Electronic Privacy Information Center

September 24, 2001

Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001
Affecting the Privacy of Communications and Personal Information

In response to the horrendous attacks that occurred on September 11, Attorney General Ashcroft has proposed the Anti-Terrorism Act of 2001 (ATA), a far-reaching legislative package intended to strengthen the nation's defense against terrorism. Several of ATA's provisions would vastly expand the authority of law enforcement and intelligence agencies to monitor private communications and access personal information. Those provisions address issues that are complex and implicate fundamental constitutional protections of individual liberty, including the appropriate procedures for interception of information transmitted over the Internet and other rapidly evolving technologies. Despite the complexity of these matters, the Attorney General has urged Congress to quickly approve the proposal, which became available for analysis only within the last several days.

As Congress considers this important piece of legislation, it should be guided by several critical factors:

- Law enforcement and intelligence agencies already possess broad authority to conduct investigations of suspected terrorist activity. In fact, Congress approved new surveillance powers to combat terrorism in late 1998. Describing those provisions after enactment, an FBI national security official said that "any one of these extremely valuable tools could be the keystone of a successful operation" against sophisticated foreign terrorists.[1]

- Any expansion of existing authorities should be based upon a clear and convincing demonstration of need. Congress should assess the likely effectiveness of any proposed new powers in combating the threats posed by terrorist activity.

- Any new authorities deemed necessary should be narrowly drawn to protect the privacy and constitutional rights of the millions of law-abiding citizens who use the Internet and other communications media on a daily basis.

- The longstanding distinction between domestic law enforcement and foreign intelligence collection should be preserved to the greatest extent possible consistent with the need to detect and prevent terrorist activity.

- Expanded investigative powers should be limited to the investigation of terrorist activity and should not be made generally applicable to all criminal investigations.

[1] Vernon Loeb, "Anti-Terrorism Powers Grow," Washington Post, January 29, 1999, p. A23.

Analysis of Specific Provisions

Pen Registers, the Internet and Carnivore

Currently, the statute authorizing the use of "pen register" and "trap and trace" devices[2] governs real time interception of "numbers dialed or otherwise transmitted on the telephone line to which such device is attached."[3] Although the use of such devices requires a court order, it does not require a showing of probable cause. There is, in effect, no judicial discretion, as the court **must** authorize monitoring upon the mere certification by a government attorney that the "information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." Therefore, these procedures lack almost all of the significant privacy protections found in Title III, the statute governing the interception of the actual "content" of a communication (e.g., a phone conversation or the text of an e-mail message).

The proposed ATA (Section 101) would significantly expand law enforcement authority to use trap and trace and pen register devices. Current law relating to the use of such devices was written to apply to the telephone industry, therefore the language of the statute refers only to the collection of "numbers dialed" on a "telephone line" and the "originating number" of a telephone call. The proposed legislation would redefine a pen register as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." A trap and trace device would be defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information relevant to identifying the source or a wire or electronic communication."

By expanding the nature of the information that can be captured, the amendment clearly expands pen register capacities to the Internet, covering electronic mail, Web surfing, and all other forms of electronic communications. The full impact of this expansion of coverage is difficult to assess, as the proposed statutory definitions are vague with respect to the types of information that can be captured and are subject to broad interpretations. The proposed ATA does not take into account the unique nature of such information, which contains data far more revealing than phone numbers, such as URLs generated while using the Web which often contain a great deal of information that cannot in any way be analogized to a telephone number.[4] Although the FBI has compared telephone calls to Internet communications to justify invocation of the existing pen register statute

---

[2] *See* 18 U.S.C. § 3121 *et seq*.

[3] 18 U.S.C. § 3121.

[4] It is not clear that these amendments would withstand Fourth Amendment scrutiny. The Supreme Court in *Smith v. Maryland* emphasized that it is only because of the very limited information revealed by a pen register that use of such a device does not constitute a search: "a pen register differs significantly from the listening device employed in [wiretapping of telephone conversations], for pen registers do not acquire the *contents* of communications. … we doubt that people in general entertain any actual expectation of privacy in the numbers they dial."

to authorize the use of its controversial Carnivore system, whether current law in fact grants such authority remains an open and debatable question. The proposed amendment would codify the FBI's questionable interpretation of the pen register statute, thereby closing the door to fully informed and deliberate consideration of this complex issue.

