2005

"Don't Be Evil": Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-Mail Privacy Rights

Jason Isaac Miller
NOTE

"DON'T BE EVIL": GMAIL’S RELEVANT TEXT ADVERTISEMENTS VIOLATE GOOGLE’S OWN MOTTO AND YOUR E-MAIL PRIVACY RIGHTS

I. INTRODUCTION

An attorney presses “send” on an e-mail message to a prospective client following an initial consultation. The prospective client has an e-mail account with Google’s recently introduced webmail service, Gmail. What the attorney does not know is that before his e-mail reaches its intended audience, Google will have scanned the contents of the message, found within it words and phrases such as “new client,” “attorneys at law,” “construction litigation,” and even the name of the city in which the attorney practices, and placed along side the e-mail, contemporaneously with the client’s viewing of it, advertisements for legal services offered by the attorney’s competitors. This seemingly hypothetical scenario is actually an everyday occurrence that is all too real.¹

¹ In fact, when this author composed and sent such an e-mail, two of the three content-sensitive advertisements Gmail placed alongside the body of the e-mail listed the author’s competitors:

Dear Mr. Jones:

It was a pleasure meeting with you yesterday in our offices. I will be preparing and mailing today the retainer agreement for your review and signature. Please do not hesitate to give me a call at the office should you have any questions or concerns. Once again, I look forward to having you as a new client and helping you with your complex construction matter.

Jason Isaac Miller
Miller & Hofstra, LLP
Attorneys at Law
Hempstead, NY

Gmail then placed the following three advertisements and accompanying links to the right of the e-mail:
The introduction of Gmail in April 2004 marked the first time relevant text advertisements were placed in e-mails, making possible this scenario, which was unheard of until then. While Google, the leader in Internet search technology, has been stirring up a frenzy with its offering of invite-only e-mail accounts with huge storage capacity and search functionality, Google's competitors are rushing to catch up. Logic and progress dictate that the technology powering Gm ail's e-mail scanning software will soon be employed by such widely used webmail providers as Yahoo, Hotmail, and AOL.

Therefore, it is necessary to step back to evaluate, as early as possible, whether e-mail users are trading their statutorily protected privacy rights for bigger inboxes and whether non-subscribers who send
e-mail messages to Gmail users are unknowingly allowing their privacy rights to be violated.

This Note contends that the statutory exception allowing electronic communications service providers like Gmail to intercept, process, and utilize e-mail intended for its users for advertising and revenue generating purposes is too broad. While this exception allows for electronic communication service providers to scan the contents of e-mails in order to offer their users services generally accepted as convenient and beneficial—such as virus protection and spell checking—the practice of text advertisement placement is distinguishable. The placement of these advertisements differs from services currently offered to e-mail users in that virus protection and spell checking features do not directly generate revenue for e-mail service providers. Moreover, unlike virus protection and spell checking, the placement of relevant text advertisements may adversely affect the non-subscriber who sends e-mail to a Gmail user in the manner described above. E-mail forwarding has become a widely used practice due to the number of individuals who maintain multiple e-mail accounts (for business, school, and personal purposes). My hypothetical attorney may very well send the potential client an e-mail message to the client’s business or personal e-mail address, unaware of the fact that the confidential communiqué will be automatically forwarded to and eventually scanned by the client’s Gmail account. Aside from inquiring about his potential client’s e-mail practices, the attorney would have no way of knowing that his e-mail message would be intercepted and scanned before the potential client receives it.

Part II of this Note will answer the question “what is Gmail?” and examine the technology and processes behind the placement of relevant text advertisements. Part III will examine the current statutory protections covering electronic communications under the Electronic Communication Privacy Act (“ECPA”). Part IV will briefly survey the

5. See Hafner, supra note 2.

6. Email Forwarding
Maybe you have a large number of email addresses and don’t want to check all of them separately. With the email forwarding feature, you can forward all your incoming email to another email address that you specify. This is similar to forwarding for your phone calls. You can easily set up your email forwarding or change it through your website control panel.


evolution of federal case law that addresses the interception of e-mail and the interpretation and the applicability of the provisions of the ECPA. Part V will examine the main problems associated with the current application of the ECPA as interpreted by the courts: the prevailing reasoning behind the most recent Court of Appeals cases is flawed; and under that reasoning, courts are likely to find Gmail is not intercepting e-mail intended for its users; and the Stored Communication Act’s ("SCA") Electronic Communications Service Provider exception is too broad as currently written, thereby allowing Gmail to intercept its users’ e-mails and encroach on statutorily protected Internet privacy expectations. Part VI will address these problems by proposing solutions and discussing their instrumental effects. These proposals include an alternate statutory mechanism for protection of both wire and electronic communications that is consistent with legislative intent; an alternate judicial interpretation that eviscerates the distinction between the protection afforded electronic communications that are in storage and those that are not; and an alternative statutory exception for electronic communications service providers which is broad enough to allow such actors to engage in the functions necessary to provide communications services to the public, while at the same time prohibiting e-mail providers like Gmail from sifting through the content of e-mail sent by unknowing parties intended for Gmail users. Finally, Part VII will conclude by suggesting that one of the above remedies, if not all, is necessary to curb the encroachment on Internet privacy by Gmail, which is in a unique position to abuse its power.

II. Gmail: A Description of the Technology

A. What is Gmail?

Founded in September 1998 by Larry Page and Sergey Brin, Google Inc. is the developer of the award-winning Google search engine, which is designed to search the Internet for information in an easy, efficient manner.\(^8\) Offering users access to an index comprising more than eight billion web pages, Google is the largest search engine on the Internet\(^9\) and maintains its leadership position in the search

---

9. Id. Google.com is available in 100 languages and it accepts payments for advertisements in forty-eight currencies. See Kevin Couglin, Google Searches for Everything on Earth, THE STAR LEDGER, May 20, 2005, at 47.
industry by continually innovating its search capabilities. On April 1, 2004, Google announced the addition of Gmail to its array of online search-related services. Gmail is a free, search-based webmail service that provides over two and a half gigabytes of webmail storage in exchange for content-sensitive advertising that appears on the right side of the user's computer screen when the user accesses e-mail. While Gmail offers many innovative features, Google explains, "[t]he backbone of Gmail is a powerful Google search engine that quickly finds any message an account owner has ever sent or received. That means there's no need to file messages in order to find them again." This search functionality, together with an attractive two gigabyte storage limit, an industry first, and other nifty innovations such as

10. "On Tuesday, March 23, 2004, WebSideStory examined a sample of over twenty-five million visits and found that Google had the top share of search referrals, 40.9 percent. It was followed by Yahoo at 27.4 percent, then MSN at 19.6 percent." Danny Sullivan, Google Tops, but Yahoo Switch Success so Far, SEARCHENGINEWATCH, Apr. 5, 2004, http://searchenginewatch.com/searchday/article.php/3334881.


12. These include: Google.com, Google Alerts, Google Answers, Google Catalogs, Google Directory, Froogle, Google Groups, Google Images, Google Labs, Google Local, Google Maps, Google Mobile, Google News, Google Print, Google Scholar, Google Special Searches, Google University Search, Blogger, Google Code, Google Desktop Search, Hello, Keyhole, Picasa, Google Toolbar, Google Translate, and Urchin. For a description of each, see Fact Sheet, supra note 8.


15. On April 1, 2005, Gmail's one-year anniversary, Google doubled the amount of storage offered on its free e-mail service to a very attractive two gigabytes. See Bloomberg News, Google Doubling Storage on Free E-Mail Service, N.Y. TIMES, Apr. 2, 2005, at C3. Google further announced that it would continue to increase e-mail storage in the next few weeks. Id. This author currently maintains a Gmail account with a free storage capacity of 2.561 gigabytes. Once again, competitors have been rushing to catch up in response to Gmail's new two gigabyte increase. In June 2005, AOL began giving away most of its popular online services free of charge on its AOL.com website. See Hiawatha Bray, You've Got Freebies as AOL Opens Up: No. 1 Internet Provider Starts Giving Away Most of its Popular Services, BOSTON GLOBE, June 21, 2005, at D1.

