IN RE PHARMATRAK & THEOFEL V. FAREY-JONES: RECENT APPLICATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

By Raechel V. Groom

A significant gap divides the popular perception of anonymity on the Internet and the reality of large amounts of data that users actually reveal during even a casual session of web browsing. Many Internet users may not know that they cannot anonymously shop or conduct research as they might in a physical store or library. The Internet has made accessible vast amounts of information on every topic imaginable. However, the very technologies that help us navigate the Internet also make users' web habits transparent and collectable to many individuals and businesses. Imagine, for example, that you have recently developed a health ailment and you use the Internet to visit pharmaceutical and preventative health care sites. These sites ask for information about you and your condition, which you provide. Without your knowledge, a third party records every website you visit, the information you provide to them, and the keywords you use to search them. The collection of such personal information could cause insurance companies to raise premiums if they discover that subscribers have expensive illnesses. Such surveillance could also lead to employers learning of employees' medical conditions, real or imagined, potentially affecting the employee's prospects for career advancement. Put simply, Internet users take the risk that their personal information could get into the wrong hands.

When Internet users have objected to profiling on the Web and to cookies and web bugs from Internet sites,[1] courts have refused to hold that such collection of personal information violates any right to privacy, but rather promotes a legitimate business practice.[2] Plaintiffs generally file

1. See *infra* Part I for an explanation of cookies and web bugs.

2. *See, e.g.*, Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001). For a thorough discussion of collecting and submitting an Internet user's personal data to law enforcement authorities, see U.S. Internet Serv. Provider Ass'n, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 BERKELEY TECH. L.J. 945 (2003) [hereinafter USISPA, *Guide*]. Although the Electronic Communications Privacy Act (ECPA) "regulate[s] how the government conducts electronic surveillance, [it] also impose[s] obligations on private parties, including ISPs." *Id.* at 947.

these claims based on the Electronic Communication Privacy Act (ECPA).[3] ECPA is the only viable federal statute for electronic privacy protection, but two recent cases demonstrate that it is at best a limited tool for protecting privacy on the Internet. Drafted in an era when only 50,000 computers were connected to the Internet, ECPA defines the core elements of a violation—intentionally "intercepting" or gaining unauthorized access to "stored" communications—in a way that is too strict for the Internet age.[4] To make matters worse, ECPA provides a consent-based defense for would-be violators that is so permissive as to render the statute ineffective in many situations. For example, in *In re Pharmatrak, Inc. Privacy Litigation*[5] the First Circuit held that a company that tracked and compared users' visits to pharmaceutical companies' websites had "intercepted" personally identifiable information, but in so holding set a standard for intent that eventually led to a summary judgment for the defendants.[6] In *Theofel v. Farey-Jones*,[7] the Ninth Circuit reversed a district court holding that e-mail turned over by an Internet Service Provider (ISP) pursuant to an overbroad civil subpoena was a stored communication, and the overbreadth of the subpoena had vitiated the ISP's consent.[8] Although *Theofel* vindicated the plaintiffs' privacy interest in their e-mail,[9] the manner in which the court reached this result points to the lack of clarity in ECPA, and suggests that other courts could reach contrary results.[10]

Part I of this Note provides a primer on the technologies at issue in *Pharmatrak*, which are also of more general significance for digital privacy. Part II describes the relevant provisions of ECPA and situates the Act in the larger framework of privacy regulation. Finally, Part III discusses how the major provisions of the Wiretap Act and ECPA were treated in *Pharmatrak* and *Theofel*, respectively.

---

3. 18 U.C.S. § 2707 (2000) (providing for civil remedies).

4. *See id.* § 2701.

5. 329 F.3d 9 (1st Cir. 2003) [hereinafter *Pharmatrak II*].

6. *Id.* at 32-35.

7. 341 F.3d 978 (9th Cir. 2003).

8. *Id.* at 983, 985.

9. *See id.* at 982 (noting that it was "Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage").

10. *See* USISPA, *Guide*, *supra* note 2, at 961 ("[*Theofel*] is the first appellate interpretation . . . and other circuits may come to different conclusions on the meaning of the language in [ECPA].").

I. TECHNOLOGICAL BACKGROUND

The plaintiffs in *Pharmatrak* alleged that Pharmatrak collected personal information from them via "web bugs," "cookies," and other devices.[11] A basic understanding of these technologies will help the reader understand why ECPA has become a common choice for privacy-related claims.

