Judicial Interpretations of the Electronic Communications Privacy Act Raise Concerns about Whether the Airline Industries' Online Business Ventures Are Protected

Christopher T. Blackford

Follow this and additional works at: https://scholar.smu.edu/jalc

Recommended Citation
https://scholar.smu.edu/jalc/vol68/iss4/8

This Comment is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Journal of Air Law and Commerce by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
JUDICIAL INTERPRETATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT RAISE CONCERNS ABOUT WHETHER THE AIRLINE INDUSTRIES' ONLINE BUSINESS VENTURES ARE PROTECTED

CHRISTOPHER T. BLACKFORD*

I am not an advocate for frequent changes in laws and institutions. But laws and institutions must go hand-in-hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change, with change of circumstances, institutions must advance also to keep pace with the times.1 Change is the law of life. And those who look only to the past or present are certain to miss the future.2

I. INTRODUCTION

II. BACKGROUND OF THE JURISPRUDEENCE SURROUNDING "ELECTRONIC COMMUNICATIONS"

A. PRIOR TO THE ENACTMENT OF THE ECPA: THE OMNIBUS ACT

B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

1. Title I of the ECPA: The Federal Wiretap Act

2. Title II of the ECPA: Stored Communications Act

3. Judicial Interpretations of the Electronic Communications Privacy Act

* B.S.E.E., 1999, M.S.E.E., 2001, University of Texas at Dallas; candidate for J.D., 2004, Southern Methodist University Dedman School of Law. The author wishes to thank Professor Gregory Crespi, SMU Dedman School of Law, for his helpful suggestions.


2 John F. Kennedy, Frankfurt, West Germany (June 25, 1963), quoted in Steere, supra note 1, at 264.
III. IMPLICATIONS OF THE DIFFERENT JUDICIAL CONSTRUCTIONS OF THE ECPA

A. Steve Jackson Games: Adopting the Narrow Reading of Intercept to the Wiretap Act, but Not to the Stored Communications Act

B. Smith: Repudiation of the Contemporaneity Requirement and Promotion of the Lesser Included Offense Theory

C. The Konop and Steiger Opinions: Two Definitions for Intercept and the Effect of the USA Patriot Act

D. Steiger: Does the Stored Communications Act Protect You from Computer Hackers?

E. Fraser: Adopting the Narrow Reading for Both Statutes

IV. PROPOSAL FOR A NEW INTERPRETATION OF THE ECPA

A. A Contemporaneous Acquisition/Access Reading, Independent of Which Statute Governs, Permits a Reading of the Wiretap Act and the Stored Communications Act that is Consistent with Congressional Intent, Follows the Plain Language of the Statutes, Provides Technological Flexibility, and Affords Privacy and Protection.

1. At what point in time is the communication acquired or accessed?

2. Was the defendant in a position to merely acquire the communication, or did the defendant actually acquire the communication?

3. Balancing congressional intent with technology and protection

a. Following congressional intent
I. INTRODUCTION

WHEN ENTREPRENEURS and scientists alike embraced the Internet as a source of endless opportunities, its infrastructure experienced unprecedented growth. Although unresponsive at first, businesses and individuals eventually accepted the Internet and the entrepreneurial ingenuity associated with it. In the end, the role of electronic communications in the world has expanded exponentially since the 1980s. Furthermore, almost all facets of the business community have become, and continue to become, increasingly connected and dependent upon both the Internet and other forms of electronic communications. While this pattern of growth seems mutually beneficial to almost everyone involved, the high level of symbiotic dependence has exposed parties to the ever increasing prospect of being victimized by computer crimes. The threat of a business being exposed to either an unauthorized disclosure of information, or rampant computer criminal activity such as eavesdropping, insider transgression, and spoofing is no longer a remote possibility.

3 While very few computers were linked to the Internet in 1981, 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).

4 In a recent study of computer crimes, “eighty-five percent of respondents detected computer security breaches within the last twelve months,” and “thirteen percent of respondents reported theft of transaction information.” John McElwaine, Cyber Attacks, 13 S.C. LxWVER 20, 22 (2002) (citing Richard Powers, 2001 CSI/FBI Computer Crime and Security Survey, Vol. 7, No. 1, Computer Security Institute (Spring 2001)). In 1999, the FBI opened 547 computer intrusion cases, and in 1999 that number escalated to 1,154 cases. Id. at 21 (quoting Louis Freeh, Director of the Federal Bureau of Investigation, before the Senate Judiciary Subcommittee for Technology, Terrorism and Government Information (Mar. 28, 2000)).

5 Eavesdropping involves the “passive collection of information through Internet channels.” Id. at 22. Cyber criminals will install programs that enable them to intercept log on identifiers and passwords. With this information, the individual’s identity is replicated and personal information becomes freely accessible. Id.

6 “An insider is a current or former employee of a company who possesses knowledge of the company’s network that allows them to gain unrestricted access . . .” Id. Such access is commonly used for two reasons: (1) to cause damage
While it is true that crime is a facet of life that businesses should be prepared to encounter, the issue of cyber-exposure is particularly troubling for a business because of the potential economic impact and the lack of appropriate legal protection.\(^8\) Although the business world is already familiar with the impact that denial of service attacks\(^9\) had on Internet sites such as Yahoo!, Amazon.com, eBay, CNN, and Buy.com,\(^{10}\) regulatory agencies do not appear to be concerned about the vulnerability of other industries who have evolved their business plans around the Internet.

Airlines, which rely heavily upon their own website’s sales, are prime examples of business entities that are economically vulnerable to cyber exposure.\(^{11}\) Considering the cumulative cost associated with developing and maintaining airline web sites,\(^2\) the net profits generated by the business,\(^3\) and the risks associated with maintaining secure business transactions over the web, the $110 billion per year airline industry is in danger of enduring considerable economic loss. Airline vulnerability is amplified by the fractured status of the airlines in a post-September 11th world.\(^{14}\) Although some economists have noted signs of

\(^{7}\) “Spoofing is accomplished by deceiving a computer user into believing that it [sic] is disclosing information to a trusted source.” \(\text{Id.}\)

\(^{8}\) The 2001 Computer Crime and Security Survey reported that 186 respondents suffered a combined financial loss of $377,828,700. \(\text{Id.}\)

\(^{9}\) “A denial of service attack is intended to tie up a computer system’s resources to such an extent that the system is unresponsive or crashes.” \(\text{Id.}\) (citing How a Denial of Service Attack Works, CNET News.com (Feb. 9, 2000), at http://www.cnet.com (last visited Sept. 7, 2003)). A “visitor” sends multiple authentication requests with false return addresses to a victim server. \(\text{Id.}\) As these false requests continue and the victim server continues to try and locate the visitor, the victim server’s system resources are consumed. \(\text{Id.}\)

\(^{10}\) \(\text{Id.}\) at 21.

\(^{11}\) The entire competitive landscape of the on-line travel industry has been valued at roughly $31 billion and has been labeled as “one of the fastest growing niches of e-commerce.” Rachel Konrad & Greg Sandoval, Orbitz Rivals Cry Foul, Claim Monopoly in Air Travel, CNET News.com (Apr. 11, 2002), at http://www.news.com/2009-1017-879314.html (last visited Sept. 7, 2003).

\(^{12}\) Airlines such as United, American, Delta, Northwest, and Continental reportedly invested $145 million in an on-line travel venture known as “T2.” \(\text{Id.}\)

\(^{13}\) On-line travel agencies such as Orbitz and Expedia reached $1 billion in annual revenue in the year 2000. \(\text{Id.}\)

\(^{14}\) Due to curtailed flights and plummeting passenger traffic, airlines suffered extraordinary losses after the September 11th terror attacks. In the immediate year after the September 11th attacks, “industry losses totaled $7.7 billion despite emergency federal cash infusions of $5 billion . . . .” Daniel G. Fricker, \textit{Airlines}
improvement in air travel, it is clear that the airline industry still faces turbulent economic times.

The combination of the airline industry's current financial problems along with the potential for further economic downfall should trigger concerns about what remedies an airline will be entitled to if its web-based business is exposed to an unauthorized cyber attack. More importantly, the legal community should be concerned about how the current laws are being judicially interpreted. Although the current laws enacted by Congress to police the Internet are far from clear, judicial constructions of the Electronic Communications Privacy Act (ECPA) have been nothing short of atrocious. Instead of truly understanding the intricate technological details of the Internet and considering how technological advancements affect the statutory rules that are applied, judges have employed linguistic gymnastics and established meaningless textual dichotomies between the governing statutes in an effort to maintain outdated precedents. Such judicial interpretations have created a mud-

Struggle in Post-9/11 Climate, DETROIT FREE PRESS (Aug. 31, 2002), at http://www.freep.com/money/business/ air31_20020831.htm (last visited Sept. 7, 2003). The staggering losses have forced airlines such as USAirways and United Airlines to declare bankruptcy. Id. Other carriers who are wavering on the point of bankruptcy will require massive restructuring to continue. Id.

Despite the spiraling costs of airline security, lost jobs have been regained and passengers are slowly returning to the airports. Arlene Fleming, Airline Losses After September 11th: The Day That Airline Travel Changed, Airtravel.About.com (Nov. 22, 2002), at http://airtravel.about.com/library/weekly/aa090902a.htm (last visited Aug. 27, 2003).

Experts' predictions have been proven true as the nations major airlines recently reported a combined loss of more than $9 billion. Dave Carpenter, United Airlines' Parent Loses $3.2 Billion, SALT LAKE TRIBUNE (Jan. 31, 2003), at http://www.sltrib.com/2003/Feb/02012003/Business/25278.asp (last visited Sept. 7, 2003). While “[t]he industry as a whole has a chance to turn a profit in 2004, . . . much of that money will be used to repay the debt from funding 2001 and 2002 losses.” Fricker, supra note 14.

