (discussing *Miller*); H.R. REP. NO. 99-647, at 23 & nn.40-41 (same); Bellia, *supra* note 22, at 1413 (noting that provisions of the SCA allow for compelled production of the contents of communications without a search warrant in some circumstances—a result that is constitutional only if a user lacks an expectation of privacy in at least some communications stored by a provider).

47. 18 U.S.C. § 2701(a) (2000).

48. *Id.* § 2701(c); 18 U.S.C. § 2703 (2000 & Supp. II 2002).

forcement officials to obtain a warrant in some circumstances,[49] in others they allow law enforcement officials to acquire communications with a subpoena or a special court order with standards lower than those required by the Fourth Amendment.[50] Whether a warrant is required turns on interpretation of key statutory terms, such as when communications are held "in electronic storage" by the provider of an "electronic communication service."[51] Those same terms also appear in the SCA's substantive prohibition, 18 U.S.C. § 2701(a), which provides for criminal penalties and civil damages against one who:

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . .

Like the Wiretap Act, the SCA presents a number of difficult interpretive issues. The first difficulty is how to reconcile the Wiretap Act with the SCA. As noted, the Wiretap Act does not define interception with enough specificity to foreclose claims that acquisition of stored communications constitute an interception. Second, § 2701(a) applies only when a defendant gains access to a "facility through which an electronic communication service is provided."[52] Although that phrase quite clearly would cover the mail servers of an e-mail provider, it is not clear what other facilities the statute covers. Third, with respect to application of the provisions authorizing government access to stored communications,[53] the Justice Department has argued quite forcefully for a narrow construction of "electronic storage"[54]—an interpretation that obviously has significant bearing on the scope of § 2701(a), which protects electronic communications only "while . . . in electronic storage."[55] Fourth, because liability under

49. *See* 18 U.S.C. § 2703(a) (Supp. II 2002).
50. 18 U.S.C. § 2703(b) (2000).
51. *See* 18 U.S.C. § 2703(a) (Supp. II 2002).
52. 18 U.S.C. § 2701(a) (2000).
53. *See* 18 U.S.C. § 2703(a), (b) (2000 & Supp. II 2002).
54. *See, e.g.*, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 88-89 (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf [hereinafter CCIPS MANUAL].
55. 18 U.S.C. § 2701(a) (2000).

§ 2701(a) turns on whether access to the communications facility is unauthorized,[56] in any given case it will be important to determine the scope of the defendant's authority. Relatedly, like the Wiretap Act, the SCA has a consent exception. Section 2701(c)(2) provides that § 2701(a) does not apply with respect to conduct authorized "by a user of [an electronic communication service] with respect to a communication of or intended for that user."[57] Accordingly, a likely point of contention in any particular case will be whether a "user" has consented to the acquisition of his or her communications.

C. The Pen/Trap Statute

The final federal statute regulating electronic surveillance activities prohibits the use of "pen registers" and "trap and trace devices."[58] The pen/trap provisions formed part of ECPA,[59] and, like the SCA, sought to provide statutory protection following a Supreme Court decision on the application of the Fourth Amendment to certain government conduct.

In the 1979 case of *Smith v. Maryland*,[60] police investigating a robbery requested that a telephone company install a "pen register"—understood at the time to mean a device that records the numbers dialed on a telephone by monitoring electrical impulses triggered when the dial is released—on the defendant's home telephone line.[61] The information gleaned (specifically, the fact that the defendant made repeated calls to the robbery victim) provided the basis for a search warrant. The defendant sought to suppress the fruits of that search on the ground that the pen register was installed without a warrant.[62] Following the reasoning of *Katz* and *Miller*, the Court concluded that the defendant lacked any expectation of privacy in the telephone numbers he dialed: "Telephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[63]

In light of *Smith*'s conclusion that use of a pen register does not implicate the Fourth Amendment, Congress passed a statute providing minimal

---

56. *Id.*
57. *Id.* § 2701(c)(2).
58. 18 U.S.C. §§ 3121-3127 (2000 & Supp. II 2002).
59. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301, 100 Stat. 1848, 1868-73.
60. 442 U.S. 735 (1979).
61. *Id.* at 736-37 & n.1.
62. *Id.* at 737.
63. *Id.* at 743.

statutory protection against the use of pen registers as well as trap and trace devices (that is, devices designed to capture the origin of an incoming communication). Unlike the Wiretap Act and the SCA, the pen/trap statute does not create a civil action for violation of its provisions. Instead, it is a misdemeanor for one to "install or use a pen register or a trap and trace device without first obtaining a court order" as specified under federal law.[64] Nor does the statute provide for suppression of evidence in violation of its provisions. As a result, litigation involving the pen/trap statute is rare. But in the debate over how electronic surveillance law applies to spyware, there is considerable uncertainty as to where to draw the line between conduct prohibited by the Wiretap Act and conduct prohibited by the pen/trap statute.

As noted earlier, the Wiretap Act prohibits the interception of the *contents* of a communication.[65] The Wiretap Act defines the term "contents" to include the "substance, purport, or meaning" of a communication.[66] Information falling outside of that category—such as dialing information associated with a telephone communication or addressing or routing information associated with an electronic communication—is statutorily protected,[67] if at all, only by the pen/trap statute. With respect to information associated with electronic communications, however, the application of the pen/trap statute has historically been unclear. Although Congress clarified the reach of the pen/trap statute in the USA Patriot Act,[68] it essentially left the determination of where to draw the line between the Wiretap Act and the pen/trap statute in the hands of the courts.

When the pen/trap statute was first passed in 1986, there was ambiguity as to whether it applied to electronic communications at all. On the one hand, portions of the statute appeared to focus exclusively on telephone numbers. For example, the statute required the court order to specify the number of the "telephone line" to which the pen register or trap and trace device would be attached[69] as well as the subscriber of that telephone line.[70] The statute also defined a pen register as a device that "records or

64. 18 U.S.C. § 3121(a) (2000); *id.* § 3121(d) (setting forth penalty).

65. *Id.* § 2510(4) (defining "intercept").

66. *Id.* § 2510(8).

67. Although *Smith v. Maryland* makes clear that dialing information associated with a telephone call is not entitled to Fourth Amendment protection, the application of the Fourth Amendment to information associated with an electronic communication is more complicated. For further discussion, see Bellia, *supra* note 22, at 1428-30.

68. *See* Pub. L. No. 107-56, § 216, 115 Stat. at 283 (codified at 18 U.S.C. § 3127(3), (4) (Supp. II 2002)).

69. 18 U.S.C. § 3123(b)(1)(C) (2000).

70. *Id.* § 3123(b)(1)(A).

decodes electronic or other impulses which identify the *numbers dialed* or otherwise transmitted on the telephone line to which such device is attached."[71] On the other hand, the statute defined a trap and trace device as a device to capture the "originating number" from which "a wire *or electronic* communication was transmitted,"[72] thereby suggesting that the statute covered at least some identifying information associated with electronic communications. It was thus unclear whether the statute regulated the use of devices to obtain address information associated with electronic communications.

In the USA Patriot Act, Congress expanded the "pen register" and "trap and trace device" definitions, thereby clarifying that the statute covers devices used to obtain information associated with electronic communications.[73] The definitions apply to devices that gather "dialing, routing, addressing, or signaling information" indicating the source or destination of a wire or electronic communication.[74] In expanding the definitions, however, Congress expressly excluded from each definition "the contents of any communication." The exclusion was designed to allay concerns that addressing information associated with electronic communications would in some cases reveal the content of a communication, as where a web page's uniform resource locator (URL) incorporates search terms.[75] Rather than responding to these concerns by specifically indicating that URLs were to be considered "contents," Congress left the matter to judicial interpretation.

With respect to spyware designed to gather URLs and similar data, de-

---

71. *Id.* § 3127(3) (emphasis added).

72. *Id.* § 3127(4) (emphasis added).

73. *See* Pub. L. No. 107-56, § 216, 115 Stat. at 283 (codified at 18 U.S.C. § 3127(3), (4) (Supp. II 2002)).

74. *See* 18 U.S.C. § 3127(3) (Supp. II 2002) (defining "pen register" in part as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted"); *id.* § 3127(4) (defining "trap and trace device" in part as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication").

75. For example, a search for a book on breast cancer on Barnes & Noble's website might generate a page displaying search results with the following URL: http://search.barnesandnoble.com/booksearch/results.asp?WRD=breast+cancer&userid=[redacted]. For privacy advocates' objections to the expansion of the pen/trap statute, see, for example, *Protecting Constitutional Freedoms in the Face of Terrorism: Hearing Before the Subcomm. on Constitution, Federalism, and Property Rights of the S. Judiciary Comm.*, 107 Cong. (2001) (testimony of Jerry Berman, Executive Director, Center for Democracy & Technology), *available at* http://www.cdt.org/testimony/011003berman.shtml.

fendants will no doubt argue that such data does not reflect the "contents" of a communication for purposes of the Wiretap Act. Although I do not independently discuss application of the pen/trap statute to spyware, I explore the content/noncontent distinction in the course of discussing application of the Wiretap Act.

III. THE CHALLENGES OF APPLYING SURVEILLANCE LAW TO SPYWARE

Part II sets forth the basic structure of the federal electronic surveillance framework. Application of surveillance statutes to spyware is intuitively appealing: the statutes prohibit the interception or unauthorized acquisition of "electronic communications," and some forms of spyware clearly do capture users' electronic communications. As discussed below, however, there are good reasons to be skeptical that surveillance law statutes will curb anything but the most extreme forms of spyware.

Controversy surrounds the application of the term "spyware," and many products might fall within or just outside of the spyware category.[76] In assessing the applicability of surveillance law statutes, I focus on two products that are often labeled spyware: keystroke monitors and software designed to track Internet usage and deliver targeted advertising. These products illustrate a number of problems with applying electronic surveillance law to spyware, although I hope to sidestep the controversy over the appropriate use of the spyware label with respect to these products. In Section A, I briefly discuss the technology at issue. In Sections B and C, I discuss application of the Wiretap Act and the SCA, respectively.

A. The Technology at Issue

I begin with the application of electronic surveillance statutes to software and hardware devices that serve as "keystroke monitors"—that is, programs and devices that monitor every keystroke typed on a given computer.[77] Other devices and programs—such as "screen shot" utilities,

---

76. *See, e.g.*, H.R. REP. NO. 109-32, at 10 (2005) (report of Committee on Energy and Commerce, noting that the committee, "received testimony that spyware represents a range of software programs on a broad continuum from the most pernicious criminal activities on one end to the less threatening but still intrusive on the opposite end of the spectrum"); FTC STAFF REPORT, *supra* note 1, at 3 ("Panelists generally agreed that reaching an industry consensus on one definition [of spyware] has been elusive because of the technical complexity and dynamic nature of software.").

77. Hardware and software advertised to have such capabilities includes KeyKatcher, http://www.keykatcher.com (last visited Sept. 1, 2005); Keylogger Pro, *see* http://www.exploreanywhere.com/kp-intro.php (last visited Sept. 1, 2005); and iSpyNow,

which store images of what a computer screen displays at particular intervals—will raise similar analytical issues.[78] Keystroke monitors represent one of the most egregious forms of spyware when deployed against an unwitting user. Keystroke monitors consist of either hardware devices that attach to a computer at a point between the computer and its central processing unit (CPU)[79] or software programs installed by a person with administrative control of a computer or perhaps even remotely, through a security vulnerability or as part of a bundle of software.[80] Keystroke monitors are used for a range of purposes including lawful ones. An employer may deploy such a tool to monitor or deter abuse of a company computer system, or a parent may use it to monitor a child's Internet usage. Such programs and devices obviously have far more problematic uses as well: for hackers to acquire passwords, credit card numbers, or financial information, for one spouse to monitor another's online behavior, or for one coworker to spy on another.

I also consider the application of surveillance law to software installed on a user's computer to track the user's Internet usage and deliver targeted advertising. Such software is often referred to as "adware"; precisely where to draw the line between "adware" and "spyware" is controversial.[81] Most commentators focus on the issue of consent: when the user does not receive appropriate notice of the software's activities or lacks the ability to decline its installation, such software meets the definition of spyware.[82] Of course, what constitutes appropriate notice or adequate consent is itself a difficult issue. For purposes of my analysis, the "adware" or "spyware" label is less important than an understanding of how the software functions.

Recent litigation over software that allegedly tracks users' Internet ac-

---

see http://www.ispynow.com (last visited Sept. 1, 2005).

78. For a case involving a dispute over a wife's use of a screen shot utility to record her husband's online activities to find evidence of infidelity, see O'Brien v. O'Brien, 899 So. 2d 1133 (Fla. Dist. Ct. App. 2005).

79. KeyKatcher operates in this manner. *See* http://www.keykatcher.com (last visited Sept. 1, 2005). For discussion of a case involving use of this device, see *infra* notes 107-113 and accompanying text.

80. For example, a tool called Perfect Keylogger was advertised as having a "unique *remote installation* feature. You can attach keylogger to any other program and send it by e-mail to install on the remote PC in the stealth mode." *See* http://www.blazing tools.com/bpk.html (last visited Sept. 7, 2004) (on file with author).

81. *See, e.g.*, FTC STAFF REPORT, *supra* note 1, at 3-4 (noting range of views on whether and when adware should be classified as spyware).

82. *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2065 (2004).

tivities sheds some light on how targeted advertising software functions.[83] WhenU.com's "SaveNow" software provides one example. Typically, a user downloads the SaveNow software as part of a bundle of free software.[84] Once loaded onto a user's computer, the SaveNow software launches whenever the user's browser is active. The software scans data from a browsing session, including URLs, search terms typed into a search engine, and the contents of a requested page.[85] The software compares the URLs, search terms, or keywords drawn from a web page to terms in its proprietary database.[86] A match triggers contextual pop-up advertising.[87]

Keystroke monitors and software for contextual advertising represent only two among a wide range of products that might be considered spyware.[88] Nevertheless, they illustrate the difficulties of applying electronic surveillance law to spyware. Because of significant overlap among the issues with respect to each type of product, I discuss the issues by statute rather than by product.