"AOL.com in the past hasn't been thought of as a place to come for great content for free," said Kerry Parkins, director of product marketing for America Online. But Parkins said this will change in the next few months, as AOL moves nearly all of its features away from the company's exclusive subscription service and onto a Web portal that will challenge major free websites like ... Google....

Id.
"conversation threads" has helped create a worldwide race to sign up for Gmail accounts.\textsuperscript{17}

\textbf{B. Relevant Text Advertisements: How do They Work?}

Privacy and civil liberties organizations as well as individuals have been raising concerns about Gmail's placement of relevant text advertisements in e-mails since the service was first announced in April, 2004.\textsuperscript{18} When the user is logged into his Gmail account, Google will display targeted advertisements and other relevant information based on the content of the e-mail message displayed.\textsuperscript{19} In a completely automated process, computers process the entire content of the e-mail message, including the header and address information, perform a mathematical analysis on it, and finally match the message to advertisements or other related information in Google's extensive database.\textsuperscript{20} Google asserts in its privacy policy that no humans are involved in this process,\textsuperscript{21} and that no e-mail content or other personally identifiable information will be provided to advertisers.\textsuperscript{22}

Advertisements are matched using the same technology that powers the Google Adsense program, which already places targeted advertisements on thousands of sites across the web by quickly

\textsuperscript{16} This feature strings together related e-mail messages, arranging them in conversation threads. The threads allow users to view e-mails messages and their responses as an entire conversation chain rather than as individual messages. See Getting Started With Gmail, http://gmail.google.com/gmail/help/start.html (last visited Aug. 25, 2005).

\textsuperscript{17} See Juliet Chung, \textit{For Some Beta Testers, It's About Buzz, Not Bugs}, N.Y. TIMES, July 22, 2004, at G1 (discussing the popularity of Gmail beta test accounts). Obtaining a Gmail account continues to be an invitation-only affair, consequently, having a Gmail e-mail address currently carries with it a bit of prestige and conveys a message of e-sophistication. See Don Fernandez, \textit{Pre-Eminent Domain: These Days, Some Folks on the Internet are Judging Us by Our E-mail Addresses}, ATL. JOURNAL-CONSTITUTION, Apr. 28, 2005, at F1 ("'The Gmail domain... lets me know someone spends a lot of time online... [while on the other hand] [w]hen I see a Yahoo or Hotmail domain I think not only cheap, but also disposable.... [a]nd I think 'dumbo' when I see someone nowadays with an AOL account.'"

\textsuperscript{18} Slightly more than three million Americans now boast a Gmail account. \textit{Id.} As of April 2005, only a year after its inception, Gmail has become the fourth-most-visited e-mail service on the Web, only behind industry standards Yahoo, AOL, and MSN's Hotmail. See Bloomberg News, supra note 15.


\textsuperscript{20} See Gmail Privacy Policy, http://mail.google.com/mail/help/privacy.html; see also About Gmail, \textit{It has Ads. But Only Good Ads}, supra note 13.

\textsuperscript{21} See Gmail Privacy Policy, supra note 20.

analyzing the content of web pages and determining which advertisements are most relevant to them. The placement of relevant text advertisements in Gmail is mandatory, and users may not opt out of receiving the advertisements.

Although Google has not released technical details of how Gmail’s “content extraction” and analysis work, the patents filed with the US Patent and Trademark Office provide some clues. “From a technical
standpoint, there is no categorical difference between Google’s ‘content extraction’ and spam filtering—each involves an automated process that analyzes the body and/or header information of e-mail messages. However, from a legal and privacy standpoint, there is a fundamental difference between filtering unwanted junk e-mail and analyzing the content of private communications in order to target paid advertisements to generate revenue. Still, as long as it is a computer, and not a person reading your e-mail, many ask, why all the fuss? In response, some contend that having a person read your e-mail to target the advertisements would be less of a privacy invasion. Unlike large computer systems, a human’s storage, memory, and associative capacity is finite. But Google has the ability to build profiles of users based on their communications, unhindered by the unrestricted Gmail Privacy Policy. "Additionally, Gmail’s ‘context extraction’ will make its privacy invasions continuous and automated, making it a difficult privacy problem to solve just as spam and telemarketing, both of which are also continuous and automated by computer."

The relevance of advertisements to a user’s interests is improved. In one implementation, the content of a web page is analyzed to determine a list of one or more topics associated with that webpage. An advertisement is considered to be relevant to that webpage if it is associated with keywords belonging to the list of one or more topics. One or more of these relevant text advertisements may be provided for rendering in conjunction with the web page or related web pages.

Advertisers are permitted to put targeted ads on page on the web (or some other document of any media type). The present invention may do so by (i) obtaining content that includes available spots for ads, (ii) determining ads relevant to content, and/or (iii) combining content with ads determined to be relevant to the content.

27. See id. (distinguishing between spam filtering and Gmail’s practices).
28. See id. at sec. 2.5.
29. See id.
30. Id. Privacy advocates have pointed out troubling gaps in Gmail’s Privacy Policy, especially relating to the threat of unlimited data retention. For example, see the Electronic Privacy Information Center’s Gmail Privacy Page where it is warned that while the prospect of never having to delete or file an e-mail is an attractive feature for space-hungry users, the implications of indefinite storage of e-mail communications presents several serious implications. Although Google has [sic] is held in high esteem by the public as a good corporate citizen, past performance is no guarantee of future behavior—especially following Google’s IPO when the company will have a legal duty to maximize shareholder wealth. Although Google currently says that they will not record the “concepts” extracted from scanned e-mails, they could decide to do so in the future.
III. CURRENT LAW: STATUTORY PROTECTION OF ELECTRONIC COMMUNICATIONS


Congress first addressed the need to protect privacy in the context of evolving technology by introducing Title III of the Omnibus Crime Control and Safe Streets Act, commonly known as the Federal Wiretap Act. The enactment of Title III was significant because Congress recognized that technological developments enabled the interception of personal and commercial communications. Title III, however, was limited in scope, as it only prohibited the interception of communications that could be heard and understood by humans as sound. Thus, there was no Title III protection against the interception of "text, digital or machine communication" because in these sources of communication, there are no audible sounds to intercept. In addition, the act of interception was narrowly construed under the language of the statute to include only the contemporaneous acquisition of the communication, thereby affording inadequate protection.

future and thereby create detailed profiles of users. Building such profiles on years of past communication in addition to current communications is made easier if users never delete e-mails. Additionally, communications stored for more than 180 days are exposed to lower protections from law enforcement access; with Gmail, many such e-mails could be made easily available to police.

Id. at sec. 1.3(b); but cf. Grant Yang, Stop the Abuse of Gmail!, 2005 DUKE L. & TECH. REV. 0014, 34-36, http://www.law.duke.edu/journals/dltr/articles/2005dltr0014.html (concluding that Gmail's practices and procedures are consistent with the standards of the webmail industry, and that Google is a business, which through Gmail provides a service, and in return "should be allowed to display its ads based on trigger words in the text.").

34. See H.R. REP. NO. 647, 99-22, at 17 (1986) (stating that Congress "did not attempt to address the interception of text, digital or machine communication").
35. See id.
36. See United States v. N.Y. Tel. Co., 434 U.S. 159, 166-67 (1977) (holding that pen registers do not intercept because they do not acquire the contents of any wire or oral communication through the use of any electronic, mechanical, or other device).
37. See United States v. Turk, 526 F.2d 654, 658 n.3 (5th Cir. 1976).
38. See H.R. REP. NO. 647, 99-22, at 17 (1986) (recognizing that these forms of communication were not as common as telephone communication or face-to-face oral communication).
By the mid-1980s, the telecommunications landscape had changed dramatically from the landscape that existed when Title III was first enacted. Technology had outpaced the privacy protections in Title III, creating uncertainty and gaps in its protections. To remedy these perceived weaknesses and to update and expand the privacy protections in the 1968 Act, Congress passed the Electronic Communications Privacy Act of 1986.

The ECPA was divided into Title I, commonly known as the Wiretap Act, and Title II, commonly known as the Stored Communications Act. The amendments provided for the protection of electronic communications along with oral and wire communications.

