LJN LAW JOURNAL NEWSLETTERS

THE PRIVACY & DATA PROTECTION LEGAL REPORTER™

Volume 1, Number 2 • March 2006

ALM

USA PATRIOT Act Impasse: E-mail Interception Rules Need Congressional Attention, Too

By Robert D. Brownstone and Christine A. Vogelei

When, if ever, can your Internet Service Provider ("ISP") legally intercept and then read your e-mail? Nearly anytime, according to almost every federal court that has tackled the issue. Due to outdated statutory language, courts have been inconsistent and tentative in applying the federal Wiretap Act to e-mail interception. In recent years, two circuits have flip-flopped on this crucial issue.

The original guiding force behind the 1968 Wiretap Act was to protect real-time wire and cable communications from interception while *in transit*. *Stored* communications, however, have been covered by the eponymous Stored Communications Act ("SCA") since 1986 — when Congress enacted the Electronic Communications Privacy Act ("ECPA"). The ECPA incorporated the old Wiretap Act as Title I and added the SCA as Title II.

With the SCA, Congress relaxed the level of protection for stored communications, divining a lower expectation of privacy in completed transmissions than in "live" conversations. Accordingly, while the SCA generally prohibits *unauthorized* access to stored e-mail, it provides an exemption for ISPs, which may need to access users' e-mails for a variety of legitimate purposes. Therefore, unless e-mail is protected under the SCA's cohort, namely the Wiretap Act, ISPs will be granted free license to read any e-mail, even before it has been read by the intended recipient.

The archaic language of two key Wiretap Act definitions was crafted long before e-mail and is thus unsuited to deal with modern reality. The inherent ambiguity is the source of much debate and has allowed the First and Ninth Circuits to come out on opposite sides of the issue. Most Americans would be shocked if they realized how little protection the law actually provides.

In 2001, Congress hastily passed the USA PATRIOT ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism") Act. One of the Act's provisions redefined the Wiretap Act language at the heart of the above-mentioned circuit split. That change not only failed to help matters, but it also led to yet another Wiretap Act case law oddity. The Ninth and First Circuits have purported to apply the pre-USA PATRIOT version of the ECPA. Yet, paradoxically, each of those courts' conflicting decisions has relied on the USA PATRIOT changes as supporting its own view on the interception issue.

Sixteen of the USA PATRIOT Act's provisions were scheduled to sunset on Dec. 31, 2005. That deadline was extended twice, and on March 2, 2006 the Senate voted to make these provisions permanent. Also on Congress' plate is the controversy surrounding the Foreign Intelligence Surveillance Act ("FISA"). The overall issue of eavesdropping/wiretapping has thus come front and center. The time is ripe for Congress to focus on amending the Wiretap Act to ensure privacy protections rising to the level of the public's expectations.

History of the Electronic Communications Privacy Act

In 1986, when e-mail and the Internet were still in their infancy, Congress passed the ECPA. 18 U.S.C. §2510 *et seq.* The ECPA amended the Wiretap Act, which had previously covered only wire communications, to also punish the interception of *electronic* communications. The ECPA also introduced the SCA, which prohibits unauthorized access to stored communications. For the most part, the 1986 definitions are the ones we rely on today.

The Wiretap Act (as Amended)

Congress passed the ECPA to add new protections for digitally generated transmissions: "any person who intentionally intercepts, endeavors to intercept, or procures any person to intercept or endeavor to intercept, any wire, oral, or *electronic* communication … shall be punished." 18 U.S.C. §2511(1) (emphasis added). The Act separately defines "wire communication" and "electronic communication." Ambiguity arises when courts are asked to interpret: 1) the scope of communications considered "electronic," and 2) the word "intercept."

As defined in §2511(1), a "wire communication" includes wire communications held in electronic storage. An example is voicemail. The definition of "electronic communication," however, is silent as to stored communications. As a result, stored *wire* communications are explicitly protected, but stored electronic communications are in an indeterminate state.

When originally enacted, the word "intercept" necessarily referred to interception contemporaneous with transmission. Yet, with the advent of voicemail and e-mail, it became possible for transmission and interception to occur at different times. Hence, the

continued on page 2

E-mail Interception

continued from page 1

question of statutory coverage of non-contemporaneous interceptions arose.

The Stored Communications Act

While the Wiretap Act punishes unauthorized interceptions of communications while *in transit*, the SCA prohibits unauthorized access of communications while *stored*. 18 U.S.C. §2701. Congress provided a lower level of protection for access to stored communications, which it considered to be less of an intrusion on individual privacy than an "interception." Consequently, §2701(c)(1) provides an exception for "the person or entity providing a wire or electronic communications service." As a result, an ISP cannot violate the SCA.