As I will show, electronic surveillance law constrains only the most extreme forms of spyware—and even then, there are pitfalls. Although the Wiretap Act presents an obvious option for controlling devices and software with keystroke monitoring capabilities, current case law suggests that the matter is more complicated. With respect to applications that gather data and communications so as to provide targeted advertising, the issue of consent will be an impediment to controlling the distribution of software that many would regard as deceptive and highly privacy-intrusive. In other words, surveillance law may be used to target the most serious forms of spyware, but it is unlikely to otherwise force change in industry practices concerning the distribution and functionality of software.

---

83. *See, e.g.*, 1-800 CONTACTS, Inc. v. WhenU.com, 414 F.3d 400, 2005 U.S. App. LEXIS 12711, at *1 (2d Cir. Jun. 27, 2005); Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d 734 (E.D. Mich. 2003); U-Haul Int'l, Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723 (E.D. Va. 2003).

84. *See 1-800 CONTACTS*, 2005 U.S. App. LEXIS 12711, at *9; *Wells Fargo*, 293 F. Supp. 2d at 743; *U-Haul*, 279 F. Supp. 2d at 725.

85. *See 1-800 CONTACTS*, 2005 U.S. App. LEXIS 12711, at *10; *Wells Fargo*, 293 F. Supp. 2d at 743-44; *U-Haul*, 279 F. Supp. 2d at 725.

86. *See 1-800 CONTACTS*, 2005 U.S. App. LEXIS 12711, at *10; *Wells Fargo*, 293 F. Supp. 2d at 743; *U-Haul*, 279 F. Supp. 2d 725-26.

87. *See 1-800 CONTACTS*, 2005 U.S. App. LEXIS 12711, at *10-*11; *Wells Fargo*, 293 F. Supp. 2d at 743; *U-Haul*, 279 F. Supp. 2d at 726.

88. For further discussion of products that might be considered "spyware," see H.R. REP. 109-32, at 10-11 (2005); FTC STAFF REPORT, *supra* note 1, at 2-8.

B. The Wiretap Act

1. *The "Interception" Problem*

As discussed earlier, § 2511(1)(a) of the Wiretap Act prohibits any person from "intentionally intercept[ing] . . . a wire, oral, or electronic communication."[89] The term "intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[90] The first question in applying the Wiretap Act to spyware, then, is whether the use of a particular spyware product in fact results in the "intercept[ion]" of the "contents" of an "electronic communication."

I alluded earlier to one difficulty with the term interception: determining whether a communication must be captured in transmission to qualify or whether the Wiretap Act also covers acquisition of communications from storage (as when an e-mail is held for retrieval by the recipient).[91] Most courts have agreed that interception occurs when electronic communications are acquired during transmission and not when they are acquired from storage.[92] But even with spyware used on an ongoing basis to monitor data as it is being transmitted, interpretive issues may still impede application of the Wiretap Act.

Keystroke monitors present particular difficulties. In many cases, a keystroke monitor will capture data solely within a single computer system—perhaps, as noted, between the keyboard and the CPU. The issue is whether acquisition of data within a single system can constitute an interception of an electronic communication.

Two courts considering that question have concluded that interception of a communication cannot occur within a single system. In *United States v. Scarfo*,[93] federal investigators, after obtaining a warrant, attached a keystroke monitor to the computer of a defendant suspected of running an illegal gambling and loan-sharking operation.[94] The investigators sought to obtain the password for the defendant's encryption software. They successfully obtained that password, which allowed decryption of other previously obtained files.[95] The defendant later moved to suppress evidence

89. 18 U.S.C. § 2511(1)(a) (2000).

90. *Id.* § 2510(4). The statute does not define the term "device."

91. *See supra* notes 33-34 and accompanying text; *infra* notes 194-229, 281-293 and accompanying text.

92. *See supra* note 34 (citing cases).

93. 180 F. Supp. 2d 572 (D.N.J. 2001).

94. *Id.* at 574.

95. *Id.*

derived from the use of the keystroke monitor on the theory that the government should have obtained a full Title III order before installing the device.[96] The issue was whether the government's use of the device resulted in the interception of communications without a Title III order.[97]

The government argued that the keystroke monitor did not "intercept" communications within the meaning of the Wiretap Act. In particular, the government configured the device to determine whether the modem on the defendant's computer was operating at any point in time; if the modem was operating, the keystroke monitor would not collect data.[98] In other words, the device would not capture a keystroke unless all of the computer's communication ports were inactive.[99] The district court concluded that in this context, no Title III order was necessary: the keystroke monitor acquired only data "within" the defendant's computer.[100]

The court's opinion was somewhat opaque in two respects. First, it alternately referred to the communications the government was alleged to have intercepted as "wire communications"[101] and "electronic communications."[102] Because the communications did not contain the human voice, they could not have been "wire" communications.[103] The distinction between electronic and wire communications in fact should have been crucial to the case. The Wiretap Act provides no suppression remedy for acquisition of an electronic communication in violation of its terms;[104] a motion to suppress electronic communications could have been based only on the Fourth Amendment. In *Scarfo*, however, the defendant sought suppression only under the Wiretap Act.[105] Second, the court never clearly explained why the modem's inactivity precluded the court from treating the

96. *Id.*
97. *Id.* at 575.
98. *Id.* at 581-82.
99. *Id.* at 582.
100. *Id.* at 582 n.5.
101. *See id.* at 576, 582.
102. *See id.* at 581-82.
103. *See* 18 U.S.C. § 2510(1) (2000) (defining wire communication as an "aural transfer"); *id.* § 2510(18) (defining aural transfer as "a transfer containing the human voice").
104. *See id.* § 2515 (barring introduction of contents of intercepted wire or oral communications into evidence); *id.* § 2518(10)(a) (permitting motion to suppress contents of wire or oral communication); *id.* § 2518(10)(c) (deeming remedies described with respect to electronic communications "the only judicial remedies and sanctions for nonconstitutional violations of this chapter"). Confusion over Title III's suppression provisions is not uncommon. *See* Bellia, *supra* note 22, at 1392-93 n.106.
105. 180 F. Supp. 2d at 576 (noting defendant's claim that government intercepted a communication "in violation of Title III").

acquisition of the communications as an interception. It is possible to construct one rationale, although the district court did not articulate it. By definition, an "electronic communication" must be transmitted by a system "that affects interstate or foreign commerce."[106] It could be argued that communications purely internal to a computer are not transmitted by a system affecting interstate commerce and therefore are not "electronic communications."

In *United States v. Ropp*,[107] the district court essentially adopted this rationale. *Ropp* involved a government prosecution under the Wiretap Act of a defendant who installed a keystroke monitor on a co-worker's computer.[108] The defendant physically attached a "KeyKatcher" device to the co-worker's computer where the keyboard attached to the computer's CPU.[109] The device picked up every keystroke as it was transmitted from the keyboard to the CPU.

In analyzing the legality of the defendant's behavior under the Wiretap Act, the district court focused on whether an "electronic communication" was involved. Recall the government's position in *Scarfo*: the Wiretap Act is not implicated where data is retrieved from within a computer system without an active communications port. In *Ropp*, the government took a slightly different position: the Wiretap Act applies to the acquisition of "any signal transmitted from a keyboard to a computer *with an internet connection*," "whether or not the internet connection was activated at the time of the transmission."[110] In other words, the government's position in *Scarfo* at least implicitly suggested that a communication that merely exists within a single computer does not constitute an "electronic communication," even if the computer can connect to the Internet. In *Ropp,* the government argued that a communication within a single computer with an available Internet connection does constitute an "electronic communication," because "the system by virtue of that connection 'affects interstate commerce.'"[111]

The *Ropp* court rejected the government's new approach and, relying on *Scarfo*, concluded that the Wiretap Act's definition of electronic communications applies only to data that is in fact being transmitted beyond a local computer by a system that affects interstate or foreign commerce.[112]

106. 18 U.S.C. § 2510(12) (2000).
107. 347 F. Supp. 2d 831 (C.D. Cal. 2004).
108. *Id.*
109. *Id.*
110. *Id.* at 835 (emphasis added).
111. *Id.*
112. *Id.* at 836, 837-38.

Even though the defendant's device captured keystrokes used in the composition of e-mail, the court concluded that no interception of an electronic communication occurred. Although the computer system from which the communications were acquired "is connected to a larger system—the network—which affects interstate or foreign commerce, the transmission at issue did not involve that system."[113]

In short, *Scarfo* and *Ropp* essentially hold that if a device or program is capturing communications at a point where the communications are internal to the user's system, then no interception occurs. Under this analysis, the Wiretap Act fails to regulate some of the most problematic forms of spyware, including keystroke monitors. Depending on how a particular piece of software operates, the Act may also fail to regulate software designed to facilitate contextual advertising, regardless of how much data the software acquires. Because such software is proprietary, it is often difficult to determine precisely how the software works. In particular, it is unclear whether such software captures data at a point within the user's computer or as communications are transmitted to the Internet. Under case law such as *Scarfo* and *Ropp*, these seemingly trivial issues become critical.

Of course, the extent to which *Scarfo* and *Ropp* will constrain distribution and use of keystroke monitors depends partly upon the extent to which they remain good law. The Wiretap Act ruling in *Scarfo* was apparently not appealed; the government sought reconsideration of the *Ropp* decision at the district court level, and its motion remains unresolved.[114]

---

113. *Id.* at 838.

114. The *Ropp* court buttressed its conclusion with one decision that is no longer good law, United States v. Councilman, 373 F.3d 197 (1st Cir. 2004), *reh'g en banc granted and opinion withdrawn*, 385 F.3d 793 (2004), *on reh'g en banc*, No. 03-1383, 2005 U.S. App. LEXIS 16803 (1st Cir. Aug. 11, 2005). *See Ropp*, 347 F. Supp. 2d at 836-38. In the *Councilman* case, the government sought to prosecute under the Wiretap Act an Internet service provider that captured the communications of its customers before transmitting them into to the customers' mailboxes. The district court and a panel of the U.S. Court of Appeals for the First Circuit held that the communications were acquired during a brief period of storage within the provider's system and therefore were not intercepted for purposes of the Wiretap Act. *Councilman*, 373 F.3d at 199. Relying on *Councilman*, the *Ropp* court reasoned that if messages momentarily stored within a provider's system are not intercepted for purposes of the Wiretap Act, then signals internal to a computer prior to transmission certainly cannot be. *Ropp*, 347 F. Supp. 2d at 838.

The reasoning in *Councilman* was weak. Several courts construing the Wiretap Act had previously held that the statute does not protect stored communications. *See supra* note 34 (citing cases). Those cases differed from *Councilman* in an important respect, however: they involved a one-time acquisition of communications maintained by a service provider for retrieval by the subscriber, whereas *Councilman* involved an ongoing acquisition of communications briefly stored during the transmission process prior to

With respect to both cases, it is tempting for commentators to argue that the cases involved erroneous reasoning or could be easily overturned with a statutory fix.[115] It is nevertheless important to recognize one outer limit on any judicial or legislative response. Most of the Wiretap Act was enacted under Congress's power under the Commerce Clause;[116] that was undoubtedly one reason for linking the definition of an electronic communication to a transmission involving a system "that affects interstate or foreign commerce."[117] It is difficult to see how, under current Commerce Clause jurisprudence, Congress could attempt to constrain use of a keystroke monitor on a standalone computer. The question then becomes whether the fact that a computer is networked, without more, necessarily sweeps it within Congress's reach.

2. *The "Consent" Problem*

If courts move past the "interception" problem, the Wiretap Act may become a tool for controlling spyware that is surreptitiously installed. For other forms of spyware, however, the problem of "consent" may become a

---

being made available to the subscriber. On rehearing *en banc*, the First Circuit rejected the district court and panel decisions, holding that the Wiretap Act prohibits the acquisition of electronic communications during transmission, even if those communications are briefly stored during the transmission process. *Councilman*, 2005 WL 1907258, at *10.

Although the *Ropp* court did discuss the panel opinion in *Councilman*, the reversal of the *Councilman* decision has little bearing on the central issue in *Ropp*: whether communications wholly within a single computer system constitute "electronic communications."

115. *See, e.g.*, Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1265, 1282 (describing *Scarfo* as involving "an end run around [the Wiretap Act] based on a technicality").

116. *See* S. REP. NO. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2180. As the report of the Senate Judiciary Committee accompanying the Wiretap Act suggested, "the facilities used to transmit wire communications form part of the interstate or foreign communications network." *Id.* For oral communications, the congressional power issues were more complicated. Such communications are far less likely to affect interstate commerce. To the extent that the provisions regulate acquisition of oral communications by state officials, the statute can be viewed as "enforcement" of the Fourth Amendment, as incorporated by the Fourteenth Amendment, because the statute defines oral communications as communications uttered by a person exhibiting a justifiable expectation that such communication is not subject to interception. *See* 18 U.S.C. § 2510(2) (2000). For provisions regulating acquisition of oral communications by private parties, the constitutional hook is less clear. The Judiciary Committee report contains an unusually candid discussion of the potential constitutional problems with application of the statute to private conduct. *See* S. REP. NO. 90-1097, *as reprinted in* 1968 U.S.C.C.A.N. at 2180.

117. *See* H.R. REP. NO. 99-647, at 35 (1986) (noting that the definition was "intended to cover a broad range of communication activities that affect interstate or foreign commerce").

major impediment to the application of the statute. As noted earlier, the Wiretap Act contains consent exceptions both for conduct under color of law[118] and purely private conduct.[119] For purely private conduct, § 2511(2)(d) of the Wiretap Act provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

What constitutes "prior consent" for purposes of the Wiretap Act? As noted earlier, employers may lawfully deploy keystroke monitors or similar devices to monitor employees' use of a company computer system. Generally, employers avoid liability under the Wiretap Act by providing notice of their monitoring activities—by displaying computer screen "banners" to inform employees that use of a company computer system constitutes consent to monitoring or by providing an "acceptable use" policy (perhaps signed by the employee) stating that monitoring may occur. But consent issues may arise even when a user is not directly confronted with a warning banner or fails to sign an acceptable use policy.

