

Electronic Frontier Foundation commentary on Title III issues raised by anti-terrorism legislation

Contact: Lee Tien, Senior Staff Attorney, tien@eff.org, (415) 436-9333 x 102

Introduction

“The point of the Fourth Amendment . . . is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.” *Johnson v. United States*, 333 U.S. 10, 13-14 (1948).

Nowhere is this constitutional rule more important than for wiretapping and other forms of covert surveillance. “Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.” *Berger v. New York*, 388 U.S. 41, 63 (1967).

Government interception of communications also implicates important First Amendment values, especially in the national security context. *United States v. U.S. District Court*, 407 U.S. 297, 313-14 (1972) (“Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. . . . Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs.”); *Marcus v. Search Warrant*, 367 U.S. 717, 724 (1961) (“Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power.”).

We recount this well-known constitutional truths because they are at risk today. A major theme of the Anti-Terrorism Act is the relaxation or outright elimination of judicial oversight. This is dangerous to civil liberties, because law enforcers “may lack sufficient objectivity to weigh correctly the strength of the evidence supporting the contemplated action against the individual’s interests in protecting his own liberty.” *Steagald v. United States*, 451 U.S. 204, 212 (1981).

ATA

Sec. 101. Modification of authorities relating to use of pen registers and trap and trace devices.

18 U.S.C. Sec. 2510(4) defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Thus, Title III establishes a fundamental legal distinction between the “contents” of a communication and all other information relating to the communication. Analysis of Title III therefore implicates the pen/trap provisions, which traditionally have been considered to govern acquisition of non-“contents” information.

We address these issues in our submission regarding pen/trap authority.

Sec. 102. Seizure of voice-mail messages pursuant to warrants.

A second distinction of great significance to Title III analysis is the temporal nature of “acquisition.” As the Justice Department states in its general manual on searching and seizing computers, “acquisition” is ambiguous. “For example, when law enforcement surveillance equipment records the contents of a communication, the communication might be ‘acquired’ at three distinct points: first, when the equipment records the communication; second, when law enforcement later obtains the recording; or third, when law enforcement plays the recording and either hears or sees the contents of the communication. . . . Courts confronted with this ambiguity have rendered inconsistent rulings.”

One view is that wire and electronic communications are intercepted only at the time of transmission between the parties to the communication. Subsequent access to a stored copy of the communication does not “intercept” the communication.

The difficulty here is that Title III was drafted in light of ordinary telephone calls, which historically took place in real time and were not stored for later listening (as they often are today).

Current law, however, defines “wire communication” to include “any electronic storage of such communication,” meaning that stored voice mail is still a “communication” that can be “intercepted.” Accordingly, the government must apply for a Title III wiretap order before it can obtain unopened voice mail messages held by a service provider. *United States v. Smith*, 155 F.3d 1051, 1058-59 (9th Cir. 1998).

ATA 102 would effectively overrule *Smith* and reduce the protection afforded to such stored voice mail. This result is not reasonable given that the expectation of privacy enjoyed by the called person ought not change simply because the message is “waiting” to be listened to.

An obvious analogy is to postal mail. The government’s position is akin to saying that letters are less private once they have been delivered to your mailbox, even before you have actually opened the envelope.

The government argues that this change would “harmoniz[e] the rules applicable to stored voice and non-voice (e.g., e-mail) communications.” But the alleged harmonization reduces privacy protections that are already unjustifiably weak for stored non-voice communications. The conceptual difficulty discussed above -- the supposed requirement that “interception” be contemporaneous with transmission -- is even greater for electronic communications such as e-mail, which is always transmitted to a virtual “mail box.” .

More generally, the issue is whether Title III protections should become less important simply because technology leads away from real-time communication and more toward stored communication. We believe that individuals in this society have legitimate and reasonable expectations of privacy in their communications that do not turn on the technological details of how their words are transmitted.

Finally, we note that while the government speaks of enabling law enforcement “to seize suspected terrorists’ voice mail messages pursuant to a search warrant,” ATA 102 affects all voice mail messages and is not limited to investigations of terrorism.

Sec. 103. Authorized disclosure.

Current law limits disclosure of information obtained from Title III interceptions, in order to protect the privacy of individuals whose communications are intercepted. For instance, 18 U.S.C. § 2517(1) limits disclosure of such information “to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.”

ATA 103 would destroy this limit by redefining the term “investigative or law enforcement officer,” 18 U.S.C. § 2510(7), to include “any officer or employee of the executive branch of the federal government.”

The Justice Department’s analysis of this section speaks only of the benefit of permitting such disclosure to “a non-law enforcement officer for such purposes as furthering an intelligence investigation.” But that analysis fails to mention that ATA 103 is in no way limited to intelligence investigations; for instance, nothing prevents such information to be disclosed to White House employees in the performance of their political duties. As written, therefore, ATA 103 destroys privacy far beyond what is relevant to the anti-terrorism justification of the bill.