Judicial Interpretation of the Wiretap Act as Applied to E-mails in Transit

Majority View: Interception Must Be Contemporaneous with Transmission

In 2002, the Ninth Circuit, in *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002) ("*Konop II*"), joined the group of courts imposing a contemporaneity requirement. *See, e.g., Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003); *U.S. v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003), *cert. denied*, 123 S. Ct. 2120 (U.S. 2003); *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 459-60 (5th Cir. 1994). *See generally* Robert D. Brownstone, *et al.*, 9 *Data Security & Privacy Law*, Privacy Litig. Ch. §9:45 (West 2001 & Supp. 2005).

Robert Konop, a Hawaiian Airlines pilot, maintained a secure Web site where he posted discussions criticizing his employer. He authorized fellow employees to access the Web site via a password and a nondisclosure agreement designed to keep the information from falling into his employer's hands. Two other pilots allowed the employer to access the Web site using their login names and passwords. In this manner, Hawaiian's vice president accessed Konop's Web site more than 30 times. Konop subsequently filed suit, alleging violations of the Wiretap Act and SCA, among other claims.

The District Court granted summary judgment on the two ECPA claims. On appeal, the Ninth Circuit initially reversed, rejecting the theory requiring contemporaneity. *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (9th Cir. 2001) ("*Konop I*"). Then, it withdrew its opinion *sua sponte* and affirmed the District Court. In its second opinion, the Ninth Circuit upheld the dismissal of Konop's claim under the Wiretap Act, but barely maintained his claim under the SCA.

At issue was whether the meaning of "intercept" differed with respect to wire and electronic communications. The court relied upon the earlier Wiretap Act decisions to determine that Congress intended the definition of "intercept" to require acquisition contemporaneous with transmission. Through the ECPA, Congress had ostensibly rescinded the contemporaneousness requirement with respect to wire communications by altering the definition of "wire communications" to explicitly include stored communications. But it had *not* done so as to the definition of "electronic communications."

Comparing the separate definitions, *Konop II* determined, as had previous decisions, that Congress had intended the Wiretap Act to protect stored wire communications but not stored electronic communications. By its very nature, a stored wire communication cannot be intercepted contemporaneously with transmission; thus, the requirement was eliminated. Therefore, *Konop II* concluded that "intercept" means two different things for wire and electronic communications. For wire communications, the interception need not be contemporaneous. For electronic communications, the interception must be contemporaneous with transmission.

In the factual context at hand, the Ninth Circuit held that interception of information on Konop's Web site had not been contemporaneous. The data on the site had been stored on the server at the time Hawaiian accessed it. Because stored electronic communications were not protected by the Wiretap Act, there could be no interception, and thus no violation, thereunder.

The court also opined that protecting stored electronic communications under the Wiretap Act would render the SCA meaningless. Congress intended the SCA to offer less protection to certain stored communications, allowing law enforcement officers to meet a lesser burden than under the Wiretap Act to access such communications. Nevertheless, if stored electronic communications were to also be protected by the Wiretap Act, law enforcement could never benefit from that lesser burden.

As to whether the employer's conduct had violated the SCA, *Konop II* remanded on a narrow factual issue. In addition to the provider exception, the SCA affords an exemption from liability if access is user-authorized. Two of Konop's fellow pilots had allowed the employer to access the site using their authorized login information. A question remained, however, as to whether the pilots qualified as "users" because they had never actually logged on to the Web site themselves.

New Minority View: Interception Need Not Be Contemporaneous with Transmission

Last year, the First Circuit performed its own flip-flop on the e-mail interception issue. *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (*en banc*) ("*Councilman II*").

continued on page 3

Robert D. Brownstone is the Practice Technology Manager at Fenwick & West LLP, a 250-attorney Silicon-Valley-based law firm specializing in providing a wide array of services to high-technology companies. Brownstone is a nationwide speaker and writer on law and technology issues arising from e-discovery, information security and compliance. He is a member of four state bars and the Information Systems Auditing and Control Association ("ISACA"). He can be reached at 650-335-7912 or *rbrownstone@fenwick.com*.

Christine A. Vogelei is an associate in the Litigation and Privacy & Information Security Practice Groups at Fenwick & West LLP and is based in the San Francisco office. She can be reached at 415-875-2348 or *cvogelei@fenwick.com*.

E-mail Interception

continued from page 2

In contrast with the Ninth Circuit, the First Circuit initially found no Wiretap Act violation, but then, in its second decision, found that there was a tenable violation. Though purporting to sidestep the contemporaneousness controversy, *Councilman II* implicitly rejected a contemporaneity requirement.