B. Title I of the ECPA: The Wiretap Act

Section 101(c)(1)(A) of the ECPA added "electronic communications" to the existing prohibitions against intercepting wire and oral communications. The amended Wiretap Act provides a private

39. See id. at 17-18 (stating that pre-ECPA Title III failed to anticipate the advent of "text, digital or machine communication" and the increasing use of communications that are not routed through communications common carriers, such as e-mail, videotex, and other private services).

40. Although it is still not twenty years old, the Wiretap Act was written in a different technological era... Today we have large-scale electronic mail operations... and a dazzling array of digitized information networks which were little more than concepts two decades ago. Unfortunately, the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government.

id. at 17-18. The legislative history surrounding the 1986 Act refers to the "dazzling array of digitized information networks", however, to put that phrase into proper perspective, the ECPA was drafted in an era when only 50,000 computers were connected to the Internet. See Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Just. of the House Comm. on the Judiciary, 99th Cong. 1 (1986) (statement of Chairman Robert Kastenmeier); see also Raechel V. Groom, In re Pharmatrak & Theofel v. Farey-Jones: Recent Applications of the Electronic Communications Privacy Act, 19 BERKELEY TECH. L.J. 455, 456 (2004). The Internet now allows millions of people to communicate and exchange information through an international network of interconnected computers. See Reno v. ACLU, 521 U.S. 844, 849-50 (1997).


45. See discussion infra Parts III.B-C.

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." Congress defined an electronic communication 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," but excluded wire and oral communications from the definition.

Plaintiffs must show five elements to make their claim under Title I of the ECPA: A defendant (1) intentionally; (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept; (3) the contents of; (4) an electronic communication; (5) using a device. This showing is subject to certain statutory exceptions, including consent. "Consent may be explicit or implied, but it must be actual consent rather than constructive consent."

C. Title II of the ECPA: The Stored Communications Act

Congress also realized that with the proliferation of large databanks of stored electronic communications in every facet of society, threats to individual privacy extended well beyond the bounds of the Wiretap Act's prohibition against the "interception" of communications.

48. 18 U.S.C. § 2510(12) (2000). In addition to altering the substantive prohibition by adding electronic communications to the list of covered communications, Congress also altered the definition of "intercept." As amended, the statute defined "intercept" as "the aural or other acquisition" of the contents of a communication, thereby clarifying that electronic communications need not be "aurally" acquired. Id. at § 2510(4).
49. See In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003).
50. (d) It shall not be unlawful... 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.
53. United States v. Councilman, 373 F.3d 197, 206 (1st Cir. 2004) (Lipez, J., dissenting) (discussing Congressional intent behind the ECPA). The Wiretap Act had already been interpreted
Therefore, the stored communications provisions were intended to address "the growing problem of unauthorized persons deliberately gaining access to, or sometimes tampering with, [stored] electronic or wire communications."54 The 1986 SCA also provides protection for private communications, barring unauthorized access to an electronic communication while it is in electronic storage.55 The SCA provides in relevant part with certain exceptions,56 that there is a criminal or civil cause of action 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."57 The statute further provides, "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."58

Congress intended for the privacy protections established by the SCA to apply to two categories of communications: "those associated with transmission and incident thereto" and those of "a back-up variety."59 The first category refers to temporary storage such as when a message sits in an e-mail user's mailbox after transmission but prior to the user retrieving the message from the mail server.60 However, this category does not include messages that are still in transmission, which remain covered by the Wiretap Act.61 The second category includes communications that are retained on a server for administrative and billing purposes.62 Electronic "communications service providers could

---

56. See discussion infra Part VI.C. and accompanying footnotes.
58. 18 U.S.C. § 2702(a) (2004). This Note is especially concerned with this prohibition as it relates to Gmail in its capacity as a provider of electronic communication services to the public.
60. See id. at 65.
61. See id.
62. See id.
use stored messages in this category to restore a user's data in the event of a system crash or to recover [an] accidentally-deleted message."63

D. The USA PATRIOT Act

The USA PATRIOT Act64 was enacted on October 26, 2001 and has played an important role in the history of the ECPA by repealing the express inclusion of stored wire communications from the definition of wire communication.65 This change was significant because the opinions of *Steve Jackson Games, Inc. v. United States Secret Service; Konop v. Hawaiian Airlines, Inc.* and *United States v. Councilman* previously rested on this textual distinction when they held that the definition of "intercept," in the context of electronic communications, requires contemporaneity.66 Furthermore, the *Konop* and *Steiger*67 opinions interpreted this congressional amendment to reflect intent to reinstate the pre-ECPA definition of "intercept"—acquisition contemporaneous with transmission—with respect to wire communications.68 The idea that Congress implicitly approved the judicial definition of "intercept" as requiring contemporaneity rests on the courts' assumption that Congress was aware of the narrow definition courts had previously given the term with respect to the unchanged definition of "electronic communications."69

IV. THE DEVELOPMENT OF JUDICIAL INTERPRETATION OF "INTERCEPT" UNDER THE ECPA

Although Congress redefined the term "intercept" in 1986 to clarify that communications need not be "aurally" acquired,70 it did not address

68. Id. at 1048-49; Konop, 302 F.3d at 878; see also Christopher T. Blackford, Comment, *Judicial Interpretations of the Electronic Communications Privacy Act Raise Concerns About Whether the Airline Industries' On-Line Business Ventures are Protected*, 68 J. AIR L. & COM. 819, 849 (2003).
69. See Steiger, 318 F.3d at 1048-49; Konop, 302 F.3d at 878.
70. See 18 U.S.C. § 2510(4) (2000). The ECPA defines the term "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." Id.
the contemporaneity issue directly. Consequently, courts, relying on other statutory clues, have concluded that an electronic communication is only intercepted when it is seized during its transmission. The following cases detail the evolution of the case law among the circuits that led to this conclusion.

A. United States v. Turk

Prior to the ECPA, United States v. Turk created a narrow interpretation of "interception" under the Wiretap Act. Even after the passage of the ECPA, circuits continue to rely on Turk and decisions from others circuits that have adopted its reasoning under the framework of the post-ECPA, Federal Wiretap Act. In United States v. Turk, police officers removed a tape recorder and two cassette tapes from a car during an arrest for cocaine possession. The officers listened to the tapes at the station house. The court noted that "[the officers] soon realized that they were listening... to a recording of a private telephone conversation... [but t]he officers continued to listen out of 'curiosity.'" The court decided the issue of "[w]hether the seizure and replaying of the cassette tape by the officers was also an 'interception'" under the original Federal Wiretap Act.

The court held that the seizure and replaying of the tapes was not an interception prohibited under the original Federal Wiretap Act because an interception "require[d] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device," and the officers were not involved in the recording of the tapes, but were merely listening to them after the

72. 526 F.2d 654 (5th Cir. 1976).
73. See Tatsuya Akamine, Note, Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act, 7 J.L. & POL'Y 519, 545 n.98 (1999).
74. See, e.g., United States v. Councilman, 373 F.3d 197 (1st Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).
75. Turk, 526 F.2d at 656.
76. See id.
77. Id. at 656-57.
78. Id. at 657.
79. Id. at 658.
fact. 80 In Turk, the court chose to base its interpretation of “interception” on the legislative history of the statute rather than derive it from a strict reading of the statutory language. 81 In requiring the contemporaneity element of an interception, the court equated the term “interception” with “wiretapping,” even though the latter was nowhere defined in the statute. 82 Subsequent cases that relied on Turk for the proposition that contemporaneity is necessary in order for an interception under the Wiretap Act failed to take into account that unlike a telephone conversation, the contents of which are ephemeral and must be acquired contemporaneously with its transmission, an un-read e-mail does not require contemporaneity with its transmission. 83 Unlike the fleeting words of a telephone conversation, an unread e-mail remains perfectly intact, a communication not yet completed, just as the contents of a sealed letter are not yet communicated to its intended recipient. The contents of the e-mail may readily be obtained at anytime. 84 While the narrow definition of “intercept” which was first crafted by Turk is no longer binding law, the reasoning behind it still carries great persuasive force. 85

B. Steve Jackson Games, Inc. v. United States Secret Service

Relying on its own precedent in Turk, the Fifth Circuit erroneously extended its reasoning concerning the wiretapping of telephone calls to the interception of e-mail messages. 86 The plaintiff, Steve Jackson

80. See id at 656.
81. See Akamine, supra note 73, at 543.
82. See id. at 544.
83. See id.
84. In a sense e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission. The sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police. The fact that an unauthorized “hacker” might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way.