A. Cookies

Cookies are pieces of information sent when a person visits certain websites. They are often stored as small text files on the hard disk of the recipient.[12] Cookies may contain a username and password for a particular site, the last time a person visited the site, the person's favorite sites, and other customizable information.[13] In summary, cookies allow the key descriptive term to be tied to web users over time, which at least enables a website to say that the same computer has returned to the site. In addition, a website can allow third parties to set and read cookies.[14] They are often used to garner statistics about what types of pages people like to visit.[15]

B. Web Bugs

A web bug is an image in an e-mail or on a webpage used to allow a third party to detect when the webpage or e-mail is viewed. E-mail and webpages can contain instructions that direct the user's e-mail program or web browser to load an image—often invisible to the user—from a third party.[16] When the user's software loads the image from the remote server, the third party can record such information as the computer's IP address and the time the message was read or the webpage was accessed.[17] The server can also send a cookie along with the image.[18] This cookie can then be used to match a computer with personally identifying information.[19]

---

11. *In re* Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 5, 7 (S.D.N.Y 2001) [hereinafter *Pharmatrak I*].

12. PRESTON GRALLA, HOW THE INTERNET WORKS 299 (7th ed. 2003); D. Kristol & L. Montulli, HTTP State Management Mechanism 2-4 (Feb. 1997), *at* http://www.ietf.org/rfc/rfc2109.txt?number=2109.

13. GRALLA, *supra* note 12, at 299.

14. *See id.* at 299, 302-03.

15. *Id.* at 299.

16. Richard M. Smith, *The Web Bug FAQ, Version 1.0* (Nov. 11, 1999), *at* http://www.eff.org/Privacy/Marketing/web_bug.html.

17. GRALLA, *supra* note 12, at 305.

18. *Id.*

19. *Id.*

II. LEGAL BACKGROUND: FEDERAL ELECTRONIC SURVEILLANCE STATUTES

An all-encompassing definition of privacy has proven elusive,[20] but it is a concept that includes elements of freedom of speech, freedom from government intrusions upon property and communications, and control over the dissemination of one's thoughts.[21] This Note is concerned with one aspect of privacy: the interest in the security of personal communications.[22] This interest has its foundation in the Fourth Amendment, which creates the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by the government.[23] In two landmark cases, *Berger v. New York* and *Katz v. United States*, the Supreme Court held that this protection against government intrusion applied to warrantless, electronic eavesdropping.[24]

A. Statutory Prohibition of Intercepting Communications

Congress codified the holdings in *Berger* and *Katz*, as well as protection against private eavesdropping, in the Wiretap Act.[25] In its original form, the Wiretap Act prohibited warrantless interceptions of "wire or oral communication,"[26] with wire communications defined as any "aural transfer made in whole or in part though the use of facilities for the transmission of communications by the aid of wire . . . between the point of origin

---

20. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088 (2002) (summarizing attempts to define privacy and noting that "privacy is a sweeping concept, encompassing . . . freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations").

21. *See id.* at 1088, 1094.

22. *See* Theofel v. Farey-Jones, 341 F.3d 978, 982 (9th Cir. 2003) (noting that the "[Stored Communications] Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility").

23. U.S. CONST. amend. IV.

24. *See* Katz v. United States, 389 U.S. 347, 351, 359 (1967) (holding that electronic eavesdropping by FBI agents on the conversation of a criminal suspect in a public telephone booth violated the Fourth Amendment and ordering evidence obtained in this search excluded from trial); Berger v. New York, 388 U.S. 41, 58-60 (1967) (invalidating a New York wiretap statute).

25. The statute originated as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 213 (1968) (codified at 18 U.SC. §§ 2510-2522 (2000)), and is sometimes referred to simply as "Title III." To add to this confusion, some courts and commentators refer to the Wiretap Act as "Title I," because the Act was amended by Title I of the Electronic Communications Privacy Act of 1986. *See infra* note 30.

26. Wiretap Act, Pub. L. No. 90-351, § 802, 48 Stat. 1066 (1968).

and the point of reception."[27] In its current form, the Wiretap Act prohibits "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[28] A warrant is not required, however, if one of the parties to the communication consents to its interception. The scope of this statutory consent exception was central to the controversy in *Pharmatrak*.