Bradford Councilman ran Interloc, an online rare book listing service. Interloc also provided its book dealer customers with e-mail addresses and acted as their service provider in that regard. Councilman instructed his employees to write a computer program that would intercept and create copies of all e-mail sent from Amazon.com to Councilman's customers. The copies were routed to Councilman's mailbox so that he could read them to gain a commercial advantage. Based on thousands of such e-mail interceptions, Councilman was criminally charged with conspiracy to violate the Wiretap Act.

The District Court denied Councilman's motion to dismiss the indictment. *U.S. v. Councilman*, 245 F. Supp. 2d 319 (D. Mass. 2003). On appeal in 2004, in its first look at the case, the First Circuit affirmed the dismissal. *U.S. v. Councilman*, 373 F.3d 197, 203 (1st Cir. 2004) ("*Councilman I*"). The government successfully sought a rehearing *en banc*. Upon reconsideration, the First Circuit reversed and remanded, potentially reinstating the charge.

The District Court, following *Konop II*, had held that only electronic communications — and not stored wire communications — were protected by the Wiretap Act. In addition, the court found that e-mails in transit were also simultaneously in storage because the process of sending e-mail necessarily requires computers to repeatedly copy an e-mail message *seriatim* as it travels from server to server to its final destination. The copies are temporarily stored on these servers, causing an e-mail to be in transit and in storage simultaneously. Because the e-mails intercepted by Councilman existed on the Interloc system's RAM, the trial court deemed them to be "in storage" and incapable of "interception."

That holding required the District Court to accept a broad definition of the term "in storage." Under the Wiretap Act, the definition of electronic storage includes "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," as well as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 28 U.S.C. §2510; *U.S. v. Councilman*, 245 F. Supp. 2d 319, 320 (D. Mass. 2003). Following the Ninth Circuit's lead, the *Councilman* trial court stated that "[t]he majority opinion in *Konop* took a strict view of the phrase 'in storage' and found that no violation of the Wiretap Act occurs when an electronic communication is accessed during storage, even if the interception takes place during a nanosecond 'juncture' of storage along the path of transmission." *Id.* at 321. This position virtually cuts off any possibility of protecting the interception of e-mail under the Wiretap Act.

On appeal, the First Circuit initially affirmed the District Court's dismissal of the Wiretap Act violation. First, *Councilman I* held that the Act did not protect electronic communications in storage. The court reasoned that because stored communications were not included in the definition of "electronic communications," Congress did not intend to protect them. Second, *Councilman I* analyzed whether the e-mails were "in storage" in order to address the so-called "contemporaneous" problem.

In concept, the *Councilman I* majority agreed with the premise that the Wiretap Act was designed to prohibit interceptions contemporaneous with transmission. The mechanics of e-mail, however, make contemporaneous interception virtually impossible. In the case at hand, copies of the e-mails had been siphoned off while in transit to the intended recipient. Because the e-mail messages existed on the defendant's server's RAM, however, the e-mails were considered "in storage" and thus no interception was possible. The court noted that "[i]t may well be that the protections of the Wiretap Act have been eviscerated as technology advances." *U.S. v. Councilman*, 373 F.3d 197, 203 (1st Cir. 2004). Judge Kermit V. Lipez authored a lengthy dissent, the logic of which is reflected in the majority opinion he ultimately wrote for *Councilman II*.

Subsequently, however, the First Circuit granted review *en banc* and reversed. *U.S. v. Councilman*, 418 F.3d 67, 76 (1st Cir. 2005). After consulting the legislative history, *Councilman II* concluded that the previous interpretations of the Wiretap Act had been inconsistent with Congress' intent. In direct contrast to the Ninth Circuit, the court held that e-mails in transit, though also temporarily in storage, *were* protected by the Wiretap Act.

The *Councilman II* decision first looked to the plain meaning of §2510. It concluded that the absence of "stored communications" in the definition of "electronic communication" did not necessarily evince Congressional intent to exclude stored messages from protection. Different canons of construction could manipulate an outcome on either side of the issue and therefore did not resolve the question.

The court thus looked beyond the canons of construction to the legislative history to ascertain Congress' intent when adding electronic communications to the Wiretap Act in 1986. The legislative history showed that the ECPA amended the Wiretap Act to bring electronic communications within its aegis. In addition, Congress had added a clause to the definition of "wire communication" to protect wire communications in storage. The legislative history had specifically referenced voicemail as an example. The *Councilman II* majority concluded that the sole reason for the new clause was to include voicemail under the Wiretap Act, not to exclude e-mail.

In fact, the legislative history indicated that "interception of electronic mail at any stage involves a high level of intrusiveness and a significant threat to civil liberties." 418 F.3d at 76. *Councilman II* thus concluded that "the purpose of the broad definition of electronic storage was to enlarge privacy protections for stored data under

continued on page 4

E-mail Interception

continued from page 3

the Wiretap Act, not to exclude e-mail messages stored during transmission from those strong protections." *Id.* Accordingly, the court rejected the notion that transient electronic communications temporarily in storage are not "electronic communications."