Assume, for example, that a user downloads a "bundle" of software products, and one piece of software within that bundle collects a user's data or communications. Those monitoring capabilities may be identified in an accompanying license agreement requiring the user to click "I Agree" before downloading the products. Does clicking "I Agree" constitute "consent" to satisfy § 2511(2)(d) of the Wiretap Act? This question will arise more commonly with software that monitors a user's communications so as to generate targeted advertising than with keystroke monitors. But in either scenario, no clear answer exists. On the one hand, courts applying related doctrines (including different provisions of the Computer Fraud and Abuse Act (CFAA)[120] and common law analogues) have broadly construed license agreements in favor of licensors—even when it

118. 18 U.S.C. § 2511(2)(c) (2000).

119. *Id.* § 2511(2)(d).

120. 18 U.S.C. § 1030 (2000 & Supp. II 2002). Technically, the title Computer Fraud and Abuse Act refers to the 1986 amendments to 18 U.S.C. § 1030, see Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 1, 100 Stat. 1213, but courts commonly use it to describe 18 U.S.C. § 1030 as a whole.

is questionable whether the licensee has manifested assent to particular notices provided by the licensor.[121] On the other hand, commentators (myself included) have criticized this trend.[122] For plaintiffs seeking to argue that the gathering of data or communications constitutes a violation of the Wiretap Act, the First Circuit's decision in *In re Pharmatrak Privacy Litigation* provides perhaps the most support.[123]

---

121. These issues arise in a variety of doctrinal contexts, including contract claims, application of the CFAA, and application of common law trespass to chattels doctrine. For contract claims, cases involving "shrinkwrap" licenses, where the consumer's act of breaking the shrinkwrap is deemed to be assent to the governing terms, form the foundation for courts' analysis. The trend among courts is to enforce such licenses, so long as the consumer has a right to reject the terms by returning the product. *See, e.g.*, ProCD v. Zeidenberg, 86 F.3d 1447, 1452-53 (7th Cir. 1996); Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149-50 (7th Cir. 1997). Extending this reasoning to the online context, courts have enforced "clickwrap" or "click-through" licenses that require a user to click "I Agree" or "I Accept" before downloading a particular product, at least where the "offer" makes clear that clicking the button will signify assent to the terms. *Compare* i.Lan Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 338 (D. Mass. 2002) (enforcing license where terms appeared on screen prior to software installation and defendant checked "I Agree" box), Forrest v. Verizon Commc'ns, Inc., 805 A.2d 1007, 1010–11 (D.C. 2002) (enforcing forum selection clause where terms were displayed in scroll box and plaintiff subscriber clicked "Accept" button), Caspi v. Microsoft Network, L.L.C., 732 A.2d 528, 530–31 (N.J. Super. Ct. App. Div. 1999) (enforcing forum selection clause contained in agreement with ISP, where prospective subscriber could only access service by clicking "I Agree"), Moore v. Microsoft Corp., 741 N.Y.S.2d 91, 92 (App. Div. 2002) (dismissing claim against software manufacturer where plaintiff user clicked on "I agree" icon before downloading software and claim was barred by license agreement), *and* Barnett v. Network Solutions, Inc., 38 S.W.3d 200, 204 (Tex. App. 2001) (finding forum selection clause enforceable where plaintiff had to scroll through terms and accept them before proceeding), *with* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 31-32 (2d Cir. 2002) (finding license terms unenforceable where terms appeared only on portion of webpage below software download button). For CFAA claims enforcing "terms of use" with minimal discussion of issues of notice and assent, see Am. Online v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1276 (N.D. Iowa 2000); Am. Online v. LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Va. 1998); *cf.* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) (suggesting that terms of use appearing on website would define the boundaries of use for purposes of CFAA). For similar approaches in trespass to chattels cases, see *LCGM*, 46 F. Supp. 2d at 448; Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d (BNA) 1020, 1025 (N.D. Cal. 1998). I discuss the nuances of these and similar cases in Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2225-45 (2004).

122. *See* Bellia, *supra* note 121, at 2245-52. Much of commentators' concern is driven by intellectual property law, in that broad enforcement of license agreements will allow content providers to appropriate control over content that copyright law would not permit. For discussion of such arguments, see *id.* at 2193-2201. There are, however, important fair notice concerns as well. *See id.* at 2192-93.

123. 329 F.3d 9 (1st Cir. 2003) [hereinafter *Pharmatrak II*], *on remand*, 292 F. Supp.

Pharmatrak constitutes one in a series of cases in which plaintiffs claimed that the placement of "cookies" on their hard drives violated the Wiretap Act, the SCA, and provisions of the Computer Fraud and Abuse Act.[124] With respect to the Wiretap Act, plaintiffs argued that, through placing cookies on their hard drives, companies intercepted their personal communications.[125] Most of the cases involved third-party advertisers who had arrangements with various sites to serve advertisements to website users.[126] Source code on the affiliated website triggered the user's browser to contact the third-party advertiser's server to provide the appropriate ad; this contact between the user and the third-party advertiser enabled the advertiser to place a cookie on the user's hard drive.[127] The third-party advertiser could associate various information in its database with that cookie (or update the cookie itself to reflect that information), including which of the advertiser's affiliated sites the user viewed and for how long.[128] Because third-party advertisers may be affiliated with a significant number of such sites, their use of cookies can result in substantial gathering of data. Once a third-party advertiser causes a cookie to be written to the user's hard drive, it can associate with that cookie (or update that cookie to reflect) not only information about the sites the user browsed that first caused the cookie to be set, but also information about sites the user subsequently browsed that were affiliated with the same advertiser.[129]

Allegations that the gathered communications included personal information stemmed from the manner in which browsers and web servers interact. When contacting a web server, browsers convey several pieces of information to facilitate the server's response, including the browser type and the language in which the browser is operating. Browsers may also convey the contents of the so-called "Referer" variable—a variable the user's browser typically sets to contain the URL of the previously ac-

---

2d 263 (D. Mass. 2003).

124. *See* In re Toys R Us, Inc. Privacy Litig., 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001); In re Intuit Privacy Litig., 138 F. Supp. 2d 1272 (C.D. Cal. 2001); In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

125. *See, e.g., Toys R Us*, 2001 WL 34517252, at *1, *6-*8; *Chance*, 165 F. Supp. 2d at 1155; *Intuit*, 138 F. Supp. 2d at 1274; *DoubleClick*, 154 F. Supp. 2d at 500.

126. *Pharmatrak* involved a third party, but not an advertiser. *See* In re Pharmatrak Privacy Litig., 220 F. Supp. 2d 4, 7 (D. Mass. 2002) [hereinafter *Pharmatrak I*]. Of the remaining cases cited, the only one not involving a third-party advertiser was *Intuit*. 138 F. Supp. 2d at 1274.

127. *See, e.g.*, *Chance*, 165 F. Supp. 2d at 1156; *DoubleClick*, 154 F. Supp. 2d at 503.

128. *See Pharmatrak II*, 329 F.3d at 14.

129. *See DoubleClick*, 154 F. Supp. 2d at 503-04 & n.12.

cessed web page.[130] The use of certain web forms can result in the incorporation of personal information into a URL.[131] Accordingly, routine interaction of a browser with a third-party advertiser's server could lead to the advertiser's acquisition of personal information.

I discuss in Part IV some of the significant problems with claims that use of cookies violates the surveillance law statutes.[132] Here, I focus on one aspect of the cases: their discussion of the Wiretap Act's consent exception. In most of the cookie cases, courts concluded that no Wiretap Act claim was available, because the companies had effectively consented to the third-party advertiser's acquisition of any communications between the users and the companies' servers.[133] Courts so held even though it was unclear whether the companies knew precisely what information the third-party advertiser could gather. The sole case to break with this trend was *Pharmatrak*.

Pharmatrak had entered into agreements with several pharmaceutical companies to aggregate certain data concerning the companies' users.[134] Like a third-party advertiser, Pharmatrak arranged with the pharmaceutical companies to require them to place on their websites certain source code causing a customer's browser to communicate with Pharmatrak's servers.[135] Communications between the customer and the pharmaceutical websites occasionally involved an exchange of personally identifiable information.[136] In certain cases, because a customer's communication with a pharmaceutical website immediately preceded its communication with Pharmatrak's servers, Pharmatrak's servers captured this personally identi-

130. "Referer" is a misspelling of referrer. *See* R. Fielding et al., Hypertext Transfer Protocol–HTTP/1.1 Request for Comments 2616, § 14.36, at 86 (1999), http://www.faqs.org/ftp/rfc/rfc2616.pdf.

131. *See, e.g.*, *Pharmatrak II*, 329 F.3d at 16; *DoubleClick*, 154 F. Supp. 2d at 504.

132. *See infra* notes 230-253 and accompanying text.

133. *See, e.g.*, *Chance*, 165 F. Supp. 2d at 1162; *DoubleClick*, 154 F. Supp. 2d at 514. In *Toys R Us*, the district court recognized that Toys R Us had consented to the third-party's acquisition of communications. 2001 WL 34517252, at *7-*8. The court declined to dismiss the Wiretap Act claim, however, because it believed that the plaintiffs had sufficiently alleged that any interception, though consensual, was undertaken with a tortious purpose. *Id.*; *see* 18 U.S.C. § 2511(2)(d) (2000) (excluding from private-party consent exception communications intercepted "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State"). Similar claims were raised but rejected in other cases. *See Chance*, 165 F. Supp. 2d at 1163; *DoubleClick*, 154 F. Supp. 2d at 519.

134. *Pharmatrak II*, 329 F.3d at 12.

135. *Pharmatrak I*, 220 F. Supp. 2d at 7.

136. *Pharmatrak II*, 329 F.3d at 15-16.

fiable information.[137]

When a group of plaintiffs brought suit alleging that Pharmatrak's conduct violated the Wiretap Act, Pharmatrak responded by asserting that the pharmaceutical defendants were parties to the allegedly intercepted communications and consented to the use of Pharmatrak's system.[138] Other courts had accepted this line of argument in cases involving third-party advertisers,[139] and the district court granted Pharmatrak summary judgment on the claim.[140] Here, however, the First Circuit rejected the consent argument. Although the pharmaceutical companies had in general terms consented to the use of Pharmatrak's proposed system for gathering data on customers, Pharmatrak never made clear that the system would gather personally identifiable information.[141] The companies' general consent to the use of the system was not sufficient to trigger the Wiretap Act's consent exception.

The First Circuit's approach in *Pharmatrak* suggests that the consent exception to the Wiretap Act's prohibition will be triggered only when the consenting party knows with a high degree of specificity what information will be acquired. *Pharmatrak* remains the exception rather than the rule, however; in none of the other cookie cases did courts examining the consent issue require that degree of specificity. Accordingly, the Wiretap Act's consent exception is likely to remain an impediment to applying the statute to software installed after a user is presented with a license agreement.[142] Of course, purveyors of spyware will sometimes use more deceptive tactics, such as installing software remotely through a security vulnerability, or allowing installation of software to proceed even when a user attempts to decline or cancel installation. The Wiretap Act may be more effective in these situations. It is important to note, however, that once software or a device with the capability to collect data or communications is installed or deployed, the method by which it was installed has little bearing on the degree to which the software or device affects the user's privacy interests. In other words, the Wiretap Act calibrates its coverage

137. *Id.* at 16.

138. *Id.* at 19.

139. *See supra* note 133 and accompanying text.

140. *Pharmatrak I*, 220 F. Supp. 2d at 12.

141. *Pharmatrak II*, 329 F.3d at 20.

142. As noted above, see *supra* note 133, plaintiffs have largely been unsuccessful in arguing that an interception, though consensual, is committed with a tortious or criminal purpose. According to the *Chance* and *DoubleClick* courts, it is not enough that the defendant has committed a tort; rather, the primary motivation or determining factor in its actions must have been to injure the plaintiff tortiously. *See Chance*, 165 F. Supp. 2d at 1163; *DoubleClick*, 154 F. Supp. 2d at 518.

based on whether the user in some sense consented to the software or device's installation, not the degree to which the software or device otherwise affects the user's privacy interests. I return to this point in Part IV.

3. *The "Content" Problem*

A final issue that arises in applying the Wiretap Act to various forms of spyware concerns whether the data seized, even if it is collected as it is transmitted from the user's computer to the Internet, is properly thought of as the "contents" of a communication. The Wiretap Act prohibits only the acquisition of the contents of a communication.[143] When Congress amended the pen/trap statute in the USA Patriot Act to allow acquisition of data associated with electronic communications, it specified that the pen/trap statute cannot be used to acquire the contents of a communication. In doing so, however, Congress created ambiguity as to precisely where the line between the contents of communications and addressing or routing information associated with a communication is to be drawn.[144]

The Wiretap Act defines the "contents" of a communication to include information concerning the "substance, purport, or meaning" of the communication.[145] No court has yet considered the status under the Wiretap Act or the pen/trap statute of URLs, which clearly identify addressing or routing information concerning the source of a communication and thus would fall within the pen register and trap and trace definitions if not for the exclusion of contents. If a Wiretap Act claim were brought in a case involving acquisition of URLs and search terms through use of a keystroke monitor or software for contextual advertising, there is little doubt that a defendant would argue that the communications in question did not reflect content.

Nevertheless, powerful arguments can be made that much of what a keystroke monitor or software designed to facilitate contextual advertising would capture constitutes the contents of a communication. There are certainly examples of URLs that convey the meaning of a communication. As noted earlier, by virtue of the operation of certain web forms, URLs can sometimes incorporate search terms or other information that a user wishes to remain private. For example, a search of an online bookstore for books on "breast cancer" may generate a page of search results identified by a URL that contains those search terms.[146] Even some URLs, without more, supply information on what the rest of a web page contains, and

143. *See supra* notes 33, 65 and accompanying text.
144. *See supra* notes 65-75 and accompanying text.
145. 18 U.S.C. § 2510(8) (2000).
146. *See supra* note 75 and accompanying text.

thus give information on the "substance, purport, or meaning" of a communication.[147]

Although there are powerful arguments that at least some URLs convey "contents" of a communication, an important impediment to courts' proper resolution of that issue still exists. As with many other statutory distinctions in electronic surveillance law, there are constitutional underpinnings to the distinctions the Wiretap Act and the pen/trap statute draw between content and non-content information.[148] In a dispute involving the government, a court would carefully apply the canon of constitutional avoidance[149] so as to construe the term "contents" fairly broadly, possibly concluding that URLs contain content. A court facing claims involving only private parties is far less likely to be sensitive to this constitutional backdrop.[150] I return to this issue in Part IV.