B. Statutory Protection for Stored Communications

As computers became more common, it became increasingly apparent that the Wiretap Act's definition of "wire communications" did not extend to documents transmitted over computer networks.[29] In 1986, Congress addressed this shortcoming in ECPA,[30] which barred warrantless interception of "electronic communications,"[31] a category that encompasses "[m]ost Internet communications."[32]

ECPA also established protection for the contents of electronic and wire communications in "electronic storage."[33] This provision, commonly known as the Stored Communications Act (SCA), prohibits the access or disclosure of stored wire communications (e.g., voicemail) and electronic communications in the absence of a valid subpoena.[34] The SCA exempts

---

27. 18 U.S.C. § 2510(1); *see also* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 117-18 (2002) [hereinafter CCIPS MANUAL], http://www.cybercrime.gov/s&smanual2002.pdf (discussing the original definition of "wire communication").

28. 18 U.S.C. § 2511(1)(a).

29. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 810-16 (2003) (discussing development of statutory Internet surveillance law against background of constitutional law).

30. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); *see* USISPA, *Guide*, *supra* note 2, at 950 (demonstrating that legislative history showed that Congress attempted to make ECPA comprehensive).

31. *See* 18 U.S.C. § 2520.

32. CCIPS MANUAL, *supra* note 27, at 118.

33. The Act provides two definitions of "electronic storage": "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," 18 U.S.C. § 2510(17)(A), and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17)(B).

34. Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1860 (1986) (codified as amended in sequence starting at 18 U.S.C. § 2701). However, the passage of the USA PATRIOT Act weakened the protection for stored wire communications, creating parity with electronic communications. USA PATRIOT Act, Pub. L. No. 107-56, § 209, 115 Stat. 272 (2001). For a thorough account of the degrees of protection given to various

access to stored communications that is authorized "by the person or entity providing a[n] electronic communications service."[35] Explicitly, the SCA forbids someone from "intentionally access[ing] without authorization a facility through which an electronic communication service is provided . . . " and thereby obtaining, altering or preventing "authorized access to a wire or electronic communication while it is in electronic storage."[36] Both the definition of a communication in "electronic storage" and the permissible scope of third-party authorization to access such communications were at issue in *Theofel*.[37] As that case shows, eighteen years of technological advances raise doubts about the ability of ECPA to address the problem of privacy violations on the Internet.[38]

III. RECENT CASES: *IN RE* PHARMATRAK PRIVACY LITIGATION & *THEOFEL V. FAREY-JONES*

As *Pharmatrak* and *Theofel* demonstrate, courts continue to struggle with federal electronic surveillance statutes. In *Pharmatrak*, the First Circuit found that an interception was made without consent, but the court articulated a standard for intent that ultimately defeated the plaintiffs' claim under the Wiretap Act.[39] In *Theofel*, the Ninth Circuit held that e-mail stored on an ISP's computers is in "electronic storage," but the "bad faith" and "gross negligence" that defendants employed to gain access to the communications leaves some doubt as to the case's broader applicability.[40] Nonetheless, these cases bring some clarity to these complex statutes.

A. *Pharmatrak*: Scope of Consent to Intercept Communications

Pharmatrak was a class action based upon alleged violations of the Wiretap Act through the use of cookies and web bugs.[41] A number of

---

forms of communications and the remedies for violations of the SCA, see the discussion in CCIPS MANUAL, *supra* note 27, at 93-110.

35. 18 U.S.C. § 2701(c)(1).

36. Theofel v. Farey-Jones, 341 F.3d 978, 982 (9th Cir. 2003) (quoting 18 U.S.C. §§ 2701(a)(1), 2707(a)).

37. *Id.* at 982-87.

38. *See, e.g.*, Jerry Berman & Deirdre Mulligan, *The Internet and the Law: Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 549, 567-68 (1999); Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1113-117 (2002); Will Thomas DeVries, Note, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 291 (2003).

39. *Pharmatrak II*, 329 F.3d 9, 21-23 (1st Cir. 2003) [hereinafter *Pharmatrak II*].

40. *Theofel*, 341 F.3d at 984.

41. *Pharmatrak II*, 329 F.3d at 12-14.

pharmaceutical companies licensed a service called "NETcompare" from Pharmatrak.[42] One capability of NETcompare was to record which pages individual users visited at a client's site, along with how long a user spent looking at each page, the path that he or she took through the site, and the location of the page that the user had visited immediately before.[43] The other purpose of NETcompare was to allow comparisons of how people used different companies' websites; Pharmatrak released these comparisons in monthly reports to its clients.[44]

Pharmaceutical companies used NETcompare by adding a small amount of code to each of their webpages.[45] This code instructed the user's computer to contact Pharmatrak's web server and retrieve from it an invisible graphic image known as a "web bug."[46] This request allowed Pharmatrak to record the time at which the pharmaceutical client's page was viewed.[47] It also allowed Pharmatrak to "plac[e] or access[] a 'persistent cookie' on the user's computer."[48] Unknown to the pharmaceutical companies, and contrary to Pharmatrak's representations and its own understanding of NETcompare, the program could and did collect personal information such as names, addresses, telephone numbers, e-mail addresses, dates of birth, gender, insurance status, educational levels, occupations, medical conditions, medications, and reasons for visiting the particular website.[49] Pharmatrak's collection of this information formed the basis for the plaintiffs' claims.[50]

---

42. *Id.* at 12.