Sec. 105. Use of wiretap information from foreign governments.

ATA 105 would, in the Justice Department’s own words, permit “United States prosecutors [to] use against American citizens information collected by a foreign government even if the collection would have violated the Fourth Amendment.”

This section is not limited to terrorism investigation. Moreover, given the possibility that U.S. and foreign agencies already share intelligence information, this section would create incentives for other nations to engage in unlawful surveillance on behalf of the United States. Cf. Lawrence Sloan, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 *Duke L. J.* 1467, 1468 (2001) (discussing Echelon, “believed to be a joint initiative led by the National Security Agency in conjunction with its counterparts in the United Kingdom, Canada, Australia, and New Zealand”).

Sec. 106. Interception of computer trespasser communications.

Title III prohibits anyone from intentionally intercepting or disclosing the contents of protected communications without meeting Title III’s requirements unless the interception or disclosure falls within specified exceptions.

ATA 106 would create a new exception that permits government interception of “computer trespasser” communications if authorized by the owner or operator of the

trespassed-upon “protected computer.” The government actor would only need to be lawfully engaged in “an investigation” and have “reasonable grounds to believe” that the contents of the communication are relevant to the investigation.

The main problem is that Fourth Amendment restrictions on interception of communications are bypassed. Under *Berger v. New York*, communications interception requires that: (1) probable cause be shown that a particular offense has been or is about to be committed; (2) the communications to be intercepted are particularly described; (3) the surveillance be for a specific and limited period of time in order to minimize the invasion of privacy; (4) continuing probable cause showings be made if the surveillance is to continue beyond the original termination date; (5) the surveillance cease once the conversation sought is seized; (6) notice must be given unless there is an adequate showing of exigency; and (7) there be a return on the warrant so that the court may oversee and limit the use of the intercepted conversations.

Virtually all of these constitutional safeguards are eliminated. Probable cause is not required; particularity is lacking; there is no limit on the duration of surveillance; there is no notice provision; and because there is no warrant, there can be no court oversight as to the use of the intercepted communications.

Equally important, whether a person is a “computer trespasser” is determined in the first instance by the owner or operator of the computer, without judicial oversight or probable cause. If this determination is incorrect in that the person does have authorization to access the computer, it is too late: the person’s communications have already been intercepted. And of course, even if the person is a computer trespasser, ATA 106 contemplates the seizure of communications “to” the computer trespasser as well, and persons communicating with the computer trespasser may be entirely innocent.

Moreover, in such a situation the person would be in no position to challenge the warrantless interception, because he or she would have no notice at all that his or her communications had ever been intercepted. In short, the risk of error as to whether a person truly is a “computer trespasser” falls entirely upon the person.

Furthermore, an existing exception permits both interception and disclosure of communications by a service provider in order to protect the service provider’s “rights or property.” 18 U.S.C. § 2511(2)(a)(i) grants providers the right “to intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of service.” *United States v. Villanueva*, 32 F. Supp.2d 635, 639 (S.D.N.Y. 1998). Employees of a cellular phone company may intercept communications from an illegally “cloned” cell phone in the course of locating its source. See *United States v. Pervaz*, 118 F.3d 1, 5 (1st Cir. 1997). Providers may monitor misuse of a system in order to protect the system from damage, theft, or invasions of privacy. For example, system administrators can track hackers within their networks in order to prevent further damage. Cf. *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (concluding that need to monitor misuse of computer system justified interception of electronic communications according to § 2511(2)(a)(i)).

CTA

changes to Title III predicates

Under current law, a basic control on wiretapping is that the government may only intercept wire communications for certain crimes listed in Title III. 18 U.S.C. § 2516(1). In contrast, Title III permits interception of electronic communications like e-mail for any federal felony. 18 U.S.C. § 2516(3).

CTA would amend Title III by adding two types of crimes to the list of Title III predicate offenses: those relating to terrorism and those relating to criminal violations of the main federal computer crime law.

Both expansions are unwarranted. While there is no doubt that these crimes are serious, the government does not need additional authority to investigate terrorism.

First, virtually every terrorist act is already a federal felony on the list of crimes for which a wiretap order may be sought: all federal offenses involving murder, kidnaping, robbery, or extortion; espionage, sabotage, piracy, and treason; assassination and hostage-taking; destruction of trains, vessels, aircraft, and aircraft facilities; and offenses involving explosives, biological weapons, and nuclear materials. 18 U.S.C. § 2516(1).