The *Councilman II* majority averred that it was only looking at the "wire" and "electronic" communications definitions and that it was not touching on contemporaneity. However, the majority opinion concluded with dicta on the "intercept" concept, finding it "impossible" for the defendant to show an e-mail transmission had been completed while the message was still "en route." *Id.* at 80. To complete the contemporaneity flip-flop cycle, the author of the *Councilman I* majority wrote a vehement dissent in *Councilman II.*

All of the *Councilman* decisions were written after the USA PATRIOT Act's October 2001 amendment of the "wire communications" definition — namely the removal of "storage." Yet the events precipitating the *Councilman* prosecution had occurred before October 2001. Thus, like *Konop II* before it, *Councilman II* was bound to interpret and apply the pre-USA PATRIOT Act version of the Wiretap Act. However, also akin to *Konop II*, *Councilman II* nonetheless infused its "intercept" analysis with its own spin on the 2001 Congressional action.

Pending Legislation Provides Opportunity for Clarification

USA PATRIOT Act

In October 2001, the USA PATRIOT Act §209 amended the Wiretap Act by eliminating "storage" from the definition of "wire communication." Given the timing of the underlying facts, *Konop II* and *Councilman II* were supposed to apply pre-USA PATRIOT Act statutory and case law. Yet, both those decisions discussed the USA PATRIOT Act's elimination of "storage" from the "wire communication" definition. Strikingly, however, the Ninth Circuit and First Circuit each drew a different inference. *Konop II* interpreted the 2001 amendment to indicate that neither stored wire communications nor electronic communications are protected. In other words, an interception must always be contemporaneous with transmission to constitute a Wiretap Act violation. As noted above, *Councilman II* drew a contrasting inference, finding that the temporary storage of e-mail in transit does not exclude it from protection under the Act.

To date, no court has been faced with a post-October 2001 factual scenario. Thus, no court has confronted the issue of how or whether the amendment changes the interpretation of the Wiretap Act. Regardless, §209 is among several provisions of the USA PATRIOT Act that the Senate voted to make permanent on March 2, 2006. While reviewing the 16 USA PATRIOT Act provisions at issue, Congress did not focus on §209 at all. Instead of automatically renewing §209, the legislature should have seized the opportunity to clarify the Wiretap Act to show the true intent regarding e-mail protection.

The E-Mail Privacy Act of 2005

Perhaps the inaction on §209 is due to the pendency of separate remedial legislation. In April 2005, Senators Patrick Leahy and John Sununu introduced the E-Mail Privacy Act. S. 936, 109th Cong. (2005). The E-Mail Privacy Act would change the definition of "intercept" in the Wiretap Act, 18 U.S.C. §2510(4), to read: "'[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication *contemporaneous with transit, or on an ongoing basis during transit*, through the use of any electronic, mechanical, or other device or process, notwithstanding that the communication may simultaneously be in electronic storage ... " (emphasis added).

On April 28, 2005, Senator Leahy's remarks to the Senate explained that this change is designed to prevent the interpretation reached by the court in *Councilman I* and restore a broader interpretation of "intercept." Leahy noted that *Councilman I*'s interpretation not only gives ISPs a license to snoop but also enables law enforcement — with the consent of an ISP — to monitor e-mail activity without a warrant. He stated that the law must be updated to match the outcome that Congress originally intended and that the American people expect.

On Sept. 19, 2005, the bill was referred to the House Subcommittee on Crime, Terrorism and Homeland Security. To the authors' knowledge, no pertinent activity has occurred in the ensuing 5 months. Enactment of the E-Mail Privacy Act would be a simple, efficient way to clear up the present case law confusion and protect the privacy of e-mail.

Conclusion

As in so many other areas, technology has outpaced the law that polices and protects it. This problem is evidenced by the courts' inability to consistently interpret the federal Wiretap Act. Furthermore, the task of gaining insight into Congress' intent regarding the scope of protection for e-mail is exceedingly challenging. The Act is outdated and impractical for modern situations. E-mail, the Internet, and the Web did not exist commercially when the Act was passed in 1968, or even when it was amended in 1986.

Congress has before it a simple solution to remedy this situation in the form of the E-Mail Privacy Act. Furthermore, the time is ripe, considering the current focus on the USA PATRIOT Act and on eavesdropping in general under FISA.

Congress should not let this opportunity pass. As a society, we rely on e-mail as a primary form of communication more than ever before. Federal law should provide a level of protection commensurate with the legitimate expectations of the American public.

—❖—