The intersection of the Electronic Communications Privacy Act (“ECPA”) and the Stored Communications Act (“SCA”) is a “complex, often convoluted, area of the law.” Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (citing United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998)); see also Steve Jackson Games, Inc. v. United States Secret Serv., 96 F.3d 457, 462 (5th Cir. 1994) (stating that the Wiretap Act “is famous (if not infamous) for its lack of clarity”). The difficulty is further compounded by the fact that “the ECPA was written prior to the advent of the Internet and the World Wide Web.” Konop, 302 F.3d at 874. Courts are thus essentially confined to using an existing statutory framework that is ill-suited for dealing with modern forms of web communication and inappropriate for the purpose of administering justice. Id.
dled pool of jurisprudence that affords airlines and other businesses a legislative bill without teeth.

This comment scrutinizes the economic, business-oriented ramifications of recent judicial reviews of the Electronic Communications Privacy Act in the context of electronic communications and web sites. It specifically questions how airlines with significant on-line business ventures will be affected. The comment is divided into five sections and will first examine the historical development of the relevant case law protecting the privacy of electronic communications. This part of the comment will also address the history of the ECPA’s passage into law and Congress’ intended purpose. The third section discusses the implications of the different judicial constructions of the ECPA’s provisions, and the fourth section of this comment proposes an interpretation of the ECPA that actually affords airlines and other businesses the appropriate statutory protection required to succeed in a post-September 11th world. Finally, this article concludes that courts should reconsider the current classification of unauthorized web site access and the type of statutory protection that it triggers, because the current judicial standards will likely promote, rather than deter, future computer criminal activity and unauthorized disclosure in the cyber world.

II. BACKGROUND OF THE JURISPRUDENCE SURROUNDING “ELECTRONIC COMMUNICATIONS”

A. PRIOR TO THE ENACTMENT OF THE ECPA: THE OMNIBUS ACT

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.\textsuperscript{18} Title III proscribes the interception or disclosure of wire or oral communications and provides a procedure through which law enforcement officials are authorized to intercept such communications in limited circumstances.\textsuperscript{19} The enactment of Title III was significant. Congress had finally recognized that technological devel-


\textsuperscript{19} Title III punished “any person who . . . willfully intercepts, endeavors to intercept, or procures any other person to intercept, any wire or oral communication . . . ” 18 U.S.C. § 2511(1)(a) (1968).
opments enable the interception of personal and commercial communications. Title III, however, was relatively limited. Title III prohibited only the interception of communications that could be heard and understood by humans as sound. Furthermore, the language of the statute was narrowly construed to restrict the act of interception to the contemporaneous acquisition of communication. In other words, protection from an unauthorized interception was confined to a narrow time frame in which transmission and acquisition of the communication occurred at the exact same time.

B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

In 1986, Congress became concerned with federal privacy protections and potential harms that new computer and telecommunications technologies posed for the protection of confidential business information. As a result, Congress sought to increase protection of personal and commercial communications. Congress acted by modifying the Wire and Electronic Communications Interception and Interception of Oral Communications Act ("Wiretap Act") through the Electronic Communications Privacy Act (ECPA) of 1986. In creating the ECPA, Congress substantially amended the Wiretap Act and created the Stored Communications Act (SCA), thus providing a statutory umbrella of protection for electronic communications.

21 "While Congress clearly was concerned with the protection of individual's privacy interests against unjustified intrusions, it did not attempt through Title III to deal with all such intrusions." United States v. Turk, 526 F.2d 654, 658-59 (5th Cir. 1976) (emphasis added). Title III dealt only with problems associated with wiretapping and electronic surveillance. See id. at 659 (citations omitted).
23 Turk, 526 F.2d at 659.
24 The narrow judicial construction of the term "intercept" emanated from the influential case of United States v. Turk. At issue in Turk was whether police intercepted a communication when they played back a tape of a telephone call that had been previously recorded by a third party. Id. at 656-58. The Fifth Circuit held that no unlawful interception occurred. Id. at 659. The court reasoned that "the words 'acquisition . . . through the use of any . . . device' suggests that the central concern is with the activity engaged in at the time of the oral communication . . . " Id. at 658.
27 Id. §§ 2701-2711.
28 The Wiretap Act and the SCA have since been amended numerous times. Most recently, the Wiretap Act and the SCA were amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept
Although Congress should be commended for recognizing that it had not fully addressed the rapid advances in communication technologies wrought by the proliferation of computers, the original enactment of the ECPA can scarcely be considered a model of clarity. When neither a Congressional nor a judicial forum are technologically competent enough to comprehend the role of technology in the advancement of communications, efforts to take into account the technological realities of electronic communications will be misplaced.

1. **Title I of the ECPA: The Federal Wiretap Act**

The 1986 Federal Wiretap Act provides in relevant part, with certain exceptions, that there is a criminal or civil cause of action against any person who:

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication . . .
(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]
(d) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.30

The most significant change made by the enactment of the ECPA was the addition of the “electronic communications”31

---

29 The United States Court of Appeals for the Fifth Circuit stated that the Wiretap Act "is famous (if not infamous) for its lack of clarity." Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994). The United States Court of Appeals for the Ninth Circuit criticized further, stating that the Fifth Circuit "might have put the matter too mildly." United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).


31 An "electronic communication" was defined, with certain exceptions, 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, photoelectric, or photo-optical system. . ." Id. § 2510(12).
category to the Wiretap Act. Another notable change introduced by the Act was the change in the definition of "wire communication," which was both narrowed and broadened. The definition of "wire communication" was narrowed from "any communication" made over the wires to "any aural transfer" made over the wires, and it was broadened to include "any electronic storage of such communication." These statutory changes have proven to be the subject of much judicial debate. The decision to include electronic storage in the definition of "wire communication" was especially problematic, because the correlating definition of "electronic communication" contained no reference for a similar form of storage medium.

As noted, the Wiretap Act provided for either a civil or criminal cause of action to punish violators. Criminal prosecution of an individual who violates the Wiretap Act under section 2511 may provide for incarceration for a period up to five years, while a suit for civil damages under section 2520 may provide for appropriate equitable and declaratory relief, punitive damages, and reasonable attorney's fees.

2. Title II of the ECPA: Stored Communications Act

The 1986 Stored Communications Act also provides protection for private communications, barring unauthorized access to an electronic communication while it is in electronic storage. However, it does not provide the same type or amount of protection as the Wiretap Act. Aside from the notable difference between the two acts concerning the forms of communication protected, the SCA provides less stringent criminal and civil penalties.

---


33 A "wire communication" was defined, with certain exceptions, as "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 . . . and such term includes any electronic storage of such communication . . ." 18 U.S.C. § 2510(1) (1986) (emphasis added).

34 Id.

35 Id.

36 Id. § 2511(4).

37 Id. § 2520.

38 Id. § 2701.

39 Compare id. §§ 2511(4)(a), 2520(c)(2)(B) (imposing penalties of up to five years imprisonment and a $10,000 fine for unlawfully intercepting an electronic
The SCA provides in relative part, with certain exceptions, that there is a criminal or civil cause of action against one who:

(1) intentionally access[es] 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.  

While the plain language of the SCA seems to suggest that the statute was enacted to address access to stored wire and electronic communications and transactional records, judicial opinions illustrate that attorneys should not jump to such a conclusion.

3. Judicial Interpretations of the Electronic Communications Privacy Act

The problems legal scholars and judges encounter when attempting to construe the ECPA become more readily apparent when trying to conceptualize both the Wiretap Act and the SCA in one harmonious legal relationship. Individuals have struggled, and continue to struggle, to determine the boundaries of the relationship between the Wiretap Act and the SCA.

The following cases are notable examples of courts struggling to determine whether a particular set of facts entitle one to relief under either the Wiretap Act or the SCA. Because the ECPA remained largely unchanged until the recent passage of the 2001 USA Patriot Act, these cases give an insight into the judicial development of the ECPA.

---

40 Id. § 2701.
43 After the passage of the ECPA in 1986 and before the enactment of the USA Patriot Act in 2001, only minor amendments were made in 1994 and 1996.
a. *Steve Jackson Games, Inc. v. United States Secret Service,* 36 F.3d 457 (5th Cir. 1994)

Suspecting that a computer text file detailing a company’s emergency 911 telephone system had been copied and was available as a document in e-mail messages on an electronic bulletin board system, the United States Secret Service (“Secret Service”) seized the computer that hosted the electronic bulletin board service by raiding the offices of Steve Jackson Games, Inc. Consequently, the Secret Service seized 162 items of unread (and un-retrieved), private e-mail messages from the hard drive of the computer running the bulletin board system. Steve Jackson and other intended recipients of the unread, private e-mail, filed suit against the Secret Service claiming that the agency had intercepted and disclosed private communications in violation of both the Wiretap Act and the SCA.

The district court held that the Secret Service had violated the SCA, but not the Wiretap Act. Relying on the Fifth Circuit’s previous narrow interpretation of intercept in *United States v. Turk,* the district court concluded that there was no violation of the Wiretap Act because the Government’s acquisition of the contents of the electronic communications was not contemporaneous with the transmission of those communications. The basis for finding a violation of the SCA was seizure of the stored electronic communications without complying with the statutory provisions. Not finding the sole statutory damage award under the SCA sufficient, the plaintiff appealed to the Court of Appeals for the Fifth Circuit.

The issue for the Fifth Circuit Court of Appeals was whether the seizure of a computer, used to operate an electronic bulletin board system and thus containing unread (and un-retrieved) private e-mail messages, constitutes an intercept proscribed by

---

44 Running off of a computer that acts like a server, an electronic bulletin board system is a collection of private e-mails maintained on the computer’s hard disk drive temporarily until the e-mail addressees access the electronic bulletin board system to retrieve their e-mail messages. After receiving their e-mail, recipients chose to either delete the e-mail message or store it on the electronic bulletin board computer’s hard disk drive. *Steve Jackson Games,* 36 F.3d at 458-59.