43. *Id.* at 13.

44. *Id.* at 14. These reports covered such topics as "the most heavily used parts of a particular site; which site was receiving the most hits in particular areas such as investor or media relations; and the most important links to a site." *Id.*

45. *Id.* at 13-14 ("A pharmaceutical client installed NETcompare by adding five to ten lines of HTML code to each webpage it wished to track and configuring the pages to interface with Pharmatrak's technology.").

46. For the technological explanation of web bugs, see *supra* Part I. The *Pharmatrak II* court also referred to web bugs as "clear GIFs," reflecting the fact that web bugs are frequently transparent GIF (Graphics Interchange Format) images. *See Pharmatrak II*, 329 F.3d at 14 (equating "web bug" with "clear GIF").

47. *Id.* (noting that "[o]n a user's first visit to a webpage monitored by NETcompare, Pharmatrak's servers would plant a cookie on the user's computer," and that "Pharmatrak's servers would access the information on the existing cookie" if the user had visited the page before).

48. *Id.* Unlike regular "cookies," persistent cookies do not expire at the end of an online session, and might not expire until after ninety days. *Id.*

49. *Id.* at 15.

50. *Pharmatrak I*, 220 F. Supp. 2d 4, 6 (D. Mass. 2002).

The district court granted Pharmatrak's motion for summary judgment on the plaintiffs' Wiretap Act claim[51] on the grounds that the pharmaceutical companies had consented to Pharmatrak's monitoring of communications between themselves and visitors to their websites.[52] Drawing an analogy to an earlier effort to use the Wiretap Act against a company that used similar methods to build advertising profiles of individual users,[53] the district court held that the consent exception provided a defense for Pharmatrak because "the Pharmaceutical Defendants were parties to communications with Plaintiffs and consented to the monitoring service provided by Defendant Pharmatrak."[54] As a result, Pharmatrak was not liable to the Internet users for intercepting their personal information.[55]

On appeal, the First Circuit held that the district court erred in its broad interpretation of the consent exception.[56] The First Circuit found that neither the pharmaceutical companies nor the plaintiffs had given their consent to Pharmatrak's acquisition of personal information.[57] Noting that a "party may consent to the interception of only part of a communication or to the interception of only a subset of its communication," the court found that the pharmaceutical companies did not consent to the interception of personal information; in fact, they received assurances from Pharmatrak that NETcompare did not have the capability to access that type of information.[58]

The First Circuit also held that the Internet users did not give their consent to Pharmatrak to access their communications with the various pharmaceutical companies.[59] Neither Pharmatrak nor the pharmaceutical companies gave notice on their websites that communications would be monitored for marketing or any other purpose.[60] Because "[d]eficient no-

51. *Id.*

52. 18 U.S.C. § 2511(2)(d) (2000) (creating an exception to interception violation where "a party to the communication . . . has given prior consent to such interception"); *Pharmatrak I*, 220 F. Supp. 2d at 12. The district court also dismissed the claims in the plaintiffs' complaint alleging violations of the Stored Communications Act and the Computer Fraud and Abuse Act. *Pharmatrak I*, 220 F. Supp. 2d at 12-15.

53. *See In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (holding that DoubleClick's use of cookies to track consumers was not a violation of the ECPA because the websites affiliated with DoubleClick consented to the interception of Internet users' communications).

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

55. *Id.*

56. *Pharmatrak II*, 329 F.3d at 19-21.

57. *Id.* at 20-21.

58. *Id.* at 19-21.

59. *Id.* at 21.