4. Summary

As this discussion suggests, there is good reason to be skeptical that the Wiretap Act will successfully curb anything but the most extreme forms of spyware. With respect to keystroke monitors, the fact that such programs or devices can capture communications before they are transmitted over the Internet suggests that, at least under existing case law, no interception occurs. For programs that capture communications as they are being transmitted over the Internet, the issue of consent will be extremely important, particularly if the programs were accompanied by a license agreement explaining their capabilities. Finally, the fact that the Wiretap Act covers only interception of the contents of a communication opens avenues for defendants to argue that certain data does not qualify as contents, and in the context of cases involving private parties, courts may be insensitive to the constitutional boundaries between content and non-content information.

147. Of course, one could argue that a URL and the accompanying web page are distinct electronic communications. The statute appears to treat as "contents" only information concerning the substance, purport, or meaning of the *communication in question*—for example, the URL—not information concerning the substance, purport, or meaning of *other communications*—for example, the web page.

148. For further discussion, see Bellia, *supra* note 22, at 1428-30.

149. *See, e.g.*, Jones v. United States, 526 U.S. 227, 239 (1999).

150. I discuss below the ways in which surveillance law's coverage of both government and private conduct can act as a double-edged sword. *See infra* notes 188-189, 294-298 and accompanying text.

C. The Stored Communications Act

The previous section explored the application of the Wiretap Act's prohibition on interception of electronic communications to various forms of spyware. Despite the intuitive characterization of spyware as a tool for intercepting communications, several interpretive issues complicate the analysis. The fit between spyware and the SCA is far less intuitive, but the statute is still likely to be invoked in efforts to curb spyware. Parties objecting to privacy-invasive practices with respect to electronic communications frequently tack SCA claims onto Wiretap Act claims.

Despite the frequency with which the SCA is invoked in privacy disputes, the statute protects an extremely narrow category of communications. As a result, it is unlikely to be of real benefit to plaintiffs objecting to most forms of spyware. To be sure, existing case law seems to leave open broader interpretations of the SCA. I return to that case law in Part IV to illustrate its flaws. For now, I focus on the SCA's text and legislative history.

1. The "Facility" Problem

Recall that the SCA prohibits one from gaining unauthorized access to a "facility through which an electronic communication service is provided," and thereby "obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in storage in such system."[151] A threshold requirement for any SCA claim, then, is a demonstration that a defendant gained unauthorized access to a "facility" through which an electronic communication service is provided.

Drawing upon the SCA's language and ECPA's legislative history, it is possible to identify some obvious examples of unauthorized access to a facility of an electronic communication service. The mail server of a service provider such as America Online would certainly qualify: the e-mail service is the "electronic communication service," insofar as it provides "users thereof the ability to send or receive wire or electronic communications,"[152] and AOL's mail server is the "facility" through which that service is provided. Were someone to hack into AOL's mail servers and obtain communications stored on AOL's servers and awaiting retrieval by a subscriber, the SCA would certainly cover the conduct. A similar example with respect to wire communications would be the system of a voicemail provider. Were someone to gain unauthorized access to the voicemail system and then obtain a wire communication, the predicate for § 2701(a)

151. 18 U.S.C. § 2701(a) (2000).
152. *Id.* § 2510(15).

would be met.

These examples are quite consistent with ECPA's legislative history. As the ECPA hearings indicate, much of the impetus for § 2701(a) of the SCA was that industry representatives feared that users would be deterred from using new communications systems if communications stored within those systems were unprotected.[153] Section 2701(a) was not designed as a general hacking statute; in fact, Congress was careful to limit the overlap between ECPA and computer crime amendments under consideration in 1986.[154] It did so by limiting the SCA's reach to communications within the facility of a provider of an electronic communication service.

Once we move beyond the servers of e-mail and voicemail providers, § 2701(a) becomes more difficult to apply. Cases presenting challenges to third-party advertisers' use of cookies provide a ready example. The SCA claims in those cases appeared to be premised on the view that the "facility" to which the third-party had gained access was the user's hard drive, by implanting the cookie. I discuss the problems with that approach in Part IV; for now, it is sufficient to recognize that a similar claim would have to be made with respect to spyware. The software that acquires a user's data or communications would be located on the user's hard drive; if § 2701(a) covers the installation of that software, it can only be because the facility to which the defendant gained unauthorized access is the plaintiff's computer. Section 2701(a) is thus unlikely to apply at all unless the facility requirement is broadly interpreted to cover an end-user's computer.

2. *The "Authorization" and "Consent" Problems*

Even if an end-user's computer is appropriately viewed as a "facility through which an electronic communication service is provided," other impediments to application of the SCA exist. To trigger the statute, a defendant's access to a protected facility must be unauthorized, whether "access without authorization" or "exceeding authorized access."[155] In addition, the SCA exempts from its prohibition conduct undertaken with the consent of a "user [of an electronic communication service] with respect

153. *See supra* notes 41-42 and accompanying text.

154. The overlap between computer crime statutes and ECPA was the subject of much discussion throughout the ECPA hearings. *See, e.g.*, *Electronic Communication Privacy: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights and Trademarks, S. Comm. on the Judiciary*, 99th Cong., 1st Sess. 94-95 (1987); *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice, H. Comm. on the Judiciary*, 99th Cong., 1st Sess. 22-23 (1986).

155. 18 U.S.C. § 2701(a) (2000).

to a communication of or intended for that user."[156]

Here, the issues are similar to those discussed above with respect to the Wiretap Act. The terms "access without authorization," "exceed[ing] authorized access," and "consent" are undefined. In the cookie cases, courts disposed of SCA claims in much the same way as Wiretap Act claims: by concluding that the websites affiliated with the third-party advertisers were parties to the communications and consented to their acquisition.[157] For software products installed following presentation of a license agreement, a defendant is quite likely to claim that the agreement adequately revealed that the software would, in the ordinary course of its operations, obtain a user's Internet communications. As in the case of Wiretap Act claims, such a defense may well be successful.[158]

3. The "Electronic Storage" Problem

One final issue is worth mentioning. The SCA requires a showing that a defendant obtained, altered, or prevented authorized access to a communication "while . . . in electronic storage" in a facility through which an electronic communication service is provided. This portion of the SCA obviously raises questions similar to the "facility" issue discussed above, since it seems unlikely that communications stored on a user's hard drive are properly viewed as stored in a facility through which an electronic communication service is provided. Even if the term "facility" were construed to cover an end-user's computer, it is not clear what communications on that computer would meet the technical definition of "electronic storage."

The SCA incorporates the definition of "electronic storage" that appears in the Wiretap Act.[159] Under the Wiretap Act, electronic storage includes "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[160] With respect to the SCA's provisions governing law enforcement access to stored communications, where the term "electronic storage" also appears,[161] the Department of Justice has argued for a narrow interpretation: to encom-

156. *Id.* § 2701(c)(2).
157. *See infra* note 245 and accompanying text.
158. *See supra* notes 120-142 and accompanying text.
159. 18 U.S.C. § 2711(1) (2000).
160. 18 U.S.C. § 2510(17) (2000 & Supp. II 2002).
161. *See* 18 U.S.C. § 2703(a) (Supp. II 2002).

pass only communications not yet retrieved by a subscriber.[162] The Justice Department bases its approach both on the definition of "electronic storage" and on the overall structure of the SCA. In terms of the definition, as long as a user has not yet retrieved a communication, a service provider's storage of it is "temporary," "intermediate," and "incidental" to its transmission. Once the user retrieves the communication, any further storage by the service provider (as, for example, when the user does not delete the communication) ceases to be "temporary" or "intermediate." Nor is such a communication stored by the provider for purposes of backup protection.[163] In terms of the structure of the SCA, the Justice Department has essentially argued that the statute's distinct treatment of providers of electronic communication services and providers of remote computing services can only be understood if electronic storage is narrowly construed.[164] In particular, once a subscriber retrieves a communication and chooses to retain it on the provider's system, the communication is no longer held in electronic storage by the provider of an electronic communication service; instead, it becomes one "held or maintained" by the provider of a remote computing service "for the purpose of providing storage . . . services" to the subscriber.[165]

I have extensively discussed this interpretation—and its limitations and implications for the SCA's government access provisions—elsewhere.[166] Here, it is sufficient to note that a fairly narrow interpretation of "electronic storage" has prevailed in various contexts.[167]

4. Summary

In sum, the SCA raises a number of difficult interpretive issues that will likely limit its application to spyware. Because keystroke monitors involve ongoing acquisition of data, they are unlikely to implicate the

---

162. *See, e.g.*, CCIPS MANUAL, *supra* note 54, at 88-89.

163. On this point, the Court of Appeals for the Ninth Circuit has concluded otherwise. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1076-77 (9th Cir. 2004). I discuss that case below. *See infra* notes 254-274 and accompanying text.

164. *See* CCIPS MANUAL, *supra* note 54, at 84-89.

165. *See* 18 U.S.C. § 2703(b)(2) (2000 & Supp. II 2002).

166. *See* Bellia, *supra* note 22, at 1416-26.

167. *See, e.g.*, In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001) (electronic storage occurs only "when an electronic communication service temporarily stores a communication while waiting to deliver it"); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) ("Retrieval of a message from post-transmission storage is not covered by the Stored Communications Act. The Act provides protection only for messages while they are in the course of transmission."), *aff'd on other grounds*, 352 F.3d 107 (3d Cir. 2003). *But see Theofel v. Farey-Jones*, 359 F.3d at 1076-77; *infra* notes 254-274 (discussing *Theofel*).

SCA at all. With respect to software designed to generate targeted advertising, the proprietary nature of the software makes it difficult to determine whether the products are operating in such a way as to collect temporarily stored communications. Moreover, the SCA was not designed as a general hacking statute to protect the computers of network end-users. Rather, the statute was designed to protect storage systems of service providers. In other words, the SCA is a narrow statute designed to protect communications at a certain point in the communications process.

In discussing the application of the SCA to spyware, I do not intend to suggest that a court would lack room to interpret the SCA broadly to encompass some objectionable conduct. I have already alluded to the fact that electronic surveillance law generally, and the SCA in particular, is somewhat unstable and not predictably applied by courts. More specifically, courts have tended to push the envelope in terms of applying the SCA to certain troubling privacy-invasive practices. In the case of the SCA, however, many judicial approaches simply cannot be justified under any appropriate canons of statutory construction. In limiting my discussion of such cases in my predictive analysis, I do not intend to overlook them. As discussed in Part IV, I am simply skeptical that such broad interpretations of the SCA will have any significant privacy benefits.

D. Conclusion

In sum, electronic surveillance statutes, by their terms, do not operate to regulate spyware activities in any comprehensive way.[168] Surveillance

168. I have not discussed another alternative for challenging spyware practices: the CFAA, 18 U.S.C. § 1030 (2000 & Supp. II 2002). The statute is not truly a surveillance statute, and a full discussion of it is therefore beyond the scope of this Article. It is nevertheless interesting to note something of a paradox: that despite the fact that the CFAA and related doctrines are mainly designed to respond to concerns about computer security rather than concerns about privacy, plaintiffs are more likely to have success pursuing spyware-related claims under the CFAA and analogous state law doctrines than they are under surveillance law statutes.

The most relevant provision of the CFAA is § 1030(a)(2), which prohibits one from "intentionally access[ing] a protected computer without authorization or exceed[ing] authorized access and thereby obtain[ing] . . . information from any protected computer if the conduct involved an interstate or foreign communication." *Id.* § 1030(a)(2). Because the CFAA requires a showing that any access to a computer was without authorization or exceeded authorized access, it raises a consent or authorization similar to the Wiretap Act and the SCA. *See supra* Parts II.B.2, II.C.2. But where a plaintiff can overcome the authorization problem—as, for example, when a defendant's installation of spyware was truly surreptitious—a CFAA claim in theory would be more likely to succeed than a Wiretap Act claim or an SCA claim. A plaintiff would not need to show for purposes of the Wiretap Act that communications were acquired contemporaneously with their transmission and not when purely internal to the computer system; and a plain-

law will combat only narrow categories of spyware: perhaps keystroke monitors, but only if courts can move past the problem of applying the "electronic communication" definition to data purely internal to a computer; and perhaps certain software designed to generate targeted advertising, but only if such software was installed surreptitiously or if a court finds that the user's consent was otherwise deficient.

The spyware story is not an unusual one. In a wide variety of contexts, plaintiffs have invoked electronic surveillance statutes in an attempt to curb certain privacy-invasive practices involving electronic communications. The next Part explores *why* surveillance law statutes have been and are likely to remain of marginal value in responding to a range of digital-age privacy threats.

IV. SURVEILLANCE LAW'S LIMITS

The discussion in Part III illustrates significant problems with applying

---

tiff would not need to show for purposes of the SCA that the defendant gained access to a "facility through which an electronic communication service is provided" or that the communications acquired were in "electronic storage."

A civil litigant will nevertheless face one significant obstacle under the CFAA: that of meeting the statute's $5000 threshold for economic damages. *See* 18 U.S.C. § 1030(g) (creating civil cause of action but specifying that underlying conduct must involve one of five "factors" set forth in § 1030(a)(5)(B)); *id.* § 1030(a)(5)(B)(i) (requiring, except with respect to action brought by government, a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5000 in value"). Of course, an impediment such as a $5000 loss threshold is a purely technical one that could be overcome by a legislative change. Moreover, the $5000 threshold does not leave a plaintiff entirely without a remedy: it simply reserves federal court involvement for the most serious claims, while funneling less significant claims into statute courts under analogous state statutes or common-law trespass to chattels claims.

This possibility that plaintiffs challenging spyware practices will be more successful with CFAA claims or analogous state law claims raises something of a paradox with respect to the spyware problem. What tends to make the forms of spyware discussed here objectionable is not merely the fact that in some cases the device or software is surreptitiously installed, but rather that spyware tools can acquire vast amounts of private information. It is that fact that at first blush seems to make surveillance law an attractive avenue to pursue. Statutes such as the CFAA and state law analogues can reasonably respond to issues of surreptitious installation, but they address the privacy concerns only incidentally—for the CFAA, by virtue of § 1030(a)(2)'s prohibition on gathering "information," and for common law trespass, only because the acquisition of private information may constitute a cognizable harm. In other words, even where significant privacy-invasive practices are at issue, a statute such as the CFAA—designed not to protect privacy but to guarantee security—seems to be a better conceptual fit than surveillance law statutes. The next Part considers why it is that surveillance law statutes respond so poorly to digital privacy threats.

surveillance law statutes to spyware. Two questions follow. First, *why* do surveillance law statutes respond so poorly, despite the privacy implications of spyware? Second, *could* surveillance law provide a more useful framework if more aggressively interpreted by the courts?