85. When Turk was decided in 1976, the statutory definition of “wire communication” did not yet include stored information. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 887 (9th Cir. 2002). Congress’s amendment of § 2510(1) to include stored information occurred ten years later, in 1986. See Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986). To the extent that Turk stands for a definition of “intercept” that requires contemporaneity, it has been statutorily overruled, at least in the context of wire communications. See United States v. Smith, 155 F.3d 1051, 1057 n.11 (9th Cir. 1998).

86. Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994).
Games, Inc., published books, magazines, and games. The company maintained an electronic bulletin board on one of its computers, where it posted public information about its products. This bulletin board also permitted customers to send and receive private e-mail. E-mail messages addressed to a customer were temporarily stored on the hard drive of the computer supporting the bulletin board. Customers could access the board from multiple locations and could choose to either store messages on the plaintiff's hard drive or delete them after reading. The plaintiff alleged that the Secret Service seized and read these private unread e-mail messages which were stored on plaintiff's computer.

The plaintiffs asked for damages as authorized by the Wiretap Act and the SCA. The district court awarded statutory damages under the SCA, but denied relief under the Wiretap Act. In affirming the district court, the Fifth Circuit held that interception does not take place where a stored electronic transmission is seized before the intended recipient reads it. The Fifth Circuit reached its decision by focusing on a key distinction between the definitions of "wire communication" and "electronic communication" as those terms are set forth in the Wiretap Act. The court pointed out that while the definition of "wire communication" includes the electronic storage of a wire communication, the definition of "electronic communication" does not likewise include the electronic storage of an electronic communication. The court deduced from this

87. *Id.* at 458.
88. *Id.*
89. *Id.*
90. *See id.*
91. *See id.* at 459.
92. *See id.*
93. *See id.* at 459-60 (relying on the reasoning in *Turk*, and holding that the Secret Service did not "intercept" the customers e-mail because its acquisition was not contemporaneous with the transmission of those communications).
94. *See id.* at 460-63.
97. The ECPA defines "electronic communication" as:

[A]ny transfer of signs, signals, writings, 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, but does not include (A) any wire or oral communication; ... (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

98. "Electronic storage" is defined as:

(A) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such
distinction that Congress did not intend for the law governing interception to be applicable to electronic communications in electronic storage.\textsuperscript{100} The court's decision in \textit{Steve Jackson Games} illustrates a problem scholars have written about before: the greater protection of the Wiretap Act applies solely to the interception of e-mail that is in transmission, leaving e-mail in electronic storage with the lesser protection afforded by the SCA.\textsuperscript{101}

One student of the subject, Tatsuya Akamine, argues that the "mere absence of the reference to 'electronic storage' does not necessarily mean that it is excluded from the meaning of 'electronic communication,'" but rather, he asserts that if the meaning of "electronic communication" is broad enough to encompass "electronic storage," it would be superfluous to add the reference to "electronic storage."\textsuperscript{102} Opposition to this statutory distinction prevailed in 2001 with the passage of the PATRIOT Act, which amended the ECPA by eradicating the statutory distinction between "wire communication" and "electronic communication."\textsuperscript{103}

\begin{itemize}
\item[18 U.S.C. § 2510(17) (1994).]
\item[99.] \textit{Steve Jackson Games}, 36 F.3d at 460-63.
\item[100.] Critical to the issue before us is the fact that, unlike the definition of 'wire communication,' the definition of 'electronic communication' does not include electronic storage of such communications . . . . Congress's use of the word 'transfer' in the definition of 'electronic communication,' and its omission in that definition of the phrase 'any electronic storage of such communication' . . . reflects that Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.' \textit{Id.} at 461-62.
\item[101.] \textit{See Pikowsky, supra} note 46, at 53 (arguing that the statutory distinctions are arbitrary, and that the intended recipient of an e-mail has the same privacy interest regardless of whether the message is intercepted while in transit or in storage); \textit{cf.} Orin S. Kerr, \textit{Internet Surveillance Law after the PATRIOT Act: The Big Brother that Isn't}, 97 Nw. U. L. REV. 607, 616-18 (2003) (claiming a retrospective search for stored e-mail is usually less intrusive because many relevant messages may have been deleted prior to the search).
\item[102.] \textit{See Akamine, supra} note 73, at 552.
\item[103.] The PATRIOT Act removed the following italicized language, leaving the statute to read: 'wire communication' means any aural transfer 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 between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication. 18 U.S.C. § 2510(1) (emphasis indicating omission).
\end{itemize}
C. Konop v. Hawaiian Airlines, Inc.

The Ninth Circuit Court of Appeals' decision in Konop v. Hawaiian Airlines, Inc.\(^{104}\) "created a significant stir in the legal community when it was released early in 2001 because the holding was contrary to the traditional judicial interpretation of the ECPA which is that the Wiretap Act does not protect communications while in electronic storage."\(^{105}\)

Robert Konop, a pilot for Hawaiian Airlines ("Hawaiian"), maintained a password-protected website, on which he posted bulletins critical of his employer, its officers, and the incumbent union, none of whom were permitted access to the site.\(^{106}\) He created a list of individuals, mostly employees of Hawaiian, who were eligible to access the website.\(^{107}\) Konop required these individuals to log in with a user name and password.\(^{108}\) To obtain a password, eligible persons were required to register and consent to a non-disclosure agreement.\(^{109}\) Other terms and conditions clearly displayed on the sign-on page prohibited members of either Hawaiian or union management from viewing the website.\(^{110}\)

Hawaiian vice-president, James Davis, was able to gain access to Konop's restricted website by obtaining passwords from two eligible Hawaiian pilots, Gene Wong and James Gardner.\(^{111}\) The two pilots freely provided their information when Davis asked for their permission to access the website using their names.\(^{112}\) By signing on, Davis accepted the terms and conditions of the website, despite the prohibition against management access.\(^{113}\) Davis continued to view the website under both pilots' identities for several months and also shared information from the website with other management and union employees.\(^{114}\)

\(^{104}\) 236 F.3d 1035, (9th Cir. 2001), withdrawn, 262 F.3d 972 (9th Cir. 2001), reargued 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003).
\(^{106}\) See Konop, 302 F.3d at 872.
\(^{107}\) See id.
\(^{108}\) See id.
\(^{109}\) See id. at 872-73.
\(^{110}\) See id. at 873.
\(^{111}\) See id.
\(^{112}\) See id.
\(^{113}\) See id.
\(^{114}\) See id.
Upon becoming aware of this unauthorized viewing, Konop filed suit against Hawaiian in the U.S. District Court for the Central District of California, alleging that Hawaiian’s unauthorized viewing and use of his secure website violated both the Wiretap Act, as amended by Title I of the ECPA, and the SCA. The district court granted summary judgment to Hawaiian on those claims. Konop then appealed to the Ninth Circuit.

In its original opinion, the Ninth Circuit Court of Appeals reversed and remanded, holding that a narrow interpretation of the Wiretap Act, limiting the term “intercept” to mean contemporaneous acquisition, was not consistent with the purpose, language, or text of the ECPA. The court reasoned that because electronic storage is necessarily a part of the entire communication process, the definition of “electronic communication” impliedly covers electronic storage, even if not specifically referenced. Although the Ninth Circuit attempted to fit its opinion within the framework of legislative intent and precedent from its own jurisdiction and the Fifth Circuit, its conclusions were diametrically opposed to those of the earlier cases, which were consistent with the first case to introduce the narrow interpretation of “intercept,” United States v. Turk. However, the Ninth Circuit avoided the implications of Turk by arguing that because the ECPA had subsequently amended the Wiretap Act, the Act’s new structure and definition of “wire communication” which included stored information did not harmonize with the older, narrower definition of “intercept” in Turk. This opinion was withdrawn however, and the court subsequently filed a new opinion in its place.