60. *Id.*

tice will almost always defeat a claim of implied consent," the court found that the consent defense failed in this case.[61]

The First Circuit also addressed the interception element of a Wiretap Act violation. Although the district court had not addressed this issue, the First Circuit held that Pharmatrak "intercepted" the communications carrying Internet users' personal information.[62] The court declined to provide its own definition of "interception," however, because Pharmatrak's actions satisfied even the narrowest definition of the term.[63]

Lastly, the First Circuit set out the definition of requisite intent for the proceedings on remand, stating that the party's conduct and the result needed to arise from a conscious objective.[64] The court noted that Congress did not intend for an inadvertent interception to give rise to criminal or civil liability.[65]

On remand, the district court found that Pharmatrak lacked this level of intent, and dismissed the case on summary judgment.[66] The district court found that the "small number of profiles" collected (232 profiles out of millions of users) pointed to an incidental and unintended interception. The court also held that programming errors by pharmaceutical companies caused the collection of personal data. Finally, Pharmatrak insisted that it did not know about the existence of personal data on its servers until after the plaintiffs filed the lawsuit, and therefore they could not have intended the result.[67]

B. *Theofel v. Farey-Jones*: Authorization to Access Stored Communications[68]

In *Theofel v. Farey-Jones*, the Ninth Circuit discussed two key features of the SCA: whether e-mail stored on an ISP's servers falls within the Act's definition of stored communications, and whether authorization to access such e-mail pursuant to an invalid subpoena is effective. Plaintiffs had appealed the district court's ruling that defendants did not violate any federal statute. The Ninth Circuit reversed the dismissal of the claims under the SCA and affirmed the dismissal of the claims under the Wiretap Act.

---

61. *Id.*
62. *Id.* at 21-22.
63. *Id.*
64. *Id.* at 22-23.
65. *Id.* at 23.
66. *In re* Pharmatrak, Inc. Privacy Litig., 292 F. Supp. 2d 263 (D. Mass. 2003).
67. *Id.* at 268.
68. 341 F.3d 978 (9th Cir. 2003).

The intersection of the Wiretap Act and the SCA is not defined by statute and has been problematic for the judiciary.[69] Technological advancements have caused these two sections of the ECPA to gradually overlap, and Congress has not given clear borders for application.[70] For example, courts have disagreed about the extent of protection e-mails receive under the ECPA.[71] The Fifth Circuit in *Steve Jackson Games v. United States Secret Service*[72] held that unread e-mails stored on a bulletin board did not receive protection under the Wiretap Act because the definition of "electronic communication" did not include a storage component.[73] Alth0ough one would assume that these same stored e-mails would then receive protection under the SCA, some courts have held that the definition of "storage" limits the protection of e-mails to intermediate storage before delivery.[74] In contrast to this interpretation, the Ninth Circuit in *Theofel* held that the protection also extends to an e-mail's "post-transmission storage."[75]

The Ninth Circuit has also addressed the SCA authorization requirement prior to *Theofel*[76] in an earlier case, *Konop v. Hawaiian Airlines*.[77] In *Konop*, two unauthorized users of the plaintiff's secured website gave a

---

69. *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003) ("[T]he intersection of these two statutes is a complex, often convoluted, area of the law."); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results."); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

70. *See Pharmatrak II*, 329 F.3d at 21-22.

71. *Compare In re* Doubleclick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001) (limiting the SCA's protection to unread e-mail stored on an ISB server), *and* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) (same), *with Theofel*, 341 F.3d at 984-85 (holding that even e-mail that has been read might be stored remotely "for purposes of backup protection," and thus qualify for protection under the SCA) (quoting 18 U.S.C. § 2510(17(B) (2000)).

72. 36 F.3d 457 (1994).

73. *Id.* at 461.

74. *See, e.g.*, *Doubleclick*, 154 F. Supp. 2d at 511-12; *Fraser*, 135 F. Supp. 2d at 636 (holding that "backup protection" does not include any form of "post-transmission storage").

75. *Theofel*, 341 F.3d at 984-85 (rejecting the holding in *Fraser*, 135 F. Supp. 2d at 633-34, as contrary to the plain language of the Act). The Ninth Circuit affirmed its interpretation of the SCA in *Theofel* in a recent amended opinion and denied a rehearing of the case. Theofel v. Farey-Jones, No. 02-15742, No. 03-15301, 2004 U.S. App. LEXIS 2555 (9th Cir. Feb. 17, 2004).

76. 341 F.3d at 978.