45 *Id.*

46 *Id.* at 459.

47 *Turk,* 526 F.2d at 654.

48 *Steve Jackson Games,* 36 F.3d at 459-60.

49 *Id.* at 459.

50 *Id.* at 457. The plaintiffs sought the increased damage award warranted by the Wiretap Act. *Id.* at 460.
the Federal Wiretap Act or the SCA. For guidance in resolving the issue, the court of appeals examined the technical definitions within the ECPA, the legislative history, and the statutory procedures and requirements for both Acts. When comparing the statutory definitions of wire and electronic communications, the court of appeals observed that unlike the definition of "wire communication," the definition of "electronic communication" does not include electronic storage of such communication. The omission of the phrase "electronic storage of such communication" from the definition of "electronic communication" was seen as critical in determining what constituted an intercept. The court of appeals stated that this omission and the use of the word "transfer" in the definition of "electronic communication" "reflect that Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'" Because the e-mail at issue was in electronic storage, the court of appeals concluded that the Secret Service's seizure of the e-mails was not an interception, and consequently, not a violation of the Wiretap Act.

To support the conclusion that Congress did not intend for the term intercept to apply to electronic communications in electronic storage, the court of appeals pointed to the ECPA's legislative history. Specifically, the court noted that the Senate Report accompanying the ECPA indicates that Congress did not intend to change the narrow definition of intercept, which requires any acquisition to be contemporaneous with transmission. If the narrow definition of intercept requiring contemporaneous acquisition holds, the court reasoned that electronic communications in storage, which have already been transmitted, cannot be intercepted.

51 Id.
52 See supra note 33.
53 See supra note 31.
54 Steve Jackson Games, 36 F.3d at 461.
55 Id.
56 Id. at 461-62 (emphasis added).
57 Id. at 461.
58 Id. at 462. The Senate Report provides that "[s]ection 101(a)(3) of the [ECPA] amends the definition of the term 'intercept' in current section 2510(4) of title 18 to cover electronic communications. The definition of 'intercept' under current law is retained with respect to wire and oral communications except that the term 'or other' is inserted after 'aural.'" S. Rep. No. 99-541, at 13 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3567, construed in Steve Jackson Games, 36 F.3d at 462.
Additionally, the court implied that if the term “intercept” did apply to electronic communications in storage, conduct prohibited under the Wiretap Act would also provide a cause of action under the SCA. In light of express differences between the substantive and procedural requirements of the Wiretap Act and SCA, the court determined that Congress could not have intended for prohibited conduct to provide a cause of action under both statutes.\(^5\) For example, whereas a governmental entity only requires a search warrant to access the contents of a stored electronic communication that has been in storage for less than 180 days,\(^6\) the requirements for authorization to intercept a stored wire communication are much more extensive and stringent.\(^6\) When procedural differences exist between the two statutes, a cause of action available under both statutes would result in the exploitation of the less stringent requirements.

b. *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998)

After calling fellow employee Angela Bravo de Rueda (“Bravo”) and leaving a voicemail message describing his involvement in insider trading, Richard Smith (“Smith”) came under investigation by the Securities and Exchange Commission for eleven counts of insider trading.\(^6\) Unbeknownst to Smith or Bravo, a third employee, Linda Alexander-Gore (“Gore”), accessed Bravo’s voice mailbox and forwarded the stored message to her mailbox.\(^6\) Gore then copied the communication and disclosed it to the U.S. Attorney’s Office.\(^6\) Although the district court suppressed the actual voicemail message as evidence after determining that it had been illegally “intercepted” within the meaning of the Wiretap Act, it refused to suppress the remainder of the evidence that was derived from the illegal wiretap.\(^6\) Claiming that all evidence emanating from the illegal wiretap should have been suppressed, Smith appealed to the Court of Appeals of the Ninth Circuit.\(^6\) The Government countered by

\(^5\) *Steve Jackson Games*, 36 F.3d at 462-63.
\(^6\) *Id.* at 463 (citing 18 U.S.C. § 2703(a)).
\(^6\) *Id.* at 462-63 (citing 18 U.S.C. § 2518 and JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE, § 4.10 at 4-126 - 4-127 (1994)).
\(^6\) *Smith*, 155 F.3d at 1053-54. Smith was later indicted and found guilty on eleven counts of insider trading in violation of section 10(b) of the Securities Exchange Act of 1934 and SEC Rule 10b-5. *Id.* at 1054.
\(^6\) *Id.*
\(^6\) *Id.* at 1055.
\(^6\) *Id.*
arguing that the district court erred in concluding that the Wiretap Act governs the case.67 The Government contended that rather than applying the Wiretap Act, the district court should have applied the SCA.68

Thus, the question the Ninth Circuit faced was whether the Wiretap Act or the SCA controls when a voicemail message on a telephone is forwarded to another voice mailbox and eventually taped. In other words, the court had to determine the precise nature of the intersection between the Wiretap Act and the SCA.69 While the court of appeals had no doubt that the voicemail message was a "wire communication" as defined in both the Wiretap Act and the SCA,70 and that the message was in "storage" within the voicemail system,71 the court struggled with the task of determining which statute applied. Particularly perplexing for the court was how Congress seemed to have made the issue regarding voicemail messages subject to both statutes when the statutes appear, on their faces, to be mutually exclusive.72

The Government attempted to alleviate the textual tension in the court by promoting the Turk case, one which narrowly construed the word "intercept" to connote contemporaneity. The Ninth Circuit, however, refused to adopt the Turk reading of.

67 Id.
68 Id. The Government sought out the application of the SCA rather than the Wiretap Act, because unlike the Wiretap Act, the SCA expressly rules out suppression of evidence as a remedy. Id. at 1056; see 18 U.S.C. § 2708 (1993) (stating specifically that section 2707's civil cause of action and section 2701(b)'s criminal penalties "are the only judicial remedies and sanctions for violations of the Stored Communications Act").
69 Smith, 155 F.3d at 1056.
70 See supra note 33. The SCA obtains its definitions from the Wiretap Act.
71 Smith, 155 F.3d at 1056.
72 Id. The court of appeals noted that the legislative history was of no help whatsoever. Id. at 1056 n.9. While the addition of the phrase "and such term[s] include any electronic storage of such communication" to the definition of wire communication in section 2510(1) and the Senate Report, which observes that "wire communications in storage like voice mail, remain wire communications, and are protected accordingly[,]" suggest that the Wiretap Act controls, the House Report suggests a different conclusion. Id. (quoting S. REP. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3566). The House Report provides:
An "electronic mail" service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, would be subject to Section 2701. A "voice mail" service operates in much the same way. . . . It would likewise be subject to Section 2701."
Id. (quoting H.R. REP. No. 99-647, at 63 (1986)).
"intercept."\textsuperscript{73} The court refused to follow the Government's proposition\textsuperscript{74} for numerous reasons. First, the court stated that it did not have the ability to look beyond the statutorily created definition of "intercept" when, as in this case, the meaning of the word is clearly explained in the statute.\textsuperscript{75} Second, and more importantly, the court concluded that the Turk interpretation of "intercept" was no longer persuasive because when Turk was decided, the statutory definition of "wire communication" did not yet include stored information, and the SCA had not yet been created.\textsuperscript{76} Finally, the court refused to adopt the contemporaneous requirement when construing the word "intercept" because it would render part of the definition of "wire communication" meaningless.\textsuperscript{77} The part of the definition of "wire communication" referring to the inclusion of stored information would be rendered meaningless because "messages in electronic storage cannot, by definition, be acquired contemporaneously."\textsuperscript{78} Thus, the court concluded that adopting the contemporaneous requirement when construing the word intercept is not viable.

\textsuperscript{73} Smith, 155 F.3d at 1056-58. The court noted that the "only cases involving wire communications that have adopted the narrow definition of "interception" have done so with little analysis." \textit{Id.} at 1057 n.11.

\textsuperscript{74} The court thought that the Government's position would establish a "fairly distinct division of regulatory labor, with the Wiretap Act governing the retrieval of wire communications \textit{while in progress} and the Stored Communications Act governing the retrieval of wire communications \textit{while in storage}." \textit{Id.} at 1056-57. For similar treatment of the two acts, see Thomas R. Greenberg, Comment, \textit{E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute}, 44 Am. U.L. Rev. 219 (1994).

\textsuperscript{75} Smith, 155 F.3d at 1057 (citing Colautti v. Franklin, 439 U.S. 379, 393 (1979) ("As a rule, a definition which declares what a term means . . . excludes any meaning that is not stated.") (other citations omitted), and Perrin v. United States, 444 U.S. 37, 42 (1979) ("A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning.") (emphasis added)).

\textsuperscript{76} Id. at 1057 n.11. The court could not square the changes in the Wiretap Act with the narrow reading of intercept because messages in storage cannot be acquired contemporaneously. The court thus concluded that the Turk definition of intercept, "at least in the context of wire communications," had been statutorily overruled. \textit{Id.}

\textsuperscript{77} Id. at 1058. The court reasoned that such an interpretation "flies in the face of the cardinal rule of statutory interpretation that no provision [of a statute] should be construed to be entirely redundant." \textit{Id.} (quoting Kungys v. United States, 485 U.S. 759, 778 (1998), and Colautti, 439 U.S. at 392 ("[I]t is an] elementary canon of statutory construction that a statute should be interpreted so as not to render one part inoperative.")