In their second opinion, the court affirmed the district court’s summary judgment ruling with regard to the Wiretap Act claim, but reversed and remanded the SCA claim on a technicality. The court

115. See id.
116. See id.
117. See id.
118. Konop, 236 F.3d at 1043-44.
119. See id. at 1045 (citing Akamine, supra note 73, at 561).
121. See supra Part IV.A.
122. Konop, 236 F.3d at 1043.
123. 262 F.3d 972 (9th Cir. 2001).
124. 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003).
125. Konop, 302 F.3d at 879-80.
adopted a narrow definition of "interception" more in line with precedent, requiring that acquisition be contemporaneous with the transfer of the communication for a violation of the Wiretap Act. The court concluded that summary judgment on the Wiretap Act claim was proper because Konop's website constituted a stored electronic communication, which is not included in the Wiretap Act's definition of "interception." With regard to the SCA claim, the court held that summary judgment was not appropriate because a question of fact existed as to whether defendant's viewing of Konop's website fell under the user authorization exemption of § 2701(c)(2).

The Konop court noted that Congress had amended the Wiretap Act to eliminate storage from the definition of wire communication, such that the textual distinction relied upon by the Steve Jackson Games court no longer existed. While the court could have interpreted Congress's amendment to the Wiretap Act as affording stored communications the greater protection of Title I, it chose not to. Rather, the court stated that the purpose of the recent amendment was to reduce protection of voicemail messages to the lower level of protection provided for other electronically stored communications. The court held that "Congress essentially reinstated the pre-ECPA definition of "intercept"—acquisition contemporaneous with transmission—with respect to wire communications" by eliminating storage from the definition of wire communication. Therefore, under the court's interpretation, the amendment under the PATRIOT Act supported the analysis of Steve Jackson Games and its progeny.

The Ninth Circuit went on to say that when Congress passed the PATRIOT Act, that body was aware of the narrow definition courts had given the term "intercept" with respect to electronic communications, but chose not to change or modify that definition. To the contrary, Congress modified the statute to make that definition applicable to

126. See id. at 878 (citing United States v. Smith, 155 F.3d 1051, 1057 (9th Cir. 1998)) (holding that Congress's use of the word "transfer" and its omission of the term "electronic storage" in the definition of electronic communication reflects Congress's intent that "intercept" not apply to electronic communications while they are in electronic storage).
127. Konop, 302 F.3d at 879.
128. See id. at 880.
130. Konop, 302 F.3d at 878.
131. Id.
132. Id.
133. See id.
134. Id.
voicemail messages as well.\textsuperscript{135} Therefore, the court held, "Congress . . . accepted and implicitly approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission."\textsuperscript{136}

\textbf{D. United States v. Councilman}

\textit{United States v. Councilman}\textsuperscript{137} is the most recent circuit court case to wrestle with the contemporaneity problem. This author believes this time the courts got it right. In \textit{Councilman}, the defendant was charged with conspiring to engage in conduct prohibited by certain provisions of the Wiretap Act.\textsuperscript{138} The district court dismissed,\textsuperscript{139} and the court of appeals affirmed the dismissal.\textsuperscript{140} Defendant Councilman was the Vice President of an online listing service for rare and out-of-print books.\textsuperscript{141} As part of its member services, Councilman's company provided e-mail addresses to certain book dealers.\textsuperscript{142} The government charged that the defendant had directed one of his employees to write a program that intercepted and copied all incoming e-mails from Amazon.com to subscriber dealers.\textsuperscript{143} Allegedly, the defendant and other employees read these messages seeking commercial advantage over their competition.\textsuperscript{144} The operations took place entirely in the RAM and hard drive of the company's computer.\textsuperscript{145} Each of the e-mails in question was an "electronic communication" pursuant to 18 U.S.C. \textsection 2510(12).\textsuperscript{146} Councilman was charged with conspiracy to intercept the electronic communications, intentional disclosure of the intercepted communications (in violation of \textsection 2511(1)(a)), using the contents of the intercepted communications (in violation of \textsection 2511(1)(c)), and causing a person to divulge the content of the communications, while in transmission, to persons other than the addressees of the

\textsuperscript{135} See id.
\textsuperscript{136} Id.
\textsuperscript{137} 373 F.3d 197 (1st Cir. 2004), \textit{reh'g en banc granted, opinion withdrawn by}, 385 F.3d 793 (1st Cir. 2004), \textit{rev'd en banc by}, 418 F.3d 67 (1st Cir. 2005).
\textsuperscript{138} 18 U.S.C. \textsection 2510-2522 (2000). The statute applicable here is the version immediately prior to the October 26, 2001 amendment to the PATRIOT Act.
\textsuperscript{140} See United States v. Councilman, 373 F.3d 197, 204 (1st Cir. 2004) [hereinafter \textit{Councilman I}].
\textsuperscript{141} Id. at 198.
\textsuperscript{142} See id.
\textsuperscript{143} See id. at 199.
\textsuperscript{144} See id.
\textsuperscript{145} See id.
\textsuperscript{146} See id. at 199.
communications (in violation of § 2511(3)(a)). The defendant moved to dismiss the case, arguing that because the e-mails in question were in "electronic storage" (as defined in § 2510(17)) they therefore could not be intercepted as a matter of law.

The government argued that the legislative history showed that if an electronic communication is obtained while simultaneously in transmission and in storage, interception occurs. The communications at issue were "electronic communications" as defined by the pre-PATRIOT Act definition of a "wire communication," under which electronic storage of a communication was included. However, in defining "electronic communication," no similar statement was made. Based on Congress's decision to recite such an explicit inclusion, the court held that electronic storage is not part of electronic communication. The First Circuit found the statute to be unambiguous: Congress meant to give lesser protection to electronic communications than to wire or oral communications. Accordingly, the court affirmed the district court's dismissal of the Wiretap Act violation.

The court relied on the reasoning set forth in Steve Jackson Games and Konop. Councilman I was the first case in which a circuit court adopted Konop's view that Congress accepted and implicitly approved the judicial definition of "intercept" as acquisition contemporaneous with transmission, originating in Turk, and continuing through Steve Jackson Games and its progeny.

In his dissent, Judge Lipez, who would later write the en banc opinion reversing the First Circuit's original opinion, described the transmission of e-mail messages in more detailed terms, and did not see the impediment that the majority saw. First, with regard to the exclusion of "electronic storage" within the definition of "electronic communication," he rejected the majority's use of the canon of

147. See id.
148. See id. at 200.
149. See id. at 203.
151. See id. at § 2510(12) (1997).
152. See Councilman I, 373 F.3d at 201 (relying on the following canon of construction: "When Congress includes a particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.").
153. See id.
154. See id. at 204.
155. See id. at 202-03.
156. See id. at 204-05 (Lipez, J., dissenting).
construction. Second, Judge Lipez employed a different canon of construction to argue that the absence of any mention of a communication in electronic storage amongst the exceptions listed under the definition of “electronic communication” indicates an exclusionary Congressional intent.

On August 11, 2005 the First Circuit reversed its previous opinion and held that Congress intended that the term “electronic communication” be interpreted broadly and did not intend, by including electronic storage within the definition of wire communications, to thereby exclude electronic storage from the definition of electronic communications. The court further held that the term “electronic communication” “includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act.”