In exploring these questions, it is helpful to place the spyware problem in the broader context of efforts to use electronic surveillance law to address digital-age privacy challenges. As I will show, the spyware story is not unique. Litigants and commentators frequently assume that surveillance statutes provide appropriate vehicles for responding to such perceived privacy threats as online profiling and employer monitoring of communications, but such claims rarely succeed. The cases in which they do succeed involve unusual facts that are not generalizable across a broad class of cases. Although I do not address the merits of the disputed practices, I explain in Section A why efforts to enhance digital privacy through litigation have largely failed.

I then turn in the remainder of this Part to the normative question of whether courts should more aggressively interpret surveillance statutes to provide broader privacy-protective functions, at least in disputes involving private parties. In other words, if we agree that certain spyware practices (or other disputed practices involving electronic communications) should be curbed, is electronic surveillance law an appropriate vehicle for doing so—particularly since courts have managed to arrive at privacy-protective outcomes in some instances? I argue that aggressive judicial interpretations of surveillance statutes have failed to achieve lasting privacy benefits. In Section B, I offer three examples of courts' attempts to adopt privacy-protective interpretations in cases involving rather bad facts. As the examples illustrate, such interpretations can do considerable violence to the statutory text or legislative intent. Moreover, as Section C demonstrates, privacy-protective outcomes have a way of unraveling, perhaps as a result of the cases' vulnerability to criticism on statutory interpretation grounds. For each case involving a privacy-protective result, one can identify or predict a privacy-destructive response. Finally, in Section D, I show how decisions that reach privacy-protective results, despite textual and other impediments, can derail legislative momentum by giving the impression that only minor, piecemeal statutory changes are necessary to address problems that in fact should be the subject of far broader reforms.

A. The Spyware Problem in Context

The challenges of applying surveillance law to spyware are not unique. Litigants and commentators have increasingly invoked electronic surveillance statutes in an effort to curb perceived privacy-invasive practices in-

volving electronic communications. Such efforts usually encounter the same impediments as discussed in Part III. Attempts to use surveillance law to challenge employer monitoring of communications or to challenge online profiling activities provide useful examples. With respect to claims that employer monitoring violates surveillance statutes, the employer's efforts to acquire the employee's consent to the monitoring will typically defeat any Wiretap Act claim, even if communications are monitored during the transmission phase. SCA claims typically fail because the employer acts as a service provider and thus could "authorize" the conduct in question. I have already discussed some aspects of the online profiling cases—that is, cases involving third-party advertisers' use of cookies to gather data across a range of websites. As noted, both Wiretap Act and SCA claims have typically foundered on the consent element.[169]

In observing that efforts to use litigation to improve privacy practices with respect to electronic communications have generally been unsuccessful, I do not intend to suggest that privacy-protective outcomes do not exist—or, for that matter, that decisions rejecting Wiretap Act or SCA claims are incorrect. In cases involving particularly bad facts, courts have on occasion allowed surveillance law claims to proceed. With respect to employer monitoring, the case of *Konop v. Hawaiian Airlines, Inc.*,[170] which involved a supervisor gaining access to an employee's password-protected website, comes to mind. In that case, the Court of Appeals for the Ninth Circuit rejected a Wiretap Act claim but allowed an SCA claim to proceed past the summary judgment phase.[171] The unique facts of the case—including that the employer did not act as a service provider with respect to the communications in question—make the case sufficiently narrow that it is unlikely to influence subsequent decisions involving more conventional facts. Moreover, as noted below, the *Konop* case itself involves a highly questionable application of the SCA.[172] With respect to the use of cookies, the *Pharmatrak* decision reflects one instance in which a court allowed a Wiretap Act claim to proceed even though the companies whose websites facilitated Pharmatrak's placement of cookies on users' computers arranged for Pharmatrak's services.[173] In addition, even the

169. *See supra* notes 124-133 and accompanying text; *see also infra* note 245 and accompanying text.

170. 302 F.3d 868 (9th Cir. 2002).

171. As discussed below, the court initially allowed the Wiretap Act claim to proceed but abandoned its analysis following a petition for rehearing. *See infra* notes 277-293 and accompanying text.

172. *See infra* note 293.

173. *See supra* notes 134-141 and accompanying text.

cookie cases preceding *Pharmatrak* are interesting in that they rely on consent as the basis for dismissal, when the plaintiffs' claims could potentially have foundered on a number of other grounds (a point to which I return below). The next Section discusses several other cases in which courts faced with bad facts have attempted to draw certain privacy-invasive conduct within the domain of surveillance law.

For our purposes, the interesting question is whether those cases involving *unsuccessful* challenges to privacy-invasive conduct are the result of reasonable application of statutes that are simply too narrow to reach the challenged conduct or the result of misinterpretation. After reading many of the cases that attempt to apply surveillance statutes, particularly to private conduct, one might conclude that cases rejecting surveillance law claims simply reflect confused application of very complex statutes. Courts routinely report substantial confusion concerning how to apply surveillance statutes,[174] particularly with respect to some of the issues discussed earlier in this Article—such as how to draw the line between the Wiretap Act and the SCA[175] and what it means for a communication to be in electronic storage.[176]

My own view, however, is that the failure of electronic surveillance law to curb or reform seemingly privacy-invasive practices is mainly attributable to the problem of narrow drafting rather than the problem of misinterpretation. In particular, ECPA pre-dates the development of our electronic communications infrastructure.[177] Certain electronic communication services existed in 1986, and Congress recognized that such services were unlikely to be widely used unless it provided some statutory protection for electronic communications.[178] The technical aspects involved in the transmission of a communication were largely the same as

174. *See, e.g.*, Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (calling Wiretap Act "famous (if not infamous) for its lack of clarity"); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (suggesting that *Steve Jackson Games* court "might have put the matter too mildly"); *Konop*, 302 F.3d at 874 ("Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.").

175. *See supra* note 34 and accompanying text; *infra* notes 183-189, 281-293 and accompanying text.

176. *See supra* notes 162-167 and accompanying text; *infra* notes 254-274 and accompanying text.

177. *See, e.g.*, *Konop*, 302 F.3d at 874 (noting that complexity of surveillance law "is compounded by the fact that ECPA was written prior to the advent of the Internet and the World Wide Web" and that "the existing statutory framework is ill-suited to address modern forms of communication").

178. *See supra* note 41 and accompanying text.

they are today, in that messages were stored regularly as part of the transmission process.[179] In addition, it was not uncommon for businesses to contract for off-site computer storage or processing services; Congress thus also understood the need to protect such remotely stored files.[180] But the Internet as we know it did not exist in 1986. Congress simply did not envision how concepts such as "electronic communication," "electronic communication service," "facility," and "electronic storage" would map onto the Internet.

One example will suffice to illustrate how the concepts reflected in the Wiretap Act and the SCA are difficult to map onto the Internet more broadly. Under the Wiretap Act, acquisition of communications with the consent of one party are not considered unlawful interceptions;[181] similarly, conduct undertaken with the consent of a user of an electronic communication service will not run afoul of the SCA.[182] A consent exception under the original version of the Wiretap Act may have been quite sensible, in that any wire or oral communication likely would have involved a relatively small number of parties, with respect to whom the speaker could gauge the risk that the conversation would be recorded or revealed. The extension of the concept to electronic communications is similarly understandable when a relatively small number of parties are involved. The concept of one-party consent, however, becomes meaningless when applied not to personal communications, but to arms'-length transactions—where a user does not or cannot know of the contractual arrangements the other party may have with third parties and therefore lacks the data to gauge the privacy risks involved.

But even if courts could adequately address issues of consent and map other statutory terms onto the Internet, a more fundamental problem exists: our surveillance law statutes, as written, simply are not general data privacy statutes. In other words, the statutes do not broadly identify a particular category of personal data that should be subject to protection or restrict the acquisition, use, or transfer of such data. The Wiretap Act deals narrowly with *communications* that are *transmitted*, not with any other

179. *See, e.g.*, Brief on Rehearing En Banc of *Amicus Curiae* Technical Experts In Support of Appellant, Urging Reversal, United States v. Councilman 6-8 (1st Cir. Nov. 12, 2004) (No. 03-1383), *available at* http://www.epic.org/privacy/councilman/tech_amicus.pdf (noting that technical specifications for e-mail were developed prior to ECPA's passage in 1986).

180. *See* S. REP. NO. 99-541, at 10 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3564.

181. 18 U.S.C. § 2511(2)(c), (d) (2000).

182. *Id.* § 2701(c)(2).

data that an individual might attempt to shield or any other process by which it might be revealed. The SCA protects only communications, and only at a very specific point in the communications process: in electronic storage in the system of an electronic communications service.

That is not to say that all cases rejecting Wiretap Act or SCA claims are properly decided. For example, the U.S. Court of Appeals for the First Circuit, sitting *en banc*, recently reversed a highly problematic decision dismissing a Wiretap Act claim. In *United States v. Councilman*,[183] a district court considered whether an Internet service provider that captured communications of its customers before transmitting them into users' mailboxes had intercepted those communications. The communications were acquired during a brief period of storage in the ISP's system before transmission to the user's mailbox.[184] Because the communications were acquired during this brief period of storage, the district court concluded that the communications were not intercepted for purposes of the Wiretap Act.[185] A panel of the Court of Appeals for the First Circuit affirmed on the same reasoning.[186]

Although several courts construing the Wiretap Act had held that the statute does not protect stored communications,[187] those cases differed from *Councilman* in an important respect. The previous cases each involved a *one-time acquisition* of communications maintained by a service provider *for retrieval by the subscriber. Councilman*, in contrast, involved an *ongoing acquisition* of communications briefly stored during the transmission process *prior to being made available to the subscriber.* The implications of the district court's and panel majority's conclusion for electronic communications were profound. By virtue of the architecture of the Internet, electronic communications are stored at numerous points during transmission. Under the district court's and panel majority's reasoning, a communication would move in and out of the Wiretap Act's protective umbrella depending upon whether, at a given moment in time, the communication was between or within the computers relaying it.

The *en banc* court's reversal of the *Councilman* decision was thus a welcome result. The case nevertheless highlights one of the real difficul-

183. 245 F. Supp. 2d 319 (D. Mass. 2003) [hereinafter *Councilman I*], *aff'd*, 373 F.3d 197 (1st Cir.) [hereinafter *Councilman II*], *reh'g en banc granted and opinion withdrawn*, 385 F.3d 793 (1st Cir. 2004), *on reh'g en banc*, No. 03-1383, 2005 U.S. App. LEXIS 16803 (1st Cir. Aug. 11, 2005).

184. *Councilman II*, 373 F.3d at 199.

185. *Councilman I*, 245 F. Supp. 2d at 321.

186. *Councilman II*, 373 F.3d at 204.

187. *See supra* note 34 (citing cases).

ties in applying surveillance law to private conduct. I discussed in Part II the fact that understanding the Fourth Amendment backdrop to each statute is crucial to applying the relevant terminology. This point is often missed by courts construing the statutes in cases involving civil or criminal actions against private parties rather than in the context of a motion to suppress evidence gathered by the government.[188] In *Councilman*, the district court's and panel majority's conclusion that a service provider can acquire the contents of a communication prior to completion of the transmission phase, merely because it is stored at a point in the transmission process, would have dramatically expanded the government's access to electronic communications: the government could have relied on the less stringent procedures of the SCA to compel production of a communication at any one of a number of points along its transmission path, rather than obtaining a Title III order.[189] Had the courts fully considered that fact, it seems unlikely that they would have reached the same result. Courts applying statutes to private conduct in isolation, without attention to the manner in which interpretations affect government conduct, are likely to apply surveillance statutes erroneously. Those errors, of course, can run in either direction: sanctioning privacy-invasive conduct by private parties, thereby opening avenues for the government to engage in the same conduct, and limiting privacy-invasive conduct, thereby constraining investigative tools available to the government.

Even if we accept that interpretation of surveillance statutes is difficult, and that some cases rejecting Wiretap Act or SCA claims are erroneous, the fact remains that surveillance law statutes are very narrowly drafted, and that much privacy-invasive conduct with respect to electronic communications remains outside of their terms.[190] That observation begs

188. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HAST. L.J. 805, 807 (2003) ("[C]ourts have not explained how the complex web of surveillance statutes apply in routine criminal cases, but instead have interpreted those statutes in unexpected civil contexts where the implications of the court's decision for the bulk of criminal cases tends to be unknown to the court and ignored by the parties.").

189. *See, e.g.*, Brief on Rehearing *En Banc* for Senator Patrick J. Leahy as *Amicus Curiae* Supporting the United States and Urging Reversal, United States v. Councilman 10-11 (1st Cir. Nov. 12, 2004) (No. 03-1383), *available* at http://www.cdt.org/wiretap/20041112leahy.pdf; Supplemental Brief of Center for Democracy and Technology et al., United States v. Councilman 1-4 (1st Cir. Nov. 12, 2004) (No. 03-1383), *available at* http://www.cdt.org/wiretap/20041112joint.pdf.

190. For another view that surveillance statutes are narrowly drafted and that courts erroneously apply them to a range of conduct, see Kerr, *supra* note 188, at 807 (arguing that surveillance law "remains unusually obscure, and the rare judicial decisions construing the statutes tend to confuse the issues, not clarify them").

the question of whether courts should more aggressively interpret surveillance statutes to provide broader privacy-protective functions, at least in cases involving private parties. The remainder of this Part explores that question. I argue that aggressive interpretations of surveillance statutes are unlikely to achieve lasting privacy benefits. Although one could offer a range of examples of privacy-protective but deeply flawed applications of surveillance law, I focus on three examples in particular: *United States v. Smith*,[191] *In re Pharmatrak Privacy Litigation*[192] (and its antecedents), and *Theofel v. Farey-Jones*.[193] I begin by explaining the difficulties each case presents as a matter of statutory interpretation; I then explore the broader consequences of the courts' approaches for privacy and for legislative momentum.