\textsuperscript{78} \textit{Id.}
Rather than adopt the definition of intercept that necessarily entails contemporaneity, the Ninth Circuit postulated a theory in which unlawful "access" is a lesser-included offense of unlawful "interception" that turns on the degree of intrusion. The court explained the lesser-included offense theory as follows:

[T]he word "intercept" entails actually acquiring the contents of a communication, whereas the word "access" merely involves being in a position to acquire the contents of a communication. In other words, "access[ ]" is for all intents and purposes, a lesser included offense (or tort as the case may be) of "interception." 79

The court found support for its "more holistically sound approach" in both textual and structural considerations. 80 First, the court found its construction to comport with the statutory definitions of "intercept"81 and "access."82 Intercept, which entails acquisition, is distinct from access, which is not statutorily defined, but commonly means "to gain access to."83 The court cited further support in the ECPA by distinguishing the broad language of the SCA, which refers to accessing a stored communications facility, from the language of the Wiretap Act, which refers to intercepting the wire communication.84 Finally, the court of appeals points to the contrasting penalty schemes that are triggered when the ECPA is violated as support for its lesser-included offense theory.85 The court of appeals explained the significance of the contrasting penalty scheme as follows:

The fact that criminal violations of the Wiretap Act are punished more severely than those of the Stored Communications Act reflects Congress’s considered judgment regarding the relative culpability that attaches to violations of those provisions and supports our conclusion that a violation of the latter is, conceptually, a "lesser included offense" of the former.86

79 Id.
80 Id. at 1058-59.
81 The word "intercept" is defined as follows: "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." 18 U.S.C. § 2510(4) (1986).
82 Smith, 155 F.3d at 1059 (quoting WEBSTER'S NINTH COLLEGIATE DICTIONARY 49 (1986)).
83 Id. at 1058.
84 Id. at 1058-59 (comparing 18 U.S.C. § 2701 with § 2515).
85 Id. at 1059. While a person in a position to acquire a wire communication could be criminally prosecuted under section 2701(b), which provides for incarceration for a period up to two years, a person who actually intercepts the wire communication could be criminally prosecuted under section 2511, which provides for incarceration for a period of up to five years. Id.
86 Id.
Pursuant to the court's rejection of the narrow reading of intercept and the adoption of the lesser included offense theory, the court concluded that the SCA did not govern because Gore's act of retrieving and recording Smith's voicemail message constituted an interception under the Wiretap Act.87


Robert Konop, a pilot for Hawaiian Airlines ("Hawaiian"), maintained a password-protected website on which he posted criticisms of his employer and the Air Line Pilots Association (ALPA).88 "Many of those criticisms related to Konop's opposition to labor concessions, which Hawaiian sought from ALPA."89 Although Hawaiian's management was prohibited from viewing the website, the Hawaiian vice president gained access to the website using an employee's login name.90

Konop filed suit in the U.S. District Court for the Central District of California, claiming that the access of his website under false pretenses was an interception of electronic communications that violated both the Wiretap Act and the SCA.91 After the district court granted Hawaiian summary judgment on the claim of violating the Wiretap Act,92 the Ninth Circuit originally reversed and remanded,93 but then withdrew its opinion after

87 Id.

88 Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 872 (9th Cir. 2002).

89 Id.

90 Id. at 873.

91 Id. Although not discussed in this comment, Konop also claimed that Hawaiian: (1) violated the Railway Labor Act ("RLA") by accessing his website, disclosing the website's content to a union leader, and threatening to sue Konop for defamation; and (2) violated the RLA by suspending him in retaliation for his protected labor activities. Id.

92 Id. (granting summary judgment to Hawaiian on all of Konop's claims except for the claim of retaliatory suspension). On the claim of retaliatory suspension, judgment was entered against Konop after a short bench trial. Id.

93 Id. (concluding that Konop had raised a triable issue of fact for all claims that were dismissed on summary judgment). Contrary to the current opinion, the withdrawn opinion was written to reflect that the court was "unpersuaded that Congress intended one definition of 'intercept' to govern 'wire communications' and another to govern 'electronic communications.'" Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1044 (9th Cir. 2001) (opinion withdrawn). The withdrawn opinion declined to follow the Turk contemporaneity requirement, and further concluded that it was irrational to distinguish between communications on the basis of whether a communication is in storage or transmission. Id. at 1043-45 (emphasis added). The withdrawn opinion thus adopted the Smith lesser included offense theory, holding that the "Wiretap Act protects electronic com-
Hawaiian filed a petition for rehearing *en banc*. The Ninth Circuit then affirmed the district court's grant of summary judgment against Konop on his Wiretap Act claims.

The issue for the court of appeals was whether the access to Konop's secure website violated either the Wiretap Act or the SCA. Although the court found that Konop's website falls under the definition of "electronic communication," it did not find that Hawaiian "intercepted" an electronic communication in violation of the Wiretap Act. The *Konop* court failed to find an "interception" by Hawaiian, because it concluded that Hawaiian's acquisition of Konop's website was not contemporaneous with its transmission. The Ninth Circuit's holding was premised upon its conclusion that the pre-ECPA narrow definition of "intercept" was still appropriate with regard to "electronic communications," but overruled with respect to "wire communications."

The Ninth Circuit's very narrow and limiting interpretation of the term "intercept" in the context of electronic communications was *supposedly* based on *Steve Jackson Games*, Smith, and the subsequent enactment of the USA Patriot Act. The Ninth Circuit found the omission of the phrase "any electronic storage of such communication" from the definition of "electronic communications from interception when stored to the same extent as when in transit." *Id.* at 1044, 1046.

The petition for rehearing *en banc* was ordered moot. *Id.*

The court also affirmed the judgment of the district court with respect to Konop's retaliation claim under the RLA, but reversed "the district court's judgment with respect to Konop's claims under the [SCA] and his remaining claims under the [RLA]." *Id.*

The amendment to the USA Patriot Act and the opinion of *Steve Jackson Games* could be construed as adopting the narrow reading of intercept within the context of electronic communications, but *never stating* that it has been statutorily overruled with respect to wire communications only (emphasis added).

See infra note 107.
munication" critical because the same phrase was included in the definition of "wire communication." Following Steve Jackson Games, the court reasoned that Congress excluded the phrase from the definition of "electronic communication" because "Congress did not intend for 'intercept' to apply to electronic communications when those communications are in electronic storage." The court of appeals further explained that "Congress' inclusion of storage in the definition of "wire communication" militated in favor of a broad definition of the term intercept with respect to wire communications..." The court of appeals thus relied on the familiar textual dichotomy recognized in Steve Jackson Games. This court, however, used the textual distinction in a different manner. It relied on the distinction between wire and electronic communications to maintain that Congress only intended for the narrow reading of "intercept" to apply to electronic communications.

The Court of Appeals for the Ninth Circuit further supported judicial maintenance of a narrow intercept requirement for electronic communications by citing a subsequent legislative change to the Wiretap Act, which was enacted in the USA Patriot Act of 2001. When Congress amended the Wiretap Act through the USA Patriot Act, it eliminated the phrase "inclusion of storage" from the definition of "wire communication."

The Ninth Circuit concluded that this Congressional action termi-

---

103 See supra note 31.
104 See supra note 32.
105 Konop, 302 F.3d at 877 (citing Steve Jackson Games, 36 F.3d at 461-62, and Wesley Coll. v. Pitts, 974 F. Supp. 375, 386 (D. Del. 1997), aff'd, 172 F.3d 861 (3d Cir. 1998)). But see Steve Jackson Games, 36 F.3d at 462 (basing its conclusion on finding the narrow reading of "intercept" to apply to wire communications).
106 Konop, 302 F.3d at 877.
107 Id. at 878 (stating that the elimination of the term storage from the definition of wire communication in the Wiretap Act supports the analysis of Steve Jackson Games and Smith).
109 18 U.S.C. § 2510(1) (2001). Under the USA Patriot Act, "wire communication" is defined as:

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.

Id.
nated the textual distinction between the two statutes and statutorily "re-instated the pre-ECPA definition of intercept – acquisition contemporaneous with transmission – with respect to wire communications."\textsuperscript{110} The court further argued that Congress was aware of the judicial definition of "intercept" applied to electronic communications, and thus accepted the notion of contemporaneity when it chose not to modify the definition of "electronic communications" in the USA Patriot Act.\textsuperscript{111}


One of the issues before the court was whether the Wiretap Act, the SCA, or neither act controlled when Nationwide Insurance retrieved an employee’s e-mail communications from its electronic storage site.\textsuperscript{112} The United States District Court for the Eastern District of Pennsylvania held that a company’s retrieval of an agent’s e-mail from post-transmission storage implicated neither the Wiretap Act nor the SCA.\textsuperscript{113} The court’s holding was based on the conclusion that each act only protects communication in the course of transmission.\textsuperscript{114}

Acknowledging the importance of understanding how e-mail communications work, the district court explained the transmission of an e-mail by describing a system utilizing intermediate storage,\textsuperscript{115} backup protection storage,\textsuperscript{116} and post-transmission storage.\textsuperscript{117} The critical point in the transmission of an e-mail communication, the court reasoned, was the point in time the message is acquired. It is at this point when the transmission is completed.\textsuperscript{118} Following Turk’s narrow reading of the term “in-

\textsuperscript{110} Konop, 302 F.3d at 878. Of course, this reasoning assumes that the pre-ECPA definition of intercept already applied to electronic communications. \textit{Id.} (assuming that courts were still using the pre-ECPA definition of intercept with regard to electronic communications). \textit{But see supra} note 107.

\textsuperscript{111} Id. at 637.


\textsuperscript{113} \textit{Id.} at 637.

\textsuperscript{114} \textit{Id.} (citations omitted).

\textsuperscript{115} The court defines intermediate storage as a temporary location for the message to reside after the message is sent and before the message is retrieved. \textit{Id.} at 633.