In an opinion that methodically unraveled the First Circuit’s panel opinion issued thirteen months earlier, Judge Lipez rejected the maxim of expressio unius est exclusio alterius, put forth by the defendant and adopted previously. Instead the court found the maxim was “not helpful,” that it was merely a presumption capable of being rebutted. The court rebutted this presumption by pointing out “Congress knew how to, and in fact did, explicity exclude four specific categories of communications from the broad definition of ‘electronic communication.’” The court also finally clarified the ambiguity that surrounded the legislative history of the ECPA, as the court explained “the purpose of the broad definition of electronic storage was to enlarge privacy protections for stored data under the Wiretap Act, not to exclude e-mail messages stored during transmission from those strong protections.” Once the court determined the term “electronic communication” includes transient electronic storage, smashing the distinction between “in transit” and “in storage,” it easily and logically

157. See id. at 209 (referring to its use as a “non-textual, inferential leap”).
158. See id. at 210.
159. See United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005) [hereinafter Councilman II].
160. Id.
161. Also referred to as the Russello maxim or canon of construction: “Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.” TRW v. Andrews, 534 U.S. 19, 28 (2001).
162. See Councilman II, 418 F.3d at 74.
163. Id. at 75.
164. Id. at 77.
found that the defendant had intercepted the e-mails in question, in violation of the Wiretap Act.

V. PROBLEMS PRESENTED BY THE CURRENT JUDICIAL INTERPRETATION OF THE ECPA

A. The Konop Argument, that Congress Implicitly Approved the Judicial Definition of “Intercept” is Flawed

The claim that the reasoning in Konop is supported by the PATRIOT Act’s recent amendment to the ECPA, is unwarranted and flawed. Such reliance is imprudent because “the views of a subsequent Congress form a hazardous basis for inferring the intent of an earlier one.”165 Moreover, the argument that the amendment reinstated the pre-ECPA definition of intercept—acquisition contemporaneous with transmission—with respect to wire communications is flawed because it rests on the supposition that Congress implicitly approved a judicial definition of “intercept” requiring contemporaneity. “Such a belief requires an assumption that Congress was aware of the narrow definition courts had given the term “intercept” with respect to electronic communications.”166 Courts have described the ECPA as caught up in a “fog,”167 “convoluted,”168 “fraught with trip wires,”169 and “confusing and uncertain.”170 “Considering how muddy this jurisprudence is and how each court starts its opinion by complaining about how convoluted the area of law governing the ECPA is, how could Congress have possibly become aware of a common judicial definition for intercept with regard to any form of communication?”171 Perhaps the more
important question, however, is whether such a common judicial definition exists.\textsuperscript{172}

The dissenting opinion in \textit{Konop} highlighted some other difficulties with the majority's decision.\textsuperscript{173} Citing a past Ninth Circuit decision,\textsuperscript{174} the dissent pointed out that in determining whether a wire communication has been intercepted, the court rejected a contemporaneous transmission requirement.\textsuperscript{175} The dissent further argued that this contradiction creates a massive loophole in the electronic communications clause of the ECPA.\textsuperscript{176} Additionally, most electronic communications do not enjoy statutory protection under the Ninth Circuit's reading of the ECPA, thereby providing a legal basis for warrantless electronic searches by federal law enforcement.\textsuperscript{177}

It has been argued that information communicated to Internet users from websites is not even protected under the Ninth Circuit's interpretation.\textsuperscript{178} While the Court used the plain-language definition of "intercept" in its decision,\textsuperscript{179} it failed to understand the essential nature of how the Internet functions.\textsuperscript{180} Information is communicated electronically on the Internet through web pages, and the process of loading a web page differs from a phone call, for example, which communicates aural information at the moment of creation, through wires.\textsuperscript{181} When a user visits a specific Uniform Resource Locator ("URL"), the information contained on the web page is transmitted contemporaneously to the user.\textsuperscript{182} Each page load becomes its own communication to the recipient.\textsuperscript{183} Therefore, the contemporaneous

\textsuperscript{172. Blackford, supra note 68, at 849.}

\textsuperscript{173. Konop, 302 F.3d at 886-87 (Reinhardt, J., dissenting). The dissent argued that "stored electronic communications" should not be exempt from the protections of the ECPA. Id.}

\textsuperscript{174. Smith, 155 F.3d at 1051, 1057 n.11.}

\textsuperscript{175. Konop, 302 F.3d at 887 (Reinhardt, J., dissenting) (citing Smith, 155 F.3d at 1058). Smith held Turk's contemporaneity requirement had been "statutorily overruled," at least with respect to wire communications, by the changes in the statute which brought stored wire communications within its purview. See id.}

\textsuperscript{176. Id. at 888.}

\textsuperscript{177. See id.}


\textsuperscript{179. The Court turned to Webster's Ninth New Collegiate Dictionary to define "intercept": "[T]o stop, seize, or interrupt in progress or course before arrival." Konop 302 F.3d at 878.}

\textsuperscript{180. Hector, supra note 178, at 995.}

\textsuperscript{181. See id.}


\textsuperscript{183. See id.}
communication resulting from a page load can be intercepted within the Ninth Circuit’s definition.\textsuperscript{184}

\textbf{B. Councilman II Strengthens the Argument that Gmail Intercepts its Users’ E-mail in Violation of the Wiretap Act}

Although there has been no litigation surrounding Gmail and its practice of scanning e-mail in order to place relevant text advertisements alongside the text of incoming e-mail messages, it is plausible that such an issue may soon arise in the courts, especially if other e-mail providers implement similar advertising techniques.\textsuperscript{185} In the event that such a suit was to be brought under the Wiretap Act, it would most likely fail in the many jurisdictions that require that an e-mail message be intercepted contemporaneously with its transfer.\textsuperscript{186}

A private right of action brought under the Wiretap Act, whether by a Gmail user or third-party sender, would most likely be met with a consent defense by Google. Google would claim the Gmail user consented to Gmail’s practice of scanning e-mail messages in order to display relevant text advertisements.\textsuperscript{187} After receiving the requisite invitation from an existing Gmail user, one must create a Google account in order to become a Gmail user. After filling out some rudimentary information—giving one’s name, and creating a desired login name—the prospective user is presented with a button to press labeled “I have read and agree to the Terms of Use. Create my account.”\textsuperscript{188} This button is simply preceded by the following language: “By registering for the Gmail service, I represent and warrant that I (or, if I am under 18, my legal guardian) understand and agree to the Gmail

\begin{footnotes}
\item[184] Hector, supra note 178, at 996.
\item[185] However, GEICO Insurance Company filed suit against Google in May or 2004 alleging that Google’s practice of showing advertisements for insurance companies when a routine search for “GEICO” was performed amounted to trademark infringement. See Google and GEICO Enter Into Settlement Over Advertising Dispute, INS. L. & LITIG. WKLY, Sept. 19, 2005, at 1. A judge declined GEICO’s request to prevent Google from using this technique. See id. Google uses the same advertisements and technology on Gmail that it does on its search engine. GEICO and Google have since settled out of court. The settlement means Google will not have to cease such advertising tactics, but the specific terms of the settlement are being kept confidential by both companies.
\item[186] See, e.g., United States v. Councilman, 373 F.3d 197 (1st Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).
\item[187] See 18 U.S.C. § 2511(2)(c) (2000) (permitting an interception when “one of the parties to the communication has given prior consent”).
\item[188] Create a Google Account – Gmail (June 24, 2005) (on file with author).
\end{footnotes}
The prospective user is also provided with links to the Terms of Use, Program Policy and Privacy Policy. This is all very misleading, as clicking on the “Terms of Use” link actually takes the prospective Gmail user to a generic Google “Terms of Service” page, not the “Gmail Terms of Use” Page, which exists and may be accessed after creating the account. Nothing on the “Terms of Service” page refers to scanning the contents of e-mail messages, relevant text advertisements or targeted advertisements. Clicking on the “Program Policy” link prior to creating an account merely displays a page that primarily refers to prohibited behavior. Finally, clicking on the “Privacy Policy” link displays a page which discusses Google’s privacy policy in general and addresses such topics as data collection, cookies, and information sharing, but again makes no mention of Gmail’s relevant text advertisements. Thus, the current Gmail registration process is not structured to provide potential users with adequate notice of, or a chance to agree to, the scanning of e-mail messages for content or the placement of relevant text advertisements, at least not until after the user has created a Google and Gmail account.