B. Deconstructing Courts' "Privacy-Protective" Approaches

1. *United States v. Smith*

United States v. Smith dealt with a frequently litigated and extremely complex issue: how the Wiretap Act's prohibition on interception of communications relates to the SCA's prohibition on acquisition of communications in electronic storage.[194] Although the case concerned wire communications rather than electronic communications, the implications of the decision for electronic communications were potentially quite significant. The Court of Appeals for the Ninth Circuit ultimately concluded that a private party could "intercept" a voicemail message even when the message was acquired from electronic storage within the voicemail provider's system.[195] The court's effort to reconcile its interpretation of the Wiretap Act with the existence of the SCA, however, resulted in an extremely confused interpretation of both statutes.

In *Smith*, a third party acquired the contents of a voicemail message by guessing a co-worker's password;[196] the message revealed possible insider trading.[197] Section 2511 prohibits the interception of a wire communication, whereas § 2701(a) of the SCA creates civil and criminal liability for one who "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby

191. 155 F.3d 1051 (9th Cir. 1998).

192. 329 F.3d 9 (1st Cir. 2003).

193. 341 F.3d 978 (9th Cir. 2003), *reh'g denied and opinion superseded*, 359 F.3d 1066 (9th Cir. 2004).

194. *Smith*, 155 F.3d at 1055.

195. *Id.* at 1059.

196. *Id.* at 1054.

197. *Id.* at 1053.

obtains . . . a wire . . . communication while it is in electronic storage in such system."[198] The determination of which statute governs the acquisition of a voicemail message by a private party is important, because § 2515 of the Wiretap Act requires exclusion of any wire or oral communication that has been illegally intercepted,[199] whereas the SCA lacks such an exclusionary rule.[200] In a criminal trial on the insider trading charges, the district court suppressed a tape of the voicemail message on the theory that it had been intercepted.[201] The district court declined to suppress other evidence despite the defendant's claim that it was derived from the illegally intercepted voicemail message.[202]

When the defendant challenged this ruling on appeal of his conviction, the government argued that the district court was correct to rule that the evidence was not derived from the voicemail message.[203] As an alternative basis for affirmance, the government also argued that the voicemail message was not in fact intercepted within the meaning of the Wiretap Act. Rather, the government suggested, the third party's retrieval of the voicemail message violated only § 2701(a) of the SCA; thus, any evidence derived from the acquisition did not need to be suppressed. In other words, the government argued that § 2511 covers acquisition of a communication only while it is being transmitted, while § 2701(a) covers acquisition of a communication once it is in storage.[204]

Although the court ultimately concluded that the evidence in question was not derived from the voicemail message,[205] it treated the government's claim that the SCA, and not the Wiretap Act, governed the case as a "threshold issue."[206] The court rejected the government's transmission/storage distinction and concluded that a private party could "intercept" a stored voicemail message.[207] The court acknowledged that the government's narrower interpretation of the Wiretap Act comported with the ordinary meaning of the term "intercept"—"'to take, seize, or stop by the way or *before arrival at the destined place*'"—but concluded that this

198. 18 U.S.C. § 2701(a)(1) (2000).

199. 18 U.S.C. § 2515 (2000).

200. The SCA allows for civil damages and criminal penalties and deems those remedies exclusive. *See* 18 U.S.C. § 2707 (2000 & Supp. II 2002) (civil action); *id.* § 2701(b) (criminal penalties); *id.* § 2708 (exclusivity of remedies).

201. *Smith*, 155 F.3d at 1054.

202. *Id.*

203. *Id.* at 1055.

204. *Id.* at 1056-57.

205. *Id.* at 1063.

206. *Id.* at 1055.

207. *Id.* at 1059.

ordinary meaning did not control.[208] The court's reasoning rested in part on a feature of the Wiretap Act that was later eliminated (subject to a sunset provision) in the USA Patriot Act. In particular, § 2510(1) had defined the term "wire communication" to cover "any electronic storage of such communication"[209]; the USA Patriot Act temporarily excised this portion of the definition.[210]

The court's approach suffers from numerous flaws. First, if acquisition of a voicemail message from electronic storage is an interception, then § 2701(a)'s coverage of the acquisition of wire communications from electronic storage is redundant or nonsensical. The court attempted to deflect this argument by reasoning that the Wiretap Act and the SCA cover two different things: the Wiretap Act prohibits acquiring the contents of the communication, whether the communication is in transit or in storage, whereas the SCA prohibits gaining "access" to a communication—with "access" understood to mean conduct that puts a person "*in position to acquire* the contents of a communication."[211] In other words, under the *Smith* court's reasoning, the Wiretap Act covers the acquisition of the communication, whereas the SCA covers preliminary conduct placing one in position to acquire a communication. There are significant problems with this approach. First, in reaching its conclusion, the court conflated two different uses of the word "access" in § 2701(a) and altered the grammatical structure of the prohibition. Section 2701(a) covers one who "intentionally accesses" a "facility" through which an electronic communication service is provided. Drawing on this language, the court observed that the Wiretap Act refers "pointedly" to intercepting a particular communication, while § 2701 refers "broadly" to accessing a communications facility.[212] The court reasoned that "[o]ne assuredly can access a communications facility—such as a company voicemail system—without listening to or recording any of the messages stored within that facility."[213] The court implied that such conduct, without more, would violate the SCA.[214] Section 2701(a), however, requires more than gaining access to a covered facility: one must also "obtain[], alter[], or prevent[] authorized access to a wire or

208. *Id.* at 1057 (quoting WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1176 (1986)) (emphasis in opinion).

209. 18 U.S.C. § 2510(1) (2000).

210. *See* Pub. L. No. 107-56, § 209(1), 115 Stat. at 283 (codified at 18 U.S.C. § 2510(1) (Supp. II 2002)); *id.* § 224, 115 Stat. at 295 (applying sunset provision to § 209).

211. *Smith*, 155 F.3d at 1058 (emphasis added).

212. *Id.* at 1059.

213. *Id.*

214. *Id.*

electronic communication while it is in electronic storage in such system." In other words, the conclusion that merely being in a position to acquire the contents of a communication violates the SCA requires excising the last portion of the prohibition, and focusing on "access[] to a facility" as the sole prohibited conduct.

The court also looked to the second appearance of the word "access" in § 2701(a) and concluded that to "obtain[] . . . access" is to be in a position to acquire its contents, not to actually acquire those contents. Even if that were an appropriate reading of the phrase "obtain[] . . . access," one must alter the grammatical structure of the prohibition to conclude that "obtain[] . . . access" is the operative phrase in the statute. As noted, Section 2701(a) reaches "whoever . . . intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby *obtains*, *alters*, or *prevents authorized access* to a wire or electronic communication while it is in electronic storage."[215] In reading the provision to prohibit one from "obtain[ing] . . . access" to a communication, however, the court assumes that "access" is the direct object of the verb "obtains." Under this approach, the statute reaches one who "obtains . . . access to a wire or electronic communication," "alters . . . access to a wire or electronic communication," or "prevents authorized access to a wire or electronic communication." The phrase "alters . . . access" is awkward; the more natural reading of the prohibition is that it reaches one who "obtains . . . a wire or electronic communication," "alters . . . a wire or electronic communication," or "prevents authorized access to a wire or electronic communication." When so read, the prohibition does not in fact cover gaining access to a facility and thereby "obtain[ing] . . . access" to a communication in electronic storage. Rather, it covers gaining access to a facility and thereby "obtain[ing] . . . a communication" in electronic storage. The court's conclusion that the SCA covers only conduct that places one in a position to obtain the contents of a communication is thus flawed. The court's interpretation of the Wiretap Act does render the SCA, properly read, redundant, because both statutes would cover acquisition of a stored wire communication.

The *Smith* court also buttressed its conclusion by focusing on the definition of "wire communication" under the Wiretap Act.[216] Prior to the passage of the USA Patriot Act, § 2510(1) defined a wire communication to include storage of such a communication. The *Smith* court reasoned that the inclusion of that phrase would be rendered meaningless if stored wire

215. 18 U.S.C. § 2701(a) (2000).
216. *Smith*, 155 F.3d at 1058.

communications could not be intercepted.[217] Here, the court ignored the most likely explanation for the reference to stored wire communications in § 2510(1). Prior to the passage of the USA Patriot Act, the SCA in fact required the *government* to seek a Title III order before acquiring the contents of any wire communication in electronic storage. Section 2701(a) prohibits the acquisition of wire or electronic communications in electronic storage, but § 2701(c)(3) exempts authorized government conduct—specifically, prior to the Patriot Act's passage, conduct authorized under §§ 2703 and 2704 of ECPA and under § 2518 of the Wiretap Act.[218] Prior to the passage of the USA Patriot Act, and when *Smith* was decided, the first two of these provisions described only how the government may compel a service provider to produce or preserve the contents of stored *electronic* communications: subsections (a) and (b) of § 2703 established the means by which law enforcement officials could require a service provider to disclose the contents of electronic communications,[219] while § 2704 authorized the government to require a service provider to create a backup copy of the contents of electronic communications pending resolution of any proceedings concerning the government's subpoena or court order.[220] Because both § 2703 and § 2704 omitted reference to any process by which the government could obtain or compel production of the contents of stored *wire* communications,[221] the reference in § 2701(c) to § 2518—the provision of the Wiretap Act under which a court grants an order authorizing law enforcement conduct—could only relate to government access to stored *wire* communications.

Accordingly, at the time *Smith* was decided, if the government wished to acquire wire communications in electronic storage without violating § 2701(a), it had to obtain a Title III order.[222] The report of the House Committee on the Judiciary accompanying ECPA confirms this reading of the statute. The analysis of § 2703, which, as noted, then governed access to the contents of electronic communications in electronic storage, states:

---

217. *See id.* at 1058 & n.12.

218. 18 U.S.C. § 2701(c)(3) (2000).

219. *Id.* § 2703(a), (b).

220. *Id.* § 2704.

221. Section 2703(d), which set forth circumstances under which a court may order a service provider to disclose a communication, did refer to "the contents of a wire . . . communication." Since the government could only seek an order under § 2703(d) for disclosure of electronic communications, see *id.* § 2703(b)(1)(B)(ii), and subscriber or customer records, see *id.* § 2703(c)(1)(B), the reference was apparently inadvertent.

222. The USA Patriot Act altered this requirement by adding procedures to compel production of wire communications to §§ 2703(a) and (b). *See* Pub. L. No. 107-56, § 209(2), 115 Stat. at 283 (codified at 18 U.S.C. §§ 2703(a), (b) (Supp. II 2002)).

"The contents of the voice portion of a wire communication in storage such as with 'voice mail' *may not be obtained under this section. [T]he provisions of chapter 119 of title 18 [i.e., the Wiretap Act] apply.*"[223] As this discussion suggests, the inclusion of "electronic storage" within the definition of a "wire communication" in the Wiretap Act served only to emphasize the procedure that law enforcement officials had to follow to gain access to voicemail messages. Under this reading, one can conclude that a private party's acquisition of stored communications violates only the SCA and still give effect to the phrase "electronic storage" in the definition of "wire communication."

Finally, in concluding that acquisition of voicemail message constitutes an interception for purposes of the Wiretap Act, the *Smith* court effectively held that the single prohibition on intercepting communications in § 2511(1)(a) would have a different meaning depending on whether wire or electronic communications were at issue. Cases addressing whether acquisition of electronic communications in electronic storage violates not only the SCA but also the Wiretap Act have held that the Wiretap Act only governs the acquisition of communications during transmission.[224] Prior to the passage of the USA Patriot Act, some courts reaching that conclusion relied in part on the inclusion of the phrase "electronic storage" in the definition of a wire communication and the exclusion of that phrase in the definition of an electronic communication.[225] The *Smith* court distinguished those cases on that basis.[226] The effect of the *Smith* decision, however, is that "intercept" is defined differently depending on the type of communication: for wire communications, intercept

223. H.R. Rep. No. 99-647, at 67-68 (emphasis added); *see also* S. Rep. No. 99-541, at 12, *as reprinted in* 1986 U.S.C.C.A.N. at 3566 (noting that amendment to definition of "wire communication" to include "any electronic storage of such communication" was designed "to specify that wire communications in storage like voice mail, remain wire communications, and are protected accordingly"). The House Report's reference to "the voice portion" of a wire communication is somewhat opaque, as a wire communication by definition contains the human voice. The error appears to be a relic of an earlier version of ECPA, in which § 2703(a) applied to government access to "non-voice wire communications." In any event, the Report's statement that Title III applies to stored voice communications is unambiguous.

224. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); Wesley Coll. v. Pitts, 974 F. Supp. 375, 388 (D. Del. 1997), *aff'd*, 172 F.3d 861 (3d Cir. 1998); Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996); United States v. Reyes, 922 F. Supp. 818, 837 (S.D.N.Y. 1996).

225. *See Steve Jackson Games*, 36 F.3d at 461-62; *Wesley Coll.*, 974 F. Supp. at 386; *Reyes*, 922 F. Supp. at 836.

226. *Smith*, 155 F.3d at 1057.

means the acquisition of a communication in transit or in electronic storage, but for electronic communications, intercept means only the acquisition of a communication in transit. That approach overlooks the fact that, under the Wiretap Act, all communications are encompassed in a single prohibition providing for criminal punishment and a private right of action against one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[227] To assign a different meaning of the term, depending on whether a wire or electronic communication was at issue, would be highly anomalous.[228]

Smith is illustrative of how courts can do violence to statutory text by reading electronic surveillance statutes in privacy-protective ways. Although the *Smith* court ultimately denied the defendant's motion to suppress,[229] the decision was privacy-protective in that the court would have applied the more restrictive provisions of the Wiretap Act to the defendant's conduct. As discussed below, however, *Smith* is among the privacy-protective cases that have in some sense unraveled.

2. *In re Pharmatrak, Inc. Privacy Litigation and its Antecedents*

In re Pharmatrak, Inc. Privacy Litigation and the "cookie" cases that preceded it provide a second example of courts reading surveillance statutes too broadly. As previously noted, the cases typically involved claims that use of cookies violated the Wiretap Act, the SCA, and the CFAA.[230] *In re Pharmatrak Privacy Litigation*[231] presents a rare example of a case in which a claim that placement of a cookie on a user's hard drive, coupled with other conduct, violated a surveillance law statute was allowed to proceed. In particular, the Court of Appeals for the First Circuit overturned a

---

227. 18 U.S.C. § 2511(1)(a) (2000).