\textsuperscript{116} The court defines backup protection storage as a protective storage process to be utilized in the event that the system crashes before the recipient retrieves the message from intermediate storage. \textit{Id.} at 633-34.

\textsuperscript{117} The court defines post-transmission storage as a location for storage of the message after it has been retrieved. \textit{Id.} at 634.

\textsuperscript{118} \textit{Id.}
tercept," which necessarily entails contemporaneity, the district court concluded that the Wiretap Act only protects communications during the course of transmission. When the communications are retrieved, the transmission is over.\(^{119}\) Because Nationwide acquired the e-mail from post transmission storage, a point in time where the email had already been retrieved and transmission was complete, there was no interception.\(^{120}\)

The district court's failure to find an unlawful access pursuant to the SCA was based upon the court's understanding of how e-mail transmission works and the court's adoption of the narrow reading of "intercept."\(^{121}\) The court focused on squaring the definition of electronic storage\(^{122}\) with its description of e-mail transmission.\(^{123}\) Following the definition, the court concluded that the SCA protects the transmission of messages that have either been in intermediate storage pursuant to part (A) of the definition, or in backup protection storage pursuant to part (B) of the definition.\(^{124}\) The court singles out the phrase "for purposes of backup protection of such communication" in part (B) of the definition as evidence that messages in post-transmission storage, after the transmission is complete, are not communications covered under the statutory definition of electronic storage.\(^{125}\) Because Nationwide acquired the e-mail from post-transmission storage, when the e-mail message was no longer in the course of transmission, the court ruled that the retrieval of the e-mail did not violate the SCA.\(^{126}\)

\(^{119}\) Id.
\(^{120}\) Id. at 635.
\(^{121}\) Id. at 635-36.
\(^{122}\) Electronic storage is defined under the ECPA as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (1993) (emphasis added).
\(^{123}\) Fraser, 135 F. Supp. 2d at 635-36.
\(^{124}\) Id.
\(^{125}\) Id. at 636.
\(^{126}\) Id. The Ninth Circuit recently criticized Fraser in Theofel v. Farey-Jones, rejecting the exclusion of post-transmission storage from the definition of backup protection. Theofel v. Farey-Jones, Nos. 02-15742, 03-15301, 2003 WL 22020268, at *4-5 (9th Cir. Aug. 28, 2003). The court in Theofel argued that if backup protection did not include any form of post-transmission storage and only included communications still pending delivery, as suggested by Fraser, subsection B of 18 U.S.C. § 2510(17) would be rendered meaningless. Id. at *5. Backup protection excluding post-transmission storage would render subsection B superfluous, the court argued, because it "would already seem to qualify as 'temporary, intermediate storage' within the meaning of subsection (A)." Id. The author rejects this

An anonymous computer hacker e-mailed information to police concerning files he found on Steiger’s computer, which revealed Steiger’s sexual exploitation of children and possession of child pornography. The threshold issue for the court was whether an anonymous source that penetrated Steiger’s computer with a “Trojan Horse” virus and downloaded files from the computer “intercepted” any electronic communications in violation of the Federal Wiretap Act. The Court of Appeals for the Eleventh Circuit held that: (1) a contemporaneous interception was required to violate the Wiretap Act with respect to electronic communications, and (2) “the anonymous source did not intercept electronic communications in violation of the Wiretap Act.” Although the court concluded that the information retrieved from Steiger’s computer falls within the statutory definition of “electronic communication,” the court failed to find an interception of the electronic communication because it did not view the anonymous source’s actions as a contemporaneous acquisition. It was critical to the court that the information downloaded from Steiger’s computer had been stored on his computer.

The court’s analysis states that it agrees with the interpretations of the Wiretap Act found in Konop and Steve Jackson Games. The court further stated, however, that it does not rely on them. While the court apparently does not rely on either case when assessing the applicability of the SCA, it seems to rely on the cases when assessing whether the Wiretap Act was violated.

argument. Backup protection excluding post-transmission storage under subsection (B) is not equivalent to temporary, intermediate storage in subsection (A) because subsection (B) includes the additional limitation of pertaining to storage provided by an electronic communication service. 18 U.S.C. § 2510(17) (1993). Theofel fails to recognize this distinction. United States v. Steiger, 318 F.3d 1039, 1046 (11th Cir. 2003).

127 The Trojan Horse virus was used by the anonymous source to enable him to view and download files from Steiger’s computer. Steiger, 318 F.3d at 1044.

128 Id. at 1046. The district court declined to address the threshold issue. Id.

129 Id. at 1046-49.

130 See supra note 32.

131 See id. at 1050.

132 Id.

133 Id. Even though the applicability of the SCA was not a direct issue, the court of appeals considered the question and concluded that the SCA would not govern the hacking activities of the anonymous source. Id. The court came to
In particular, the court of appeals seems to follow Konop when it decided to apply one definition of “intercept” to govern wire communications, and another to govern electronic communications.135

C. USA PATRIOT ACT OF 2001

Enacted October 26, 2001, the USA Patriot Act has played an important role in the history of the ECPA because it repealed the express inclusion of stored wire communications from the definition of wire communication.136 This change was significant because the opinions of Steve Jackson Games, Konop, and Steiger previously rested on this textual distinction to hold that the definition of “intercept,” in the context of electronic communications, requires contemporaneity.137 Furthermore, the Konop and Steiger opinions have interpreted this Congressional amendment to signal that Congress wanted to re-instate the pre-ECPA definition of “intercept” – acquisition contemporaneous with transmission – with respect to wire communications.138 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 given the term with respect to the unchanged definition of “electronic communications.”139

III. IMPLICATIONS OF THE DIFFERENT JUDICIAL CONSTRUCTIONS OF THE ECPA

In the opinion of the author, the inability of courts and legal scholars to “square” the two statutes primarily stems from poor Congressional drafting of the ECPA.140 Rather than following a consistent model, Congress instead opted to define some statutory terms in great detail and others in almost no detail.141 Although this criticism is being constructed in hindsight, it seems fair because the Congressional shortcomings are of such a tone that one would suspect them to emanate from incompetence rather than mistake.142 Compare 18 U.S.C. § 2510(1) (explaining “wire communication” as including stored information) with 18 U.S.C. § 2510(12) (explaining “electronic com-

135 See id. at 1048-49.
137 Konop, 302 F.3d at 877; Steve Jackson Games, 36 F.3d at 461-62; Steiger, 318 F.3d at 1048.
138 Konop, 302 F.3d at 878; Steiger, 318 F.3d at 1048-49.
139 Konop, 302 F.3d at 878; Steiger, 318 F.3d at 1048-49.
140 Although this criticism is being constructed in hindsight, it seems fair because the Congressional shortcomings are of such a tone that one would suspect them to emanate from incompetence rather than mistake.
141 Compare 18 U.S.C. § 2510(1) (explaining “wire communication” as including stored information) with 18 U.S.C. § 2510(12) (explaining “electronic com-
though silence is consistent with the presumption that Congress acts with awareness of prevailing judicial constructions when it reenacts or amends a law, the existing judicial constructions were anything but prevailing or widely accepted.

Despite Congress’ inability to pass a clear statute, judges should also be admonished for failing to properly adjudicate these matters. While judges have done an exceptional job analyzing both the language of the ECPA and its legislative history, one cannot expect to produce an acceptable product when the tools used to complete the job are defective. Instead of focusing entirely on legislative history and statutory language that is ambiguous, judges would likely rectify their problems if they construed the ECPA in light of modern communications technology. Even if one supposes that the language of the ECPA and its legislative history were models of clear Congressional construction, it would be foolish not to look to communications technology for guidance in statutory interpretation.

Understanding the concepts that enable modern day communication to occur in an electronic medium is crucial to understanding how the ECPA should be construed because it was the rapid development of communications technology that motivated the enactment of the ECPA. Without understanding what motivated Congress to take action and enact the ECPA, i.e., the cause of the legislation, there can be no hope for fair judicial administration of the ECPA. It is equivalent to allowing a referee with a rulebook to officiate a game, even though the referee has no concept of how the sport is actually played. Whether it is a lack of appreciation or a case of apathy, the end result is the same when judges fail to truly understand communications technology. They produce ad-hoc decisions, which in turn fail to provide guidance to other courts.

---


143 When courts have debated whether Congress intended for the Turk contemporaneity rule to apply to both the Wiretap Act and the SCA of the ECPA, few judges have adopted Turk’s rather narrow reading of “intercept.” See Konop, 236 F.3d at 1044 (stating that it knew of only one apparent adoption of Turk’s reading by a circuit court – a case that pre-dated the passage of the ECPA), withdrawn, 302 F.3d 868 (9th Cir. 2002); Smith, 155 F.3d at 1057 n.11 (noting that the select few cases involving wire communications that adopted a narrow definition of intercept did so with little analysis).
The following sections of this comment analyze the implications of the various judicial constructions of the ECPA.

A. **Steve Jackson Games: Adopting a Narrow Reading of Intercept for the Wiretap Act**

When the Fifth Circuit found no violation of the Wiretap Act, the decision largely depended on: (1) classifying the e-mail messages as stored electronic communications, and (2) recognizing that the definition of electronic communication, unlike the definition of wire communication, does not include electronic storage of such communication.\(^{144}\) The court of appeals stated that the omission of "electronic storage" from the definition of electronic communication "reflects that Congress did not intend for [a narrow reading of] intercept to apply to electronic communications when those communications are in electronic storage."\(^{145}\)

Although this case concerns electronic communications in storage, it can likely be distinguished as a very narrow holding. The case is distinguishable because the acquisition of the e-mail communications in storage were the result of a physical seizure, rather than a seizure through an electronic medium. Nonetheless, the errors in this opinion should be discussed because *Konop* and *Steiger* rely heavily on this opinion.