77. 302 F.3d 868 (9th Cir. 2002).

third party access to the website.[78] The court held that the consent exception did not apply because only a "user" of the service, who is authorized to use that service, can authorize a third party to access communications.[79] In *Theofel*, the Ninth Circuit further elaborated on the meaning and application of the authorization requirement.[80]

1. Theofel

During discovery in litigation over a commercial matter, defendant lawyer ordered the plaintiff's Internet service provider, NetGate, to produce "all copies of e-mails sent or received by anyone" at plaintiff's place of employment.[81] The subpoena had no limitations as to time or scope.[82] Defendants read a sample of 339 messages posted to a NetGate website without notifying opposing counsel, and without consideration for messages that were personal or privileged.[83]

2. Authorization Based Upon Mistake Is Invalid

The Ninth Circuit reversed the lower court's dismissal of the SCA claim based on the defendants' lack of authorization to access the e-mails.[84] Because Congress did not give a definition for the term "authorize" in the SCA, the Ninth Circuit instead compared the SCA authorization requirement to the tort of trespass, in that it protects an individual's interest in privacy and property.[85] Just as trespass protects a person's privacy and proprietary interest in a physical structure, so the Act protects someone's interest in electronic storage.[86] In either case, a defendant is not liable if his access to the stored information was authorized.

However, § 2701(c)(1) does not protect a defendant who gains authorization "by exploiting a known mistake that relates to the essential nature of his access."[87] The Ninth Circuit held that an assertion of permis-

78. *Id.* at 872-73.

79. *Id.* However, the court noted that § 2510 does not define "user," leaving that definition to the courts. *Id.*

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

81. *Theofel*, 341 F.3d at 981.

82. *Id.*

83. *Id.*

84. *Id.* at 985. However, the *Theofel* court found that the district court properly dismissed the Wiretap Act claim because the Ninth Circuit had previously held that "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'" *Id.* at 986.

85. *Id.* at 982 ("Like the tort of trespass, the Stored Communications Act protects individuals' privacy and proprietary interests.").

86. *Id.* at 982-83.

87. *Id.* at 983.

sion to access a stored communication is only valid if it would "defeat a trespass claim in analogous circumstances."[88] Though NetGate gave permission for the defendant's attorney to access the e-mails upon receipt of the subpoena, its "egregiously" overbroad demands invalidated the subpoena under the Federal Rules of Civil Procedure.[89] NetGate, however, did not recognize this effect.[90] In addition to finding the subpoena invalid on the basis of the common law background of "consent induced by mistake,"[91] the *Theofel* court cited the expense of challenging a subpoena and the potential of abuse of knowing use of invalid subpoenas as broader reasons to invalidate NetGate's alleged consent.[92]

3. *E-mail Is Communication in "Electronic Storage"*

The Ninth Circuit also declined to affirm the dismissal on the alternative ground that the e-mails had not been in "electronic storage" and therefore fell outside the SCA.[93] Under the SCA, "electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission" and "(B) any storage of such communication by an electronic communication service for purposes of backup protection."[94] The court, liberally interpreting the storage requirement of the SCA, held that the e-mail messages saved for backup are also considered "stored" for the purposes of the SCA, and therefore receive protection under that statute upon a finding of unauthorized access.[95] Some courts have held that the first part of the definition could include e-mail messages pending delivery stored on an ISP's server, but that part (B) would not apply if the backup protection did not assist the ISP in its service and if it did not have a supplemental purpose to the electronic transmission covered in part (A).[96] The Ninth Circuit disagreed with this finding and held that part (B) applied to *any* messages stored for backup protection.[97]

---

88. *Id.*
89. *Id.* at 981; *see id.* at 984.
90. *Id.*
91. *Id.* (citing RESTATEMENT (SECOND) OF TORTS § 174 (1965)).
92. *Id.* at 984.
93. *Id.* at 984-85.
94. 18 U.S.C. § 2510(17) (2000).
95. *Theofel*, 341 F.3d at 985.
96. *Id.* (citing *In re* Doubleclick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001)).
97. *Id.*

IV. CONCLUSION

The legislative history, case law, and the plain language of both the Wiretap Act and the SCA clash against each other and against common sense in light of current technology. The intersection of the Wiretap Act and the SCA has become a large grey area, leaving judges to grope in the dark when trying to apply the law. While courts proclaim the statute to be convoluted and "infamously unclear,"[98] and while commentators clamor in academic journals and call for new law, Congress has remained fairly dormant on this issue. As long as the ECPA remains outdated and unevenly applied,[99] and Congress does not provide new protections for electronic communications, online privacy protection will remain in the dark ages.

98. *See supra* note 69; *see also* USISPA, *Guide*, *supra* note 2, at 948 ("The court's interpretation of these provision has been disjointed due in large part to the complexity of the statutes.").

99. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2000) ("We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites . . . will remain a confusing and uncertain area of the law.").