228. The discussion above suggests that the court's textual and structural arguments are unpersuasive. The court also dismissed the Senate and House reports accompanying ECPA because it found the reports' discussions of whether the wiretap provisions or the stored communications provisions govern acquisition of stored communications to be inconsistent: The Senate report suggests that stored wire communications are protected by Title III, while the House report suggests that they are subject to the stored communications access provisions of ECPA. *See Smith*, 155 F.3d at 1056 n.9. The reports, however, can be easily reconciled, on the theory that the Senate report is focusing on *government* access to stored wire communications (which must occur via a Title III order) and the House report is focusing on *non-governmental* access to stored communications (which is regulated by the prohibitions of § 2701(a) of the SCA). *See supra* notes 217-223 and accompanying text.

229. *Smith*, 155 F.3d at 1063.

230. *See supra* notes 123-142 and accompanying text.

231. *Pharmatrak II*, 329 F.3d at 9.

district court's grant of summary judgment to Pharmatrak on a Wiretap Act claim.[232] The court of appeals' reasoning, though privacy-protective, has significant problems. Some of those problems simply build upon problems in prior "cookie" cases. Although most of the cookie cases preceding *Pharmatrak* resulted in summary judgment to the defendant or dismissal, they reflect unusual and unduly broad interpretations of portions of the electronic surveillance statutes.

The first and most important case in the series of cookie cases was *In re DoubleClick Inc. Privacy Litigation*,[233] a class action suit by individuals alleging that DoubleClick's use of cookies resulted in the unauthorized acquisition of personally identifiable information in violation of federal law.[234] Although the court granted DoubleClick's motion to dismiss the Wiretap Act and SCA claims on the ground that DoubleClick's conduct fell within exceptions in each statute for certain consensual conduct,[235] the court assumed, or DoubleClick conceded, that certain substantive predicates for liability with respect to each statute were met.[236] Despite the fact that other portions of the opinion rendered the *DoubleClick* court's conclusion with respect to the substantive predicate for liability dictum, the *DoubleClick* court's framework paved the way for other courts to take a similar approach, with some bizarre consequences.

The premise of the *DoubleClick* plaintiffs' claim that use of cookies violated the Wiretap Act was that DoubleClick had acquired private information when interaction between the plaintiffs' computers and DoubleClick-affiliated websites caused that information to be incorporated into a URL.[237] The plaintiffs claimed that acquisition of the communications constituted an interception.[238] DoubleClick's motion to dismiss rested on the view that any interception was undertaken with the consent

232. *See Pharmatrak I*, 220 F. Supp. 2d at 12 (granting summary judgment on Wiretap Act claim), *rev'd*, *Pharmatrak II*, 329 F.3d at 9. The court of appeals remanded for further consideration of whether Pharmatrak's conduct satisfied the intent requirement of the Wiretap Act. On remand, the district court again granted summary judgment to Pharmatrak. 292 F. Supp. 2d 263 (D. Mass. 2003).

233. 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

234. For discussion of the factual basis for the claims, see *supra* notes 127-131 and accompanying text.

235. *DoubleClick*, 154 F. Supp. 2d at 514, 519.

236. *See id.* at 508 ("Assuming the communications are considered to be in 'electronic storage,' it appears that plaintiffs have adequately pled that DoubleClick's conduct constitutes an offense under § 2701(a) . . . ."); *id.* at 514 (noting DoubleClick's concession for purposes of motion to dismiss that its conduct, as pled, violated Wiretap Act's prohibition on interception).

237. *See id.* at 504; *supra* notes 130-131 and accompanying text.

238. *DoubleClick*, 154 F. Supp. 2d at 514.

of a party to the communication—that is, the website for which DoubleClick had arranged to provide advertising. The *DoubleClick* court agreed. The court apparently accepted DoubleClick's concession that the substantive predicates for liability under the Wiretap Act were otherwise met. But note the extremely awkward fit between DoubleClick's conduct and the offense under the statute. Recall that the Wiretap Act prohibits the interception of electronic communications and defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[239] Assuming that the personally identifiable information constitutes the "communication" that was intercepted, it is not clear what "device" DoubleClick used to intercept that communication. The cookie is not itself an intercepting device; the cookie is merely stored on the user's hard drive and communicated to DoubleClick by the user's browser at an appropriate time. DoubleClick may associate information with this cookie in its own database, but the cookie itself does not gather information. To the extent that DoubleClick has access to personally identifiable information, it has access because *the user's browser* and *its client's site* are configured in such a way as to reveal this information. It is difficult to see how this constitutes an interception on DoubleClick's part.[240]

Although the court's ultimate conclusion that the DoubleClick-affiliated sites did consent to any interception meant that the court's apparent assumption that the substantive predicate for liability under the Wiretap Act was met was of little consequence in *DoubleClick* itself, that assumption essentially hardened into law in the court of appeals decision in *Pharmatrak*. Recall that Pharmatrak tracked certain data for several pharmaceutical company clients through the use of cookies.[241] As in *DoubleClick*, the plaintiffs claimed that Pharmatrak intercepted certain personally identifiable information that they revealed to the pharmaceutical companies by filling out electronic forms on the companies' websites.[242] The court of appeals found that any "consent" by Pharmatrak's pharmaceutical partners was too general to trigger the § 2511(d) exception.[243] The *Pharmatrak* court's underlying premise was that Pharmatrak's conduct satisfied

239. 18 U.S.C. § 2510(4) (2000).

240. For related criticism of *DoubleClick* and its progeny, see Kerr, *supra* note 188, at 830-33 (characterizing the court's interpretations as "hallucinogenic").

241. Pharmatrak II, 329 F.3d at 12.

242. *Id.* at 15-16.

243. *Id.* at 20 (concluding that mere purchase of service does not always imply consent).

the elements of § 2511(1)(a)[244]—except for the element of intent, as to which the court remanded for further consideration. Again, however, any information revealed to Pharmatrak was revealed because the user's browser was configured to reveal it or because the pharmaceutical companies' sites were configured in such a way as to reveal it.

The reasoning of courts considering whether use of cookies violates the SCA is equally problematic. There too, courts typically disposed of the claims on the issue of consent—under the exception in § 2701(c)(2) for conduct authorized "by a user of [a wire or electronic communication service] with respect to a communication of or intended for that user."[245] Several courts glossed over the numerous problems with applying the statutory framework at all, either by assuming the elements of the SCA were met or relying on parties' concessions. I alluded to some of these problems above in my discussion of spyware. First, it is difficult to identify a "facility through which an electronic communication service is provided" to which the content provider or advertiser gains unauthorized access.[246] In *DoubleClick*, for example, the plaintiffs seemed to object to the access that DoubleClick had *to the user's hard drive* in placing a cookie.[247] But even if the user's hard drive is properly viewed as a "facility"—a proposition that the *DoubleClick* district court and other courts seemed to accept[248]—that facility provides no electronic communications service. The court treated "internet access" as the relevant electronic communication service,[249] but if it is, then the user's hard drive is not a "facility" through which this service is provided.[250]

---

244. *Id.* at 18 (discussing elements).

245. *See, e.g.*, *Pharmatrak I*, 220 F. Supp. 2d at 13-14; In re Toys R Us, Inc. Privacy Litig., 2001 WL 34517252, at *6 (N.D. Cal. 2001); Chance v. Avenue A, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001); In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001). *But see* In re Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1275 (discussing consent exception, but stating that "[i]t is unclear to the court how this exception buttresses defendant's contention").

246. The *Pharmatrak* district court recognized this problem. *See Pharmatrak I*, 220 F. Supp. 2d at 13.

247. *DoubleClick*, 154 F. Supp. 2d at 509 (referring to "personal computer" as "facility").

248. *See Toys R Us*, 2001 WL 34517252, at *2 n.7 (describing defendant's interpretation of 'facility' as "limited"); *Chance*, 165 F. Supp. 2d 1153, 1161 ("[I]t is possible to conclude that modern computers, which serve as a conduit for the web server's communication to Avenue A, are facilities covered under the Act."); *DoubleClick*, 154 F. Supp. at 508 (concluding that plaintiffs had adequately pled offense under § 2701(a)(1), and thus implicitly assuming that hard drive constituted facility).

249. *DoubleClick*, 154 F. Supp. 2d at 508.

250. *See Pharmatrak I*, 220 F. Supp. 2d at 13 ("The relevant *service* is Internet ac-

As noted, the *DoubleClick* court disposed of the SCA claim on a consent theory. In particular, the court reasoned that its acquisition of communications was authorized by the websites DoubleClick served, because the communications were intended for the websites and the companies providing primary content for sites had contracted with DoubleClick to engage in profiling activities—even if the companies did not know the specifics of whether DoubleClick would have access to personally identifiable information.[251] Again, because of the court's ultimate conclusion with respect to consent, its treatment of the other elements of the SCA may not seem important. But the *Pharmatrak* case illustrates the difficulty in this approach. Although the court of appeals in *Pharmatrak* did not address the plaintiffs' claims under the SCA,[252] its disposition of the issue of consent under the Wiretap Act suggests that it would reject the theory that Pharmatrak's website clients authorized acquisition of the communications at issue for purposes of the SCA's consent exception.[253] As with the Wiretap Act, then, the *DoubleClick* court's approach to the substantive predicate for liability has the potential to harden into an accepted framework for similar claims, despite the awkward fit with the statutory text.

3. *Theofel v. Farey-Jones*

Theofel v. Farey-Jones[254] provides a final example of a privacy-protective but deeply flawed application of surveillance law. A group of plaintiffs alleged that Farey-Jones, a plaintiff in a separate civil suit in which some of the *Theofel* plaintiffs were defendants, and his attorney improperly acquired their electronic communications.[255] In the course of discovery in the separate case, Farey-Jones's attorney issued a civil subpoena seeking certain communications from the *Theofel* plaintiffs' ISP.[256] The subpoena was overbroad and was subsequently quashed,[257] but only after the ISP complied and turned over numerous communications unrelated to the subject matter of Farey-Jones's lawsuit.[258] The *Theofel* plaintiffs filed

---

cess, and the service is provided through ISPs or other servers, not [through] Plaintiffs' PCs.").

251. *DoubleClick*, 154 F. Supp. 2d at 511.

252. The district court had granted Pharmatrak summary judgment on the SCA claims, *Pharmatrak I*, 220 F. Supp. 2d at 14, and the plaintiffs apparently did not appeal that disposition, *Pharmatrak II*, 329 F.3d at 13.

253. *See Pharmatrak II*, 329 F.3d at 19-22.

254. 341 F.3d 978 (9th Cir. 2003) [hereinafter *Theofel I*], *reh'g denied and opinion superseded*, 359 F.3d 1066 (9th Cir. 2004) [hereinafter *Theofel II*].

255. *Theofel I*, 341 F.3d at 982.

256. *Id.* at 981.

257. *Id.* at 981-82.

258. *Id.* at 981.

suit alleging violation of § 2701(a) of the SCA.[259]

The district court dismissed the SCA claim, apparently in part on the theory that the defendants acquired the communications with the authorization of the service provider.[260] The ISP had provided the defendants with access to the communications in response to the subpoena.[261] Section 2701(a) only covers unauthorized access to a communications facility. In addition, § 2701(c)(1) exempts from § 2701(a)'s coverage conduct authorized by the service provider.[262] If the ISP authorized the defendants' access, then § 2701(a) would not prohibit their conduct.

On appeal, the Court of Appeals for the Ninth Circuit reversed.[263] The court analogized § 2701(a) of the SCA to a common-law trespass action.[264] Although a defendant is not liable for a trespass if the plaintiff authorizes his conduct, in some circumstances (though not all) deceit will vitiate consent.[265] Here, because the subpoena was blatantly invalid, it could not form the basis for the ISP's consent to the defendants' access to the plaintiffs' communications.[266] In other words, since the ISP's authorization for the defendants' access to the communications was improperly obtained, it did not qualify as authorization at all.

The court also rejected the defendants' alternative argument that the communications to which the ISP provided access were not in "electronic storage," and therefore were not covered by the SCA.[267] Section 2701(a) of the SCA only prohibits obtaining, altering, or preventing authorized access to a communication while that communication is in electronic storage within the provider's facility.[268] Section 2510(17) defines "electronic storage" to include "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[269] The court acknowledged that other courts have limited application of the term electronic storage to communications not yet retrieved by the intended re-

259. The plaintiffs also brought Wiretap Act and CFAA claims, which I do not discuss here.

260. *Id.* at 982.

261. *Id.* at 981.

262. 18 U.S.C. § 2701(c)(1) (2000).

263. *Theofel I*, 341 F.3d at 985.

264. *Id.* at 983.

265. *Id.*

266. *Id.* at 983-84.

267. *Id.* at 984.

268. 18 U.S.C. § 2701(a) (2000).

269. 18 U.S.C. § 2510(17) (2000 & Supp. II 2002).

cipient.[270] The court concluded, however, that communications not deleted by the recipient and therefore remaining on the ISP's server are stored "for purposes of backup protection."[271]

In response to a petition for rehearing with a suggestion for rehearing en banc, the court replaced its discussion of "electronic storage" with a lengthier discussion reaching the same result.[272] In particular, the court rejected a suggestion by the United States in an *amicus* brief that the court's interpretation of "electronic storage" rendered substantial portions of the SCA irrelevant.[273]

Notwithstanding the egregiousness of the defendants' conduct, the court of appeals's effort to extend the SCA to reach the conduct is problematic for several reasons. First, § 2701(a) of the SCA requires a showing that a defendant gained unauthorized access to a facility through which an electronic communication service is provided. In this case, the relevant facility presumably would have been the service provider's mail servers. But the defendants never gained access to that facility at all. Instead, the service provider copied the e-mail messages in question and made them separately available to the defendants on a website.[274] As to the website, even if it were a "facility through which an electronic communication service is provided" for purpose of § 2701(a), the defendants' access was authorized: the service provider supplied the defendants with the link to the site. The service provider could just as easily have printed the communications and mailed them to the defendants. The court of appeals's application of § 2701(a) and its discussion of common law trespass gives one the impression that the defendants gained access to mailboxes on the service provider's servers dedicated to the plaintiffs' use, but that is simply not the case. In other words, the court took great pains to explain why defendants' access was unauthorized, when there was no "access" to the provider's mail servers at all.