To begin with, when the court concluded that the narrow reading of intercept does not apply to electronic communications in storage, it had already concluded that the proper reading of intercept in the context of the Wiretap Act entailed contemporaneous acquisition. The latter conclusion, which is based in part upon a statement from a Senate Report providing that "the definition of intercept under current law is retained with respect to wire and oral communications[,]"\(^{146}\) is likely wrong. The faulty conclusion assumes that the definition of intercept under "current law" included a contemporaneity requirement. Contrary to what the majority asserts, the "current law" concerning the definition of intercept did not clearly adopt the contemporaneity requirement. The extent to which the "current law" promoted *Turk* was limited to a single case that adopted the contemporaneity requirement before the ECPA was

---

144 Steve Jackson Games, 36 F.3d at 461.
145 Id. at 461-62.
146 Id. at 462.
enacted. Furthermore, if intercept were defined as solely contemporaneous acquisition, judges and scholars have suggested that almost all acquisitions of electronic communications would fall outside of the umbrella of statutory protection provided by the Wiretap Act. A 1996 amendment to the ECPA, which provided that an “electronic communication . . . does not include . . . electronic funds transfer information stored by a financial institution . . . [.,]” indicates the opposite of what the majority opinion suggests. The decision to exclude certain kinds of stored information from the definition of electronic communications indicates that Congress understood the definition of electronic communication to include stored information.

Finally, the Fifth Circuit’s reasoning is likely flawed because it fails to consider the difference between “access,” as used in the SCA and “intercept,” as used in the Wiretap Act. Whereas intercept is statutorily defined as the actual acquisition of the contents of a communication, access, which is not statutorily defined, is commonly defined to mean “getting near or into contact with . . . and to gain access to . . . ” The difference in the terms indicates that Congress did not intend “access to a communication” to equate with “acquisition to a communication.” Rather, Congress likely intended the Wiretap Act to only

147 Konop, 302 F.3d at 1044 n.2.
148 Id. at 888 (Reinhardt, J., dissenting) (quoting Jarrod J. White, Commentary, E-Mail@Work.Com: Employer Monitoring of Employee E-Mail, 48 Ala. L. Rev. 1079, 1083 (1997) (“Following the Fifth Circuit’s rationale, [and excluding stored electronic communications from the intercept prohibition,] there is only a narrow window during which an E-mail interception may occur – the seconds or milliseconds before which a newly composed message is saved to any temporary location following a send command. Therefore, . . . [assuming that stored communications are excluded from the intercept prohibition,] interception of E-mail within the prohibition of the ECPA is virtually impossible.”)).
149 Steve Jackson Games, 36 F.3d at 461-62.
151 See id. § 2510(4).
152 Konop, 302 F.3d at 889 (Reinhardt, J., dissenting) (quoting the definition of access in the Oxford English Dictionary); see also Smith, 155 F.3d at 1058-59.
prohibit the actual acquisition of a communication, while the SCA would prohibit access to the communication. As pointed out by the dissent in *Konop*, the Fifth Circuit "erroneously conflates the terms, reading them both to refer to the acquisition of the contents of a communication."\(^{153}\)

B. **Smith: Repudiation of the Contemporaneity Requirement and Promotion of the Lesser Included Offense Theory**

When the Ninth Circuit found a violation of the Wiretap Act, the decision largely depended on: (1) the court's rejection of the narrow reading of intercept, and (2) the promotion and adoption of the lesser included offense theory. Although the holding of this case is restricted to issues concerning wire communications in storage, it is likely still persuasive for businesses or individuals concerned with the protection of stored electronic communications because stored wire communications are technologically equivalent, in some instances, to stored electronic communications.

The Ninth Circuit's repudiation of the contemporaneity requirement that had previously been read into the term "intercept" is not being questioned here. The reasoning utilized by the court, however, is being brought into question. Rather than recognizing that Congress possibly never intended for *Turk* to be interpreted as the "current law,"\(^{154}\) the Ninth Circuit relied on the inclusion of storage within the definition of wire communication to repudiate the contemporaneity requirement.\(^{155}\) The court reasoned that if the *Turk* contemporaneity requirement governed, the part of the definition of "wire communication" referring to the inclusion of stored information would be rendered "meaningless because messages in electronic storage cannot, by definition, be acquired contemporaneously."\(^{156}\) While this argument is logically sound, there is concern as to whether it wilts under the USA Patriot Act's recent amendment, which eliminated the inclusion of storage in the definition of wire communication.\(^{157}\)

\(^{153}\) *Konop*, 302 F.3d at 891-92 (Reinhardt, J., dissenting) (citing *Steve Jackson Games*, 36 F.3d at 463).

\(^{154}\) *Supra* note 143 and accompanying text.

\(^{155}\) *Smith*, 155 F.3d at 1057-58.

\(^{156}\) *Id.* at 1058.

\(^{157}\) See *supra* notes 107-10 and accompanying text.
There is also a judicial disagreement as to whether Smith repudiated the contemporaneity requirement in whole, or only with regard to wire communications. The opinion provides that "to the extent that Turk stands for a definition of "intercept" that necessarily entails contemporaneity, it has, at least in the context of wire communications, been statutorily overruled." 158 Contrary to the Konop and Steiger opinions, which read Smith as stating that it only repudiates contemporaneity with regard to wire communications, 159 Smith never stated that it only repudiated the contemporaneity requirement for wire communications. The "at least" language of Smith suggests a minimal amount of action or a floor, and thus supports the opposite of what Konop and Steiger conclude. It suggests that the contemporaneity requirement is also likely repudiated for electronic communications.

This argument is further supported by other arguments made by the Ninth Circuit in Smith. Namely, the court argues that contemporaneity does not govern wire communications because it would not be viable to divide the statutory provisions between those concerning in-progress wire communications and those concerning in-storage wire communications. 160 Surely, the court would not support a narrow reading of the term "intercept" for electronic communications because that would only promote a similar statutory division between in-progress electronic communications and in-storage electronic communications. Why would the court accept this statutory division when they concluded that the exact same statutory division was not viable with regard to wire communications?

The Ninth Circuit's promotion and adoption of a lesser-included offense theory 161 is one of the few bright stars in the ECPA's judicial pool of mud. A concept whereby "access" is a lesser included offense of the "acquisition" of a communication not only addresses the problems that originally motivated Congress to pass the ECPA, but it also enables the Wiretap Act and the SCA to co-exist without any provisions becoming superfluous. The concept of a lesser included offense addresses the concerns of Congress because it accounts for the computer hacker who often does a great deal of damage to stored communica-

158 Smith, 155 F.3d at 1057 n.11 (original quotations omitted and secondary emphasis added).
159 Konop, 302 F.3d at 877; Steiger, 318 F.3d at 1048-49.
160 Smith, 155 F.3d at 1058.
161 Supra notes 85-86 and accompanying text.
tions facilities without ever acquiring the contents of those communications.162 Were Congress to prohibit only actual acquisition of the contents of communications in storage, law enforcement personnel would be powerless to do anything to individuals such as hackers, who are likely to do damage without ever acquiring communications.

These arguments also explain how the lesser-included offense theory allows the two statutes to co-exist without creating redundant provisions. Quite simply, it promotes a distinction between the terms “access” and “intercept,” and such a distinction supports the structure of the statutes. The interpretation supports the SCA’s ability to enforce lenient penalties against those who only put themselves in the position to acquire a communication, while allowing the Wiretap Act to enforce harsher penalties against those who go further and acquire the communication.163

C. THE KONOP AND STEIGER OPINIONS: TWO DEFINITIONS FOR INTERCEPT AND THE EFFECT OF THE USA PATRIOT ACT

The Konop and Steiger opinions, which base their decisions in part on the Steve Jackson Games and Smith opinions,164 are flawed. Both courts’ assessments of whether the Wiretap Act governed adopt a multi-definitional reading of the term intercept, such that one definition is used to govern wire communications and another is used to govern electronic communications. More specifically, the courts attach a contemporaneous requirement to intercept when a potential illegal interception of an electronic communication arises, but do not attach such a requirement to intercept when a potential illegal interception of a wire communication arises.165 Clearly, the only thing that these two courts have accomplished is a twisted reading of the ECPA. Somehow, the Ninth and Eleventh Circuits have come to the rather unpersuasive conclusion that Congress intended different definitions of the same word to govern different forms of

162 See Smith, 155 F.3d at 1059.
163 Id.
164 Although the court in Steiger states that it agrees but does not rely on the Fifth and Ninth Circuits’ previous interpretations of the Wiretap Act, it is evident that it does rely on the previous cases as precedent when forming its decision with regard to the applicability of the Wiretap Act. See supra notes 133-35 and accompanying text. The Steiger court somehow feels that the manner in which it denies protection from the SCA completely distinguishes itself from Konop. See Steiger, 318 F.3d at 1048-49.
165 Konop, 302 F.3d at 877-78; Steiger, 318 F.3d at 1048-49.
communication. As a result of this highly questionable conclusion, neither court found that the Wiretap Act was implicated. If this common reasoning stands for other courts to follow as precedent, fragile businesses such as airlines, which have become increasingly dependent upon the Internet to satisfy business goals, will risk economic catastrophe.

Not only are the Konop and Steiger opinions unpersuasive, but they are clearly flawed. The court in Konop, with which Steiger agrees, claims to garner its support from Steve Jackson Games when it focuses on the difference between the wire and electronic communication definitions that existed before the enactment of the USA Patriot Act. While Konop is correct in pointing out that Steve Jackson Games also recognized the difference between the statutory definitions, Steve Jackson Games did not rely on the difference between the statutory definitions to adopt two different definitions for intercept. Steve Jackson Games does stand for a definition of “intercept” that entails contemporaneity, but it does not stand for two different definitions of “intercept” to govern wire and electronic communications. It stands for only one governing definition. Does Konop propose to adopt the reasoning of Steve Jackson Games to further its conclusion of a contemporaneity requirement for electronic communications and then spurn the part of the opinion that fails to further its conclusions concerning wire communications?