Once empowered with the elite status of “Gmail user,” the user may stumble upon the Gmail Terms of Use, which presumably, was originally intended for his assent by clicking a small link at the very bottom of his inbox. But who would do so immediately, after creating an account, and presumably having visited the page? Once at the Gmail Terms of Use page the user is immediately greeted with the following: “Welcome to Gmail! Before you register for your Gmail account, you must read and agree to these Gmail Terms of Use and the following terms and conditions and policies, including any future amendments (collectively, the ‘Agreement’).” Oops, too late. Continuing down the page, Google states, “[i]f you do not accept and abide by this Agreement, you may not use the Gmail service.” This sentence is hollow and of no force since Google’s registration process and the opportunity for the user to manifest agreement was flawed at the outset.

189. Id.
190. Id.
192. Gmail Terms of Use, supra note 22.
193. This certainly creates confusion for the user, who having registered for Gmail has missed his opportunity to explicitly agree to the Terms of Use, but now is not sure if he will be deemed to have agreed to the Terms of Use by continuing to use the service.
194. Gmail Terms of Use, supra note 22.
and because there is no way for the user to now indicate his agreement, nor is there a means of enforcing the prohibition on the use of Gmail following non-acceptance or non-adherence to the Agreement.

The two provisions in the Terms of Use relating to relevant text advertisements are as follows:

1. Description of Service. Gmail is a free, search-based email application from Google (the "Service"). You understand and agree that the Service may include content-targeted ads or other related information, as further described below and in the Gmail Privacy Policy. In addition, you understand and agree that the Service is provided on an AS IS and AS AVAILABLE basis. Google disclaims all responsibility and liability for the availability, timeliness, security or reliability of the Service. Google also reserves the right to modify, suspend or discontinue the Service with or without notice at any time and without any liability to you.

8. Advertisements. As consideration for using the Service, you agree and understand that Google will display ads and other information adjacent to and related to the content of your email. Gmail serves relevant ads using a completely automated process that enables Google to effectively target dynamically changing content, such as email. No human will read the content of your email in order to target such advertisements or other information without your consent, and no email content or other personally identifiable information will be provided to advertisers as part of the Service.\(^{195}\)

The first paragraph refers to the inclusion of content-targeted ads but does not specifically mention the means by which these ads are delivered. Moving down, the eighth paragraph addresses the advertisements specifically. The use of the term "completely automated process" is vague. The Terms of Use accurately describe where the advertisements will appear, but fails to explain how this "process" works. Even if the user were to agree in principle to the inclusion of the advertisements, Google does not fully explain that it is actually scanning the contents of each and every one of the user's e-mail messages, each and every time he opens them. Therefore, there is a strong argument that there is an absence of consent by the Gmail user. Google provides a flawed registration process that robs prospective users of the opportunity

\(^{195}\) Id.
to give informed consent and manifest their agreement to the Terms of Use purported to govern their Gmail account.

Regardless of any finding of consent or lack thereof, courts following the reasoning originating from the Fifth Circuit in *Steve Jackson Games* and employing a narrow definition of "intercept" would refuse to find that Gmail intercepts its users' e-mails while in transit, but such a court might find that the e-mails are acquired while in storage, or while simultaneously in transit and storage. A Gmail user may not open a new e-mail for hours or even days after the e-mail has reached his mailbox. *Councilman II* is the first case to break with *Steve Jackson Games* and its progeny. However, in the thirteen months it took for the First Circuit decide *Councilman II*, district courts in the Ninth and Tenth Circuits have decided similar questions of Wiretap Act interpretation based upon *Councilman I*, which is now bad law. According to the reasoning of *Councilman I*, while that e-mail message remains delivered but unopened, it is both in transit and in a form of temporary electronic storage on Gmail's servers. *Councilman I* held that this duality places an unopened, post-transmission e-mail in storage outside of the scope of

---

196. See, e.g., United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003), cert. denied, 538 U.S. 1051 (2003) ("We hold that a contemporaneous interception—i.e., an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications."); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003) ("We therefore hold that for a website such as Konop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003) (adopting the reasoning in *Steve Jackson Games* as to the meaning of intercept under the Wiretap Act); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994) (holding that seizure of stored but unread e-mail messages was not an interception and citing with approval the lower court's requiring interception to be contemporaneous with transmission). On the other hand, e-mail messages opened by the Gmail user, stored, and viewed at a later time (at which time Gmail would re-scan the message and once again match it with a relevant text advertisement) are beyond the purview of the Wiretap Act. See Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635-38 (E.D. Pa. 2001), aff'd on other grounds, 352 F.3d 107 (3d Cir. 2003) (concluding that e-mails taken from post-transmission storage are not in "electronic storage"); H.R. REP. NO. 99-647, at 64-65 (1986) (noting that opened e-mail messages stored on a server are protected under provisions relating to remote computing services).

197. See United States v. Jones, 364 F. Supp. 2d 1303 (D. Utah 2005) (citing *Councilman I* for the rule that in order to prove a violation of the Wiretap Act, the defendant would have to prove that the e-mail messages were intercepted contemporaneously with their transmission); United States v. Ropp, 347 F. Supp. 2d 831, 837 (C.D. Cal. 2004) (holding that "if an electronic communication which is in the process of transit, even if momentarily "parked" in an electronic lot, can be acquired without violating the Act... it [is] difficult to conclude that the acquisition of internal computer signals that constitute part of the process of preparing a message for transmission would violate the Act").

198. See *Councilman I*, 373 F.3d 197, 202-03 (pointing to the presence of the words "any temporary, intermediate storage" in 18 U.S.C. § 2510(17) as controlling).
the Wiretap Act.\textsuperscript{199} Since unopened e-mail messages addressed to Gmail users remain in temporary storage on Gmail's servers before they are retrieved for the first time by the Gmail user, a court adopting this reasoning would have to find that Gmail is not violating the Wiretap Act when it scans its users e-mail in order to lace them with relevant text advertisements. On the other hand, a court following Councilman II could and should come to the opposite conclusion, that Gmail is intercepting its user's e-mails, electronic communications in transient electronic storage.

C. Gmail is Protected by the SCA's Over-Broad Electronic Communications Service Provider Exception

18 U.S.C. § 2701(c)(1) excepts from Title II seizures of e-mail authorized "by the person or entity providing a wire or electronic communications service."\textsuperscript{200} There is no circuit court case law interpreting this exception.\textsuperscript{201} The advent of Gmail's relevant text advertisement technology has rendered this exception over-broad since its effects are of a nature not contemplated by Congress in 1986. While electronic communications service providers may need the ability to access user's stored electronic communications for backup purposes, maintenance of their own servers, or perhaps in order to provide benign services to users such as spell-checking or virus protection software, Gmail's relevant text advertisements are of a completely different nature. The impetus behind the placement of these advertisements is greed. Google generates the overwhelming majority of its annual revenue through Internet advertising.\textsuperscript{202} The only reason Google can afford to provide so many free oversized two and a half gigabyte mailboxes to Gmail's users is that Google is able to guarantee companies that their advertising dollars will be spent on targeted advertisements, and that there will be many targets to choose from. Gmail offers massive storage space and encourages its users to "never delete" their e-mails, thereby providing fodder for the relevant text advertising scanning process.\textsuperscript{203} Gmail is not only scanning users' e-mail

\textsuperscript{199} See id at 203.
\textsuperscript{202} See REVOLUTION MAGAZINE supra note 24.
\textsuperscript{203} See Welcome to Gmail: A Google Approach to Email, http://www.gmail.com (last visited Sept. 10, 2005).
messages contemporaneously with their transmission, but also every time the Gmail user re-opens an e-mail. Each of these previously viewed e-mails is in “electronic storage.” Gmail continues to lure in prospective users with the promise of bigger inboxes. Once they are users, the e-mail service provider from the parent company whose motto is “Don’t Be Evil” exploits them for profit, comfortably shielded from the penalties of the SCA by the statute’s electronic communication service provider exception.