In addition, on the issue of electronic storage, the Ninth Circuit's interpretation reflects a strained reading of the statutory text. The definition of "electronic storage" implies that, in a determination of whether a com-

---

270. *Theofel I*, 341 F.3d at 985.

271. *Id.*

272. *Theofel II*, 359 F.3d at 1069-70, 1076-77.

273. *Id.* at 1076. I alluded earlier to the government's view that messages held by a server after retrieval by a subscriber are no longer in electronic storage with the provider of an electronic communication service; if held by a public provider they are instead merely "held or maintained" by the provider of a remote computing service. *See supra* notes 162-165 and accompanying text.

274. *Theofel I*, 341 F.3d at 981.

munication is in backup protection, the relevant perspective is that of the *service provider*, not the user. The provision covers storage *by* the electronic communication service *for purposes* of backup protection. Moreover, the term "backup" presupposes the creation of a second copy of a communication. A user who simply chooses not to delete a communication may wish to continue to store the communication, but he or she is not actually "backing up" the communication. The court also completely overlooked the relevance of the fact that the defendants simply gained access to a web-based database for which the provider supplied a link rather than to the provider's mail server. There is no theory under which data indefinitely maintained on a website is in "temporary, intermediate storage" "incidental to its transmission." And the service provider's purpose in copying the communications to a web server was quite obviously not to provide backup protection, but to make the communications available to the defendants.

C. The Unraveling of Privacy-Protective Approaches

The cases above reflect instances of courts aggressively interpreting surveillance law statutes in a privacy-protective way in response to bad facts. Even when courts' approaches do not result in an ultimate ruling in favor of the party challenging a particular practice, they constrain other parties' behavior or mark an incremental step toward an ultimate ruling in favor of plaintiffs challenging similar practices. One might argue that courts' approaches are perfectly appropriate—that courts can and should aggressively interpret electronic surveillance statutes, particularly in light of the fact that technological changes have made it difficult to apply those statutes. There are serious difficulties with such a view, however. First, as this section illustrates, some privacy-protective approaches are sufficiently vulnerable on statutory interpretation grounds that they are likely to unravel. Second, as discussed in Section D, decisions that appear to be privacy-protective can derail momentum for legislative change—even when the decisions are sufficiently tailored to specific factual disputes that they are unlikely to affect a broad class of privacy threats.

United States v. Smith[275] provides a useful example of a case in which an approach that appeared to be privacy-protective ultimately unraveled. Congress, of course, amended the definition of wire communication in the SCA so as to overturn the specific result of the *Smith* case.[276] Both before and after Congress's action, however, the Ninth Circuit wrestled with the

275. 155 F.3d 1051 (9th Cir. 1998).

276. *See supra* notes 198-206 and accompanying text; *infra* notes 290-293 and accompanying text.

implications of *Smith* for cases involving private acquisition of *electronic* communications. The result was eventual abandonment of the *Smith* approach with respect to the Wiretap Act.

Konop v. Hawaiian Airlines, Inc.[277] involved claims that a Hawaiian Airlines supervisor violated both the Wiretap Act and the SCA by obtaining communications from the password-restricted portions of an employee's website. Konop, a pilot for Hawaiian Airlines, created and maintained a website where he posted bulletins critical of his employer and union officials.[278] Although the site was password-restricted, a Hawaiian Airlines supervisor, Davis, gained access to it by using the user names and passwords of employees who could legitimately use the site.[279] Konop claimed that the supervisor's conduct violated both the Wiretap Act's prohibition on interception of communications and the SCA's prohibition on accessing a facility without authorization and thereby "obtain[ing] . . . a communication in electronic storage" in that facility.[280]

In its first decision in the *Konop* case (*Konop I*), the Ninth Circuit applied *Smith*'s holding with respect to wire communications to the electronic communications at issue.[281] As noted above, *Smith*'s endorsement of prior precedent concluding that an *electronic* communication can only be intercepted during transmission, coupled with its adoption of a definition of interception that covered acquisition of stored *wire* communications, created an anomaly: the term "intercept" had two different meanings depending on whether wire or electronic communications were at issue.[282] The *Konop I* court acknowledged this problem,[283] but rather than recognizing the error of the *Smith* case, the court concluded that an electronic communication need not be acquired while in transmission to be intercepted for purposes of the Wiretap Act: "[T]he Wiretap Act protects electronic communications from interception when stored to the same extent as when in transit."[284]

Significant problems exist with the approach of the *Konop I* court, both on a practical level and as a matter of statutory interpretation. If acquisition of an electronic communication in storage constitutes an inter-

277. 236 F.3d 1035 (9th Cir. 2001) [hereinafter *Konop I*], *withdrawn*, 262 F.3d 972 (9th Cir. 2001), *new opinion filed*, 302 F.3d 868 (9th Cir. 2002) [hereinafter *Konop II*].

278. *Konop I*, 236 F.3d at 1041.

279. *Id.*

280. *Id.* at 1040.

281. *Id.* at 1046.

282. *See supra* notes 224-228 and accompanying text.

283. 236 F.3d at 1044.

284. *Id.* at 1046.

ception, then law enforcement officials would presumably need a full Title III order to acquire access to such communications. But requiring the government to seek a Title III order to acquire stored electronic communications would render the governmental access provisions of the SCA[285] meaningless, since law enforcement officials presumably could not use them. Moreover, the *Konop* court failed to consider the implications of extending *Smith*'s reasoning not only to ordinary electronic communications such as e-mail, but also to files held on a web server. Under the court of appeals' theory, any acquisition of such material against the wishes of the operator of the web server might constitute an interception for purposes of the Wiretap Act.[286] Perhaps concerned about this fact, the court emphasized that two exceptions would limit application of the Wiretap Act to viewing of a website: § 2511(2)(g)(i)'s exception for accessing an electronic communication "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public," and § 2511(2)(d)'s exception for acquisition of a communication where "one of the parties to the communication has given prior consent to such interception."[287] Because Konop's site was configured to require a password, neither exception applied. And even though Davis accessed the site by using the password of another pilot who did have authority to view Konop's posting, the court concluded that the other pilot was not in fact a "party" to the communication, because that pilot never actually participated in any communication with Konop.[288]

In light of the practical and interpretive difficulties, the *Konop I* court's decision was understandably the target of a petition for rehearing, and the court ultimately withdrew its opinion and abandoned its problematic reading of the Wiretap Act. The superseding opinion followed the line of cases, acknowledged in *Smith*, holding that interception of an electronic communication occurs only during the communication's transmission.[289] By the time the court of appeals reconsidered the case, the USA Patriot Act had eliminated the phrase "in electronic storage" from the definition of a wire communication.[290] The *Konop II* court therefore believed that it could, without disturbing the reasoning of *Smith*, abandon its previous conclusion that stored electronic communications could be intercepted.[291]

285. *See* 18 U.S.C. § 2703 (2000 & Supp. II 2002).
286. *See Konop I*, 236 F.3d at 1040.
287. *Id.* at 1046-47.
288. *Id.* at 1047.
289. *Konop II*, 302 F.3d at 878.
290. *Id.* at 877 n.5, 878; *see also supra* notes 198-206 and accompanying text.
291. *See id.* at 877-78.

Of course, the USA Patriot Act did not in any way affect the definition of the term "intercept," so there remained a strong argument that the *Smith* court's interpretation of that term (if correct) should still control. The dissent so argued,[292] although, as I have shown above, the *Smith* court's interpretation simply was erroneous and should have been more explicitly abandoned.[293]

Smith and *Konop* raise another interesting point about why aggressive interpretations of electronic surveillance statutes ultimately fail to provide greater privacy protection. The fact that surveillance statutes restrain both private parties and the government proves to be a double-edged sword. Because privacy-protective outcomes will constrain the government, the Justice Department has a significant incentive to oppose them. Indeed, the Justice Department, as *amicus curiae*, was one of the main proponents of rehearing both *Konop* and *Theofel*. The Justice Department's brief in *Konop* forcefully objected to the fact that, under that case's reasoning, the government would have to secure Title III orders before accessing stored communications—when the SCA clearly contemplated government access upon presentation of a search warrant (or, in some cases, a subpoena or special court order). Similarly, the *Theofel* court's conclusion that communications retained in a user's mailbox can be in backup storage prompted a petition for reconsideration by the government arguing that the court's interpretation would render portions of the SCA meaningless.[294]

To be sure, the government's incentives in this context are quite complicated. To the extent that the government succeeds in pressing for interpretations of surveillance statutes that allow for greater government access to communications, it constrains its own ability to prosecute bad actors.[295]

---

292. *Id.* at 891 (Reinhardt, J., dissenting).

293. While reversing its problematic reading of the Wiretap Act, the *Konop II* court adopted an equally strained reading of the SCA. As discussed earlier, the SCA prohibits one from intentionally accessing without authorization a facility through which an electronic communication service is provided, or exceeding an authorization to access that facility, and thereby "obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a)(1) (2000). Konop claimed that Davis's viewing of material posted on his website violated this provision. Applying this statutory framework to websites, however, is fraught with some of the same problems discussed with respect to spyware and the cookie cases. *See supra* notes 151-167 and accompanying text. A detailed discussion of this aspect of *Konop II* is beyond the scope of this Article.

294. *See supra* notes 273-274 and accompanying text.

295. For an argument that the dual nature of the Wiretap Act successfully limits aggressive government interpretations of the statute, see Paul K. Ohm, *Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1603 (2004).

The *Scarfo* and *Ropp* cases well illustrate that point: the government's argument in *Scarfo* that its keystroke monitor did not require a Title III order played a prominent role in the *Ropp* court's conclusion that a private party's use of a keystroke monitor did not violate the Wiretap Act.[296] The fact that the government both prosecutes offenses under and is constrained by application of the surveillance statutes can therefore act as a disciplining force. Indeed, the *Councilman* case provides a prominent example of a case in which the government opposed an interpretation of the Wiretap Act that would have been quite favorable to its interests. The district court and First Circuit panel majority essentially held that the Wiretap Act does not cover communications briefly stored at any point prior to being made available to the recipient.[297] Under the courts' reasoning, the government would not need to apply for a full Title III order before obtaining such communications; it could instead proceed under the less protective provisions of the SCA, which at most would require a search warrant.[298] The government nevertheless sought reversal of the decisions.

Despite the complexity of the government's incentives, the fact that the effects of too-aggressive interpretations of surveillance statutes will profoundly affect government investigations means that such interpretations will not go unchallenged.

D. The Impetus for Legislative Change

Apart from the instability of case law that aggressively interprets electronic surveillance statutes, such case law has potentially harmful effects on the momentum for legislative change. Here, the *Pharmatrak* case provides a useful example. Nearly all the cookie cases decided prior to *Pharmatrak* resulted in dismissal or summary judgment. To be sure, those cases could have more plainly shown how poor the fit was between the surveillance law statutes and the conduct complained of in those cases.[299] But to the extent that the conduct complained of in those cases was normatively objectionable (and I do not intend to express an opinion on this point), the dismissals made it more likely that such conduct would have been the subject of legislative attention, perhaps to develop a tailored data privacy statute. When a case such as *Pharmatrak* is decided, however, it appears that surveillance statutes *are* in fact successful in combating data privacy challenges posed by the Internet, rendering the need for a legislative response far less urgent.

---

296. *See supra* notes 93-113 and accompanying text.
297. *See supra* notes 114, 183-189 and accompanying text.
298. *See supra* note 189 and accompanying text.
299. *See supra* notes 230-253 and accompanying text.

Indeed, it is not difficult to envision the same phenomenon occurring with the *Councilman* case. The First Circuit panel majority's decision in June of 2004 was quickly condemned in the popular press, and a legislative fix was introduced soon after.[300] *Councilman* served an extremely useful function of bringing attention to the problems that arise at the intersection of the Wiretap Act and the SCA. The problems were in fact far more significant than popular accounts of the *Councilman* case suggested. In particular, although the district court and panel majority were quite clearly wrong to conclude that communications move in and out of the Wiretap Act's protective umbrella during transmission, depending on whether they are between or within computers transmitting them, a significant privacy problem lurks even now that the *Councilman* decision has been reversed by the *en banc* court. Because the defendant in *Councilman* acted as the provider of an e-mail service, he would have been entitled to access the communications in question as soon as the communications were made available in the system for retrieval by the subscriber. Even though such communications would have been in "electronic storage" in the provider's system for purposes of § 2701(a) of the SCA,[301] § 2701(c)(1) provides that the prohibition does not apply with respect to conduct authorized by the service provider.[302] In other words, Councilman's conduct clearly should have been covered by the Wiretap Act because the communications were seized prior to delivery to the subscriber's mailbox; but had Councilman only waited to seize the communications until they were stored in the subscriber's mailbox, retrieval of those communications would have been perfectly legal as a matter of federal law. The overturning of *Councilman* is a welcome result, but it has one unfortunate consequence: sapping much of the legislative momentum for reconsidering the intersection of the Wiretap Act and the SCA.

V. CONCLUSION

The prospects for using surveillance law to effect a significant change in spyware practices are quite limited. Although surveillance law may curtail extreme forms of spyware (if courts overcome obstacles that current case law imposes), a range of seemingly invasive practices will be unaffected, and there is virtually no prospect of reforming industry practices through surveillance law litigation.

The spyware story is simply not unusual. Plaintiffs have sought to use

300. *See, e.g.*, H.R. 4977, 108th Cong. (2004); H.R. 4956, 108th Cong. (2004).
301. 18 U.S.C. § 2701(a) (2000).
302. *Id.* § 2701(c)(1).

surveillance law statutes to address a number of digital-age privacy problems. In many cases, such efforts have failed. Perhaps more damaging, however, are some of the cases in which such efforts have succeeded. Aggressive privacy-protective approaches to surveillance law statutes do not last; they give a false sense that existing law is adequate; and they derail momentum for much-needed legislative change, both with respect to surveillance law itself and with respect to specific data privacy problems such as spyware. As I have suggested, we would do better simply to make surveillance law's limits plain.