Also, in terrorism cases, the government is likely to be able to invoke its secret surveillance powers under the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801 et seq., which permits wiretapping if there is probable cause to believe that the target is a member of a foreign terrorist group or an agent of a foreign power. If the target is a U.S. citizen or permanent resident, there must also be probable cause to believe that he or she is engaged in activities that “may” involve a criminal violation. Indeed, news reports have said that government agents presented ISPs with FISA warrants after the attack on September 11, showing that the government has authority to investigate terrorist activity under existing law.

The expansion to violations of 18 U.S.C. § 1030, the Computer Fraud and Abuse Act (CFAA) is also easily criticized. As enacted in 1984, CFAA was deliberately and narrowly tailored to protect classified U.S. defense and foreign relations information, financial institution and consumer reporting agency files, and access to computers operated for the government. See Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 456 (1990) (discussing history of 1984 Act and its 1986 amendments).

By 1996, however, CFAA had been amended to reach all computers involved in interstate and foreign commerce or communication, whether or not any federal government proprietary interest was involved.

Two sections of CFAA are especially broad. 18 U.S.C. §§ 1030(a)(5)(A), (a)(5)(C). Violations of these sections are felonies if the offense was committed for purposes of commercial advantage or private financial gain, for the purposes of committing any

criminal or tortious act in violation of the laws of the United States or of any State, or if the value of the information obtained exceeds \$ 5,000.

This damage requirement is easy to meet. Under § 1030(e)(8), damage means “any impairment to the integrity or availability of data, a program, a system, or information that (A) causes loss aggregating at least \$5000 in value during any 1-year period to one or more individuals.”

§ 1030(a)(5)(A) states that “[one who] knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer” has committed a crime.

Several civil cases have construed this language. For example, in *Shaw v. Toshiba America Information Systems, Inc.*, 91 F.Supp.2d 926 (E.D.Tex.,1999.), defendant knowingly distributed laptop computers containing disk drives with faulty microcode that allowed unwanted corruption/deletion of data. The court squarely held that manufacturers of computer equipment could be reached by Sec. 1030(a)(5)(A) -- "transmission" includes the design, manufacture, creation, distribution, sale, and marketing of floppy-disk controllers allegedly made faulty by defective microcode.

One court has found that placing a cookie on a user's computer to monitor websurfing habits could violate Sec. 1030(a)(5)(A). In *re Intuit Privacy Litigation*, 138 F.Supp. 2d 1272 (C.D.Cal. 2001). Defendant operated a website that used cookies to track its users, and were sued for privacy violations on several theories, including Sec. 1030. On motion to dismiss, the court found that this conduct fell within Sec. 1030(a)(5)(A). (Because the class-action plaintiffs had not alleged economic damages, the motion to dismiss was granted, but without prejudice, to allow the plaintiffs to make the proper allegations.)

Meanwhile, § 1030(a)(5)(C), generally prohibits accessing a protected computer "without authorization" or "in excess of authorization" if it results in the person's obtaining information from the protected computer.

The problem here is that “without” or “in excess of authorization has been very broadly interpreted by the courts. In *America Online, Inc. v. LCGM, Inc.*, 46 F.Supp.2d 444, 450-51 (E.D.Va. 1998), a court held that spamming civilly violated 18 U.S.C. § 1030(a)(2)(C) because the spammers used their AOL membership to harvest other AOL members’ e-mail addresses in violation of AOL’s terms of service, thus exceeding their authorization. The spammers also violated 18 U.S.C. § 1030 (a)(5)(C) because AOL suffered damage of more than \$5000 in dealing with the spam and in lost goodwill, revenue, and customers.

In *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121(W.D. Wa. 2000), the court found on a motion to dismiss that e-mails containing trade secrets sent by a former employee while he was still a Shurgard employee constituted violations of CFAA. In effect, the court found that an employee’s using his employer’s computer system in a disloyal way could violate CFAA, because the disloyalty caused an implied revocation of authorization.

In *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), the court issued a preliminary injunction enjoining Verio, Inc. from either using a search robot to get information from Register.com's Whois database, or using information derived from that database for mass unsolicited advertising by telephone, direct mail or electronic mail. The court held that Verio's actions would likely violate CFAA, 18 U.S.C. §§ 1030(a)(2)(c) and (a)(5)(c). The court noted that “[i]f the strain on Register.com's resources generated by robotic searches becomes large enough, it could cause Register.com's computer systems to malfunction or crash. Such a crash would satisfy § 1030(a)(5)(C)'s threshold requirement that a plaintiff demonstrate \$5000 in economic damages.”

It is clear that CFAA extends to many activities that have nothing to do with terrorism. Moreover, Title III already permits the use of CFAA as a predicate for intercepting electronic communications, which are likely to be used by CFAA violators.

USAA

Sec. 201. adds terrorism laws to Title III predicate offenses

USAA and CTA are identical here.

Sec. 202. adds felony violations of CFAA to Title III predicate offenses

USAA and CTA are identical here.