VI. PROPOSED SOLUTIONS AND INSTRUMENTAL EFFECTS

A. Proposed Statutory Interpretation of the Wiretap Act: Moving Past the Assumptions of Konop

Under the narrow reading of the Wiretap Act we adopt... very few seizures of electronic communications from computers will constitute ‘interceptions.’... Therefore, unless some type of automatic routing software is used... interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.204

The dissenting opinions in Konop and Councilman I discuss the problematic and conflicting interpretations of “intercept” as the term applies to electronic communications.205 By holding that Congress implicitly approved the judicial definition of “intercept” as acquisition contemporaneous with transmission,206 the Ninth Circuit created a paradigm in Konop that supports the same statutory distinction that has troubled scholars for almost twenty years. Although the majority opinion addresses the law prior to the passage of the PATRIOT Act, the issues presented by this distinction will remain relevant for as long as cases like

---

Gmail is an experiment in a new kind of webmail, built on the idea that you should never have to delete mail and you should always be able to find the message you want. The key features are:

- Don’t throw anything away.
- Over 2604.977204 megabytes (and counting) of free storage so you’ll never need to delete another message.

Id.

204. United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003).
206. Konop, 302 F.3d at 878.

Published by Scholarly Commons at Hofstra Law, 2005
Konop, Steiger, and Fraser are allowed to stand.\textsuperscript{207} The First Circuit’s decision in \textit{Councilman II} is not only a fair interpretation of the ECPA, but it makes practical sense. In similar cases arising in the future, the other circuits should reevaluate their jurisprudence on the Wiretap Act’s contemporaneity requirement in light of \textit{Councilman II}. The First Circuit’s interpretation of the statute must supplant those currently held and promulgated in other circuits in order to conform to Congress’s intent and the reality of modern technology.

If the courts were to find electronic communications in temporary, intermediate storage incident to the transfer of those communications that may be intercepted contemporaneously with transmission, Gmail’s scanning of e-mail messages as they are opened in order to deliver relevant text advertisements would most certainly violate the Wiretap Act. While Google might adjust Gmail so that it only begins scanning the second time the Gmail user views a particular e-mail message, this practice may violate the SCA depending on the interpretation of the electronic communications service provider exception. It is possible Gmail would have to completely abandon the practice of scanning users’ e-mail messages.

\section*{B. Statutory Amendment of the Wiretap Act}

It will be up to Congress to step in and remedy the situation if the courts refuse to follow \textit{Councilman II} and fail to realize Gmail’s dramatic encroachment on Internet privacy rights authorized under a narrow definition of “intercept.” One solution is to amend the Wiretap Act to create a uniform meaning of “interception” for both wire and electronic communications.\textsuperscript{208} “If the current interpretations are applied, the privacy rights of all Internet users will be severely compromised.”\textsuperscript{209} To prevent this erosion of Internet privacy, Congress should amend the pertinent statutes to specifically include unopened, post-transmission e-mail messages in temporary storage within the list of communications that may be intercepted.\textsuperscript{210} There would be no need to include all stored

\textsuperscript{207} Id. at 887-88 (Reinhardt, J., dissenting) (discussing the interception and investigation of stored electronic information).
\textsuperscript{208} See Hector, supra note 178, at 1003; see also Konop, 302 F.3d at 887-88 (Reinhardt, J., dissenting) (indicating that this term’s statutory meaning has not been firmly established by the courts). Justice Reinhardt’s dissent points out that the varying definitions of “interception” “have rendered the intercept prohibition . . . meaningless.” Id. at 887.
\textsuperscript{209} Hector, supra note 178, at 1003.
\textsuperscript{210} Cf. id. (arguing that “Congress should amend the pertinent statutes to specifically include stored electronic and wire communications within the list of communications that can be intercepted”). Since \textit{Councilman I}, the House of Representatives has introduced bills that would
electronic or wire communications within such a class of communication that may be intercepted under the statute because the SCA would cover e-mail messages a Gmail user views, stores, and views again. However, unopened, post-transmission e-mail messages should not be denied protection under the Wiretap Act simply because temporary electronic storage is incident to their communication to the Gmail user. This proposal is based on the argument that the electronic communications process envisioned by the ECPA includes more than mere “transmission”; it includes “transfer”—the entire process of communication, from the e-mail message’s point of origin to receipt by its intended recipient. The new text could read as follows:

§ 2510. Definitions

As used in this chapter [18 USCS §§ 2510 et seq.]
(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication, including those in any temporary, intermediate storage incidental to the electronic transmission thereof, through the use of any electronic, mechanical, or other device.

The goal of this amendment would be to broaden the very narrow judicial interpretation of “intercept” under the Wiretap Act. Even though this amended definition of “intercept” would include some e-mail messages in temporary electronic storage, it is still consistent with the developing case law, because the unopened e-mail messages this proposal seeks to cover under the Wiretap Act are still intercepted contemporaneously with their transmission. Under this definition of “intercept,” Gmail would violate § 2511(1)(a) of the Wiretap Act and be subject to its penalties for scanning previously unread e-mail messages contemporaneously with their first viewing by a Gmail user in order to place relevant text advertisements next to the e-mail message.


211. See Hector, supra note 178, at 1003.
212. See Akamine, supra note 73, at 562-565 nn.207-08.
B. Proposed Statutory Amendment of the SCA: Narrowing the Electronic Communications Service Provider Exception

Gmail's exploitation of its users must be stopped because Congress did not anticipate the use of technology in this manner when they passed the ECPA, and because there is no case law interpreting the statute. Congress should address the need for an updated statute that contemplates the use of relevant text advertisements. The amended SCA could read:

§ 2701. Unlawful access to stored communications
(a) Offense. Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided;

....

(c) Exceptions. Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service, so long as the conduct of the person or entity does not confer a pecuniary benefit upon the electronic communications service grossly disproportionate to the benefit received by the user of that service;
(2) by a user of that service with respect to a communication of or intended for that user; or
(3) in section 2703, 2704 or 2518 of this title [18 USCS § 2703, 2704, or 2518].

The addition of language prohibiting the electronic communications service from engaging in conduct that monetarily benefits the service places Gmail's conduct within the scope of the SCA while still granting electronic communications services the access to perform the functions and processes necessary to electronic communications. The "grossly disproportionate" language would give courts flexibility to determine whether a service provider has violated the statute on a case-by-case basis, and would invite the courts to employ a simple test balancing the benefits received by both user and service provider.
As access to the Internet continues to burgeon, the number of people communicating via stored electronic and wire communications will continue to increase. Therefore, it is absolutely imperative that judicial interpretation of these protective statutes be consistent with the legislative aim of protecting the privacy rights of those individuals communicating electronically.

The introduction of Gmail and its relevant text advertisement technology poses a large threat to the privacy of senders and recipients of e-mail messages. Google is luring individuals to use their service with the promise of bigger inboxes and powerful search capabilities, and then exploiting those individuals. Gmail is harnessing the advertising revenue potential deep within the billions of e-mail messages of its users as those messages arrive and while those messages sit in storage on Gmail servers. The courts have reduced the effectiveness of the Wiretap Act by narrowly interpreting the word “intercept” and thereby expelling unopened, post-transmission e-mails in storage outside of the scope of the Wiretap Act and leaving them to be protected by the SCA, whose electronic communications service provider exception is out of date and so overbroad as to not protect e-mail messages sent to Gmail users. Councilman II is a step in the right direction, and should guide other circuits in interpreting the Wiretap Act broadly to include unopened, post-transmission e-mails in storage. Failing a change in judicial interpretation, or a grant of certiorari by the Supreme Court, Congress should amend the Wiretap Act and the SCA in order to create a uniform meaning of “interception” for both wire and electronic communications, and to narrow the electronic communications service provider exception. The time for these changes is now, before the placement of relevant text advertisements becomes firmly entrenched as just another privacy concession in the rapidly evolving sphere of e-mail communication.

Jason Isaac Miller*

---

213. See Hector, supra note 178, at 1003.

* J.D. candidate, 2006, Hofstra University School of Law. I would like to thank Professor Michael R. Siebecker and Lauren Reaves for their assistance with this Note. I would also like to express my deepest gratitude to my colleagues at the Hofstra Law Review for their diligent review and hard work, especially Adam Wactlar, Alexis Collentine, Kara Mannix, and Peter Siroka. This Note is dedicated to my parents. Thank you for your endless love and your time and energy; you are my inspiration.
***