The conclusions in Konop and Steiger concerning the multi-definitional form of intercept are also flawed to the extent that they rely on Smith to support the argument that a contemporaneity requirement has only been repudiated with regard to wire communications. As discussed earlier, Smith never stated that it only repudiated the contemporaneity requirement for wire communications. Instead, Smith suggests that the contemporaneity requirement is also likely repudiated for electronic communications.

\*\*\*\*\*

166 Konop, 302 F.3d at 877 (“[r]elying on the same textual distinction as the Fifth Circuit in Steve Jackson Games . . .”).
167 Steve Jackson Games, 36 F.3d at 461.
168 See id. at 462.
169 See id. at 461-62.
170 See id. at 462.
171 Smith, 155 F.3d at 1057 n.11.
172 Id.
To the degree that both Konop and Steiger claim that their reasoning is supported by the USA Patriot Act's recent amendment to the ECPA, this claim is both unwarranted and flawed. This argument should never have been an influence on either of the decisions because "the views of a subsequent Congress form a hazardous basis for inferring the intent of an earlier one."\(^\text{173}\) Furthermore, the argument that the amendment re-instated the pre-ECPA definition of intercept – acquisition contemporaneous with transmission – with respect to wire communications is flawed because it rests on the belief 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. 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,\(^\text{174}\) how could Congress have possibly become aware of a common judicial definition for intercept with regard to any form of communication? More importantly, how could such a common judicial definition exist?

D. **Steiger: Does the Stored Communications Act Protect Businesses from Computer Hackers?**

Although Steiger is troubling because the court found no violation of the Wiretap Act when a hacker used a "Trojan Horse" virus to access and download files from another computer connected to the Internet, it is even more troubling because it also failed to find a breach of the SCA. The court failed to classify the hacker's presence in the computer as an unauthorized access pursuant to the SCA because it did not believe that the computer whose security was breached was maintained as an "electronic communication service."\(^\text{175}\)

This is clearly an example of a decision that is erroneous because the court did not understand the technology at issue. Generally speaking, the Internet is composed of servers and cli-

\(^{173}\) Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc., 447 U.S. 109, 117 (1980) (quoted in Konop, 302 F.3d at 891 n.2 (Reinhardt, J., dissenting) (other citations omitted)).

\(^{174}\) Supra note 17 and accompanying text.

\(^{175}\) An "electronic communication service" is defined as: "any service which provides to users thereof the ability to send or receive wire or electronic communications[.]" 18 U.S.C. § 2510(15) (1993).
Computers that provide service to other machines are servers and machines that are used to connect to servers are clients. It is immaterial whether a person intends for his or her computer to be a client or a server. If a hacker is able to gain access into a computer on-line, the hacker becomes a user of that computer and the computer becomes a server for the hacker. Thus, the on-line computer that has been penetrated gives the hacker the ability to send out information from that computer at anytime. In other words, the computer that has been penetrated provides a service which in turn provides users thereof [i.e., a hacker] the ability to send or receive electronic communications. Contrary to the majority's opinion, the facts of Steiger fit the definition of “electronic communication service” like a glove.

E. Fraser: Adopting a Narrow Reading of Intercept for Both Statutes

When the Eastern District of Pennsylvania determined that there was neither a violation of the Wiretap Act nor the SCA, it based its decision on (1) the adoption of a narrow reading of “intercept” that necessarily entails contemporaneity for both the Wiretap Act and the SCA, and (2) the adoption of the lesser-included offense theory. Although this comment has previously suggested that the courts may be wrong for reading the term intercept to require acquisition contemporaneous with transmission, this court utilizes a novel approach.

Rather than adopting the narrow reading of intercept to apply to only one form of communication or all forms of communication protected by the Wiretap Act, Fraser interprets the narrow reading of intercept to apply to all communications independent of which statute governs. In other words, the court foregoes any quantitative analysis and looks at all communications temporally. From this perspective, the determining factor

---

177 Id.
178 While the integrity of the Steiger court is not questioned, there is concern whether the judges presiding over this case had ulterior motives in mind. When a case such as Steiger arises, in which the defendant is accused of sexual exploitation of children and possession of child pornography, it would be understanda ble, but not acceptable, if a court lost track of its unbiased duty and became overrun with emotion.
179 See supra notes 149-50 and accompanying text.
for whether interception has occurred is the point in time when
the message is acquired.\textsuperscript{180} If the communication is acquired
before the communication is received, i.e., when the transmis-
sion ends, an unlawful interception has occurred. The court
thus held that both the Wiretap Act and SCA provide protection
for communication only while a communication is in the course
of transmission.\textsuperscript{181}

This court also excelled where other courts have failed. In-
stead of merely brushing over the concepts of the underlying
technology buried within the issues, the court squared its legal
conclusion with the underlying technology.\textsuperscript{182} The court ac-
complished this when it recognized that an electronic communi-
cation such as e-mail is still in transmission when it resides in
intermediate storage or a form of back-up protection storage.\textsuperscript{183}

Although the court distinguished the withdrawn opinion
from \textit{Konop} because it was factually dissimilar, the court later
states that the withdrawn opinion from \textit{Konop} should be control-
ling.\textsuperscript{184} Despite the additional language supporting the with-
drawn \textit{Konop} opinion, it is unlikely that \textit{Fraser} can be construed
as supporting the lesser-included offense theory. The court
does not expressly state whether it agrees with such an analysis,
and it does not apply what the lesser-included offense theory
provides – a distinction between “intercept” and “access.”
Rather than addressing the applicability of the SCA by question-
ing whether there was unauthorized access, the court simply
concluded that the statute did not govern because the message
was retrieved from post-transmission storage.\textsuperscript{185}

\section*{IV. PROPOSAL FOR A NEW INTERPRETATION
OF THE ECPA}

In light of the USA Patriot Act’s recent amendment to the
ECPA and the apparent split between the Fifth, Ninth, and Elev-
enth Circuits, this comment has been written as a guide for
those who face the task of construing and/or administering the
Wiretap Act and the SCA. Thus, this comment proposes a new
interpretation of the ECPA. It proposes an interpretation that

\textsuperscript{180} \textit{Fraser}, 135 F. Supp. 2d at 634.
\textsuperscript{181} \textit{Id.} at 635, 637.
\textsuperscript{182} \textit{Id.} at 633-34.
\textsuperscript{183} \textit{Id.} at 634.
\textsuperscript{184} \textit{Id.} at 636 (“In arguing that it should be controlling, \textit{Fraser} was seduced by
the . . . Ninth Circuit [withdrawn] opinion in \textit{Konop}.”).
\textsuperscript{185} \textit{Id.}
(1) addresses the issues Congress faced when it enacted the ECPA, (2) follows the plain language of the statutes, (3) provides technological flexibility, and (4) affords privacy and protection to both the public and business sectors. It proposes an interpretation that combines the lesser-included offense theory from *Smith* with the transmission/storage dichotomy exposed in *Fraser*.

A. A Contemporaneous Acquisition/Access Reading, Independent of Which Statute Governs, Permits a Reading of the Wiretap Act and the Stored Communications Act that Is Consistent with Congressional Intent, Follows the Plain Language of the Statutes, Provides Technological Flexibility, and Affords Privacy and Protection

The interpretation of the ECPA promoted by this comment suggests that when a court is forced to determine whether there is an unauthorized interception pursuant to the Wiretap Act or an unauthorized access pursuant to the SCA, the court should look at the facts from two different angles. More specifically, the court should view the actions of the defendant from both a temporal and a quantitative perspective.

1. At What Point in Time Is the Communication Acquired or Accessed?

   The court should first determine whether the defendant’s actions took place during the transmission of the communication or when the transmission was over and was in post-transmission storage. The temporal analysis is thus the critical question. While it does not solely determine whether a violation of the ECPA occurred, the second part of the test would be moot if a court determined that the communication in question was in post-transmission storage during all phases of the defendant’s alleged activities.

2. Was the Defendant Merely in a Position to Acquire the Communication, or Did He Actually Acquire the Communication?

   Assuming that the court finds questionable activity by the defendant while the communication is still in transmission, the second phase of the test charges a court with determining whether the defendant’s actions constituted an unauthorized
“interception” or “access.” In other words, the court must determine whether the defendant was merely in a position to acquire the communication or whether he actually acquired the communication.

3. **Balancing Congressional Intent with Technology and Protection**

A proposed interpretation of the ECPA that focuses on whether a communication is in storage or transmission, and on whether the communication has been accessed or intercepted balances all the concerns of each party.

a. **Following Congressional Intent**

The proposed interpretation is consistent with congressional intent because it follows the language of the statute and supports the contrasting penalty schemes. Acknowledging the difference between “intercept” and “access” is critical because it promotes the adoption of the “lesser included offense theory.” This theory, which is based on the degree of intrusion, is supported by both textual and structural considerations. First, it comports with the statutory definition of “intercept” and the ordinary meaning of “access.” Second, it supports the contrasting penalty schemes assigned to each act.

The fact that criminal violations of the Wiretap Act are punished more severely than those of the Stored Communications Act reflects Congress’s considered judgment regarding the relative culpability that attaches to violations of those provisions and supports our conclusion that a violation of the latter is, conceptually, a “lesser included offense” of the former.

Third, the separation of “access” from “intercept” explains the absence of an evidentiary exclusion remedy from the SCA. While it would be appropriate to prevent the contents of an illegally intercepted communication from being introduced in court, there would be no need for an exclusion remedy if someone merely accesses, but does not acquire, a communication. Finally, this proposed interpretation does not force any provi-

---

186 Smith, 155 F.3d at 1051-59.
187 Id. at 1059 (comparing 18 U.S.C. § 2707 and § 2701(b) with § 2520 and § 2511, respectively).
188 Id. (original emphasis added).
189 Id.
190 Id.
sion of the statutes to become redundant or superfluous. rather, it allows each provision of each statute to coexist with the other.

b. Adapting to Technology

The proposed interpretation is flexible enough to co-exist with rapidly developing technology because a temporal analysis in the context of the SCA recognizes that temporary storage does not terminate transmission. Fraser recognized this first hand when comparing the steps involved in an e-mail transmission with the statutory definition of "electronic storage." The court's comparison demonstrated that an electronic communication process such as e-mail, which inherently includes intermediate or backup storage, can still be intercepted or acquired contemporaneously. Therefore, the court confirmed that the law could account for technology. If a court can determine when a transmission has been totally completed, or when it has been actually received, the issue of how to delineate between the transmission and storage phase becomes less burdensome.

The picture becomes slightly more complicated when considering an unauthorized access of a website. In determining whether the alleged unauthorized website access occurred before or after the transmission was completed, courts will have to consider the implications of cache. Cache, a temporary storage device, increases the complexity of the analysis once an individual has accessed his or her user account on a website for the first time. At this point in time, the browser on a computer caches or temporarily stores the HTML page into the computer's memory. The next time the user requests access to the same web page, the browser determines whether the date of the file requested on the Internet is newer than the one

191 Id.
192 Id.
193 Fraser, 135 F. Supp. 2d at 636.
194 In the context of the Web, cache is essentially a small temporary memory bank that provides quick retrieval of Web objects such as HTML documents. By storing frequently used web objects in a convenient location, caching creates the distinct advantages of reduced bandwidth consumption, reduced server loads, and reduced latency. See Brian D. Davison, Web Caching Overview, Web-Caching.com at http://www.web-caching.com/welcome.html (last visited Sept. 7, 2003).
If the dates are the same, the computer's browser retrieves the file from cache rather than from the Internet. A court must therefore determine whether cache is being used as temporary storage or post-transmission storage. Such a conclusion is critical when attempting to determine whether the alleged activities of a cyber intruder occurred before or after the electronic communication transmission completed.\textsuperscript{197}

c. Providing Protection

The proposed interpretation affords proper protection to both private and business oriented groups because it supports the contrasting penalty schemes while also providing a protective shield against criminals that may gain access without actually acquiring a communication.\textsuperscript{198} While this proposed interpretation does leave an unprotected hole where a communication has already been received and the transmission is consequently over, it is a very narrow hole that is only completely vulnerable to a physical seizure. If a communication that has been received and stored is accessed by a hacker through an electronic medium, then it could likely still be argued that the SCA governs. For what minor lapses in protection that do surface, courts must recognize that, even in the original Wiretap Act, Congress did not intend to protect all intrusions into an individual's privacy.\textsuperscript{199} Indeed, scholars have noted that the strong expectation of privacy of communications diminishes once a transmission is complete.\textsuperscript{200}

With regard to on-line business ventures and airlines in particular, there is admittedly some concern that the economic compensation afforded an airline under either statute for an instance of cyber intrusion would likely not be sufficient enough to compensate the airline for its full economic loss.\textsuperscript{201} However,

\begin{footnotesize}
\begin{enumerate}
\item Id.
\item Generally speaking, when comparing the date of a cached file with the date of the file on the Internet, the file from the Internet will come first in time if new information has been added to the user's account. If an individual gains access to a user's web account on a website before the user has retrieved the information, the individual would be receiving the information before the intended transmission to the true user was completed. This individual would thus be intercepting the information from the user's account.
\item See Smith, 155 F.3d at 1058-59.
\item See Turk, 526 F.2d at 658-59.
\item See Akamine, supra note 42.
\item Even if both statutes provided for substantial compensation, the typical cyber criminal would be unable to financially meet the requisite civil damages.
\end{enumerate}
\end{footnotesize}
the significance of the judicial interpretations does not concern compensation;\textsuperscript{202} rather, the significance lies in the fact that they do nothing to deter such activities from occurring in the future. Deterrence is the primary and implicit form of protection that an airline or any other business entity seeks when it chooses to hide under a statutory umbrella. Thus, if the judicial ruling in \textit{Konop} had triggered the protection of the Wiretap Act for the unauthorized interception of data on a web site instead of triggering the SCA, the stiffer penal and civil penalties that would apply to the perpetrators would serve as a more forceful deterrent. The current judicial interpretations of the ECPA in the context of unauthorized web access and interception provide little to no deterrence, and thus afford little to no protection to airlines and other business entities with significant financial investments in on-line business ventures.

There is no doubt that legal scholars who disagree with the proposal set forth in this comment will cite a lack of website incapacitation among the airlines as positive and encouraging proof that the current set of statutory regulations and judicial interpretations do indeed deter. Although such an argument seems logical, it is flawed. A theory that allows one to imply that a procedural safeguard is effective just because an unfortunate victim has not suffered an injustice is a theory that smacks of ignorance. While the airline industry in America has not yet encountered any significant on-line criminal activity or unauthorized cyber exposure, the international community of airlines has not been so fortunate. A recent controversy embroiling both the German Parliament and the national flagship air carrier Lufthansa, which is believed to have emanated from an unauthorized access of the carrier's private data, suggests that it is inappropriate for airlines to assume that their on-line data storage systems are impregnable.

This political controversy surfaced in the Bundestag, Germany’s parliament, when German media, including the mass-circulation newspaper Bild, published the names of several politicians who allegedly cashed in bonus miles earned on politi-

\textsuperscript{202} Even if the perpetrator of the cyber crime could meet the financial demand of substantial civil damages, financial compensation will not be able to remedy every injustice absorbed by the victim. As airlines are experiencing first hand in a post-September 11th world, no fixed amount of money will ever immediately cure the corrosion of consumer confidence.
While such a scandal may be considered common in the American political arena, the affair in Germany led to the resignation of Gregor Gysi, an economics minister in the city-state of Berlin who is a prominent member of the Party of Democratic Socialism. At the peak of the scandal, Lufthansa was the subject of enormous criticism for its role in the affair and, thus, likely suffered considerable damage to its public reputation. Despite accusations of violating the country’s personal data protection laws by supplying the names of the politicians to the newspapers, Lufthansa held steadfast and refused to comply with subsequent demands requesting the airline to release a list of all elected officials who have used miles earned during government travel for personal use. Lufthansa’s subsequent actions in the wake of the controversy suggest that it never released the information voluntarily, but was instead the unfortunate victim of an unauthorized access and disclosure of proprietary data.

V. CONCLUSION

In light of the legislative and judicial history of the ECPA, it is understandable that courts continue to find the intersection between the Wiretap Act and the SCA a complex and convoluted area of the law. The courts themselves recognize that they have “struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.” The courts have further stated that “until Congress brings the laws in line with modern technology, protection of the Internet... will remain a confusing and uncertain

203 Roland Eggleston, Germany: Politician Resigns Over Frequent-Flyer-Miles Scandal, Radio Free Europe at http://www.rferl.org (last visited Nov. 5, 2003). While frequent flyer programs such as Lufthansa’s “Bonus Miles” program are common to almost all Western airlines, German politicians are forbidden from earning frequent flyer points while on official business trips. Id.

204 Id. A handful of other German politicians, including the Green Party’s Rezzo Schlauch, were also enveloped by the scandal. Id.


206 Despite Lufthansa’s pleas of innocence, the German Federal Commissioner for Data Security, Joachim Jacob, led further attacks against the air carrier, stating that when over 4,000 employees have access to customer data, it is decidedly too many. German News Team, Thierse on the Frequent Flyer Miles Scandal, German News (English Edition) at http://www.mathematik.uni-ulm.de/de-news/2002/08/032100.html (last visited Oct. 27, 2003).

207 Konop, 302 F.3d at 874; Steiger, 318 F.3d at 1047.
area of the law." While no one doubts that the burden on the judicial system is quite onerous when courts are held responsible for administering a legislative bill that is far from clear, the failure of Congress to listen to the judicial cries for help is not an excuse for judicial incompetence. Instead of focusing entirely on legislative history and statutory language that is ambiguous, courts would likely rectify their problems if they construed the ECPA in light of modern communications technology. While some courts, such as Fraser, have made concerted efforts to do just this, many courts do not understand the concepts that enable modern day communication to occur in an electronic medium.

Applying common law rules to different forms of technology without truly understanding the intricacies of that technology does nothing more than afford airlines and other businesses a legislative bill without teeth. Courts should thus consider the proposed interpretation of the ECPA that is set forth in this comment. It proposes a fair interpretation that (1) addresses the issues Congress faced when it enacted the ECPA, (2) follows the plain language of the statutes, (3) provides technological flexibility, and (4) affords privacy and protection to both the public and business sectors. It proposes an interpretation that combines the lesser-included offense theory from Smith with the transmission/storage dichotomy exposed in Fraser.

208 Steiger, 318 F.3d at 1047.
209 See Conroy v. Aniskoff, 507 U.S. 511, 519 (1993) (Scalia, J., concurring) (recounting Judge Harold Leventhal's description of the use of legislative history as "the equivalent of entering a crowded cocktail party and looking over the heads of the guests for one's friends." cited in Smith, 155 F.3d at 1056 n.9).
210 The Steiger court ends its analysis of the ECPA by concluding that its reading of the Wiretap Act and the SCA reveals a legislative hiatus that creates no remedy. Steiger, 318 F.3d at 1049. This conclusion is erroneous. It is the judicial construction of the ECPA that yields no remedy.