When the FBI's use of Carnivore was revealed in July 2000, there was a great deal of concern expressed by members of Congress, who stated their intent to examine the issues and draft appropriate legislation. To facilitate that process, former Attorney General Reno announced that issues surrounding Carnivore would be considered by a Justice Department review panel and that its recommendations would be made public. That promised report had not been released when Ms. Reno left office, and Attorney General Ashcroft recently announced that a high-level Department official would complete the review process. As a result of the delay, Congress does not yet have the benefit of the promised findings and recommendations. Because Carnivore provides the FBI with access to the communications of **all** subscribers of a monitored Internet Service Provider (and not just those of the court-designated target), it raises substantial privacy issues for millions of law-abiding American citizens.

Expanded Dissemination of Wiretap Information

The proposed ATA (Section 103) would amend the definition of "investigative or law enforcement officer" (for purposes of 18 U.S.C. § 2517) to include "any officer of or employee of the executive branch of the federal government." 18 U.S.C. 2517 governs the permissive disclosure and use of intercepted communications; information captured through interception can be disclosed 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,"[5] and the information can be used by any officer properly in possession of the information "to the extent appropriate to the proper performance of his duties."[6] The amendment would thus permit broad disclosure of information obtained through wiretaps to any employee of the Executive branch, without clear limits on what information may be disclosed, to whom, or for what purposes. Although the Justice Department states that "[t]his section facilitates the disclosure of Title III [wiretap] information to other components of the intelligence community in terrorism investigations,"[7] the proposal is far more expansive, as the permitted disclosure to and use by Executive employees would not be limited to information relating to investigations of terrorist activities.

[5] 18 U.S.C. § 2517(1).

[6] *Id*. § 2517(2).

[7] Anti-Terrorism Act of 2001 Section by Section Analysis (Consultation and Discussion Draft 9/19).

Use of Wiretap Information from Foreign Governments

The proposed legislation (Section 105) would permit United States prosecutors to use against American citizens information collected overseas by foreign governments even if the interception would have violated the Fourth Amendment if conducted by the United States. The proposed amendment would not permit use of such information if obtained with the "knowing participation," or at the direction, of American law enforcement personnel if gathered in violation of constitutional protections. The most immediate problem with this provision is its general applicability; the amendment is not limited to use of intercepted information relating to terrorism investigations. Furthermore, permitting use of private communications obtained by foreign governments without Fourth Amendment compliance could easily invite undetectable collusion between U.S. and foreign agencies in circumstances where U.S. authorities would be constitutionally precluded from obtaining the information themselves.

Interception of "Computer Trespasser" Communications

Existing law prohibits anyone from intentionally intercepting or disclosing the contents of any intercepted communications without complying with the requirements of the wiretap statute, unless such interception and disclosure falls within one of several statutory exceptions.[8] The proposed ATA (Section 106) would create a new exception, permitting government interception of the "communications of a computer trespasser"[9] if the owner or operator of a "protected computer" authorized the interception. The proposed exception has potentially broad implication, given that a "protected computer" includes one "which is used in interstate or foreign commerce or communication."[10]

In light of the potential breadth of this exception, it would be particularly inappropriate to remove any judicial oversight from surveillance of suspected "intruder" communications. The proposed amendment would place the determination solely in the hands of law enforcement and the system owner or operator. In those likely instances in which the interception does not result in prosecution, the target of the interception would never have an opportunity to challenge the activity. Indeed, such targets would never even have notice of the fact that their communications were subject to warrantless interception. For that reason, such a broad expansion of the now limited statutory exceptions should be carefully evaluated, and consideration of the issue should include an examination of current practices and experiences in cases involving suspected computer intrusions.

[8] *See* 18 U.S.C. § 2511

[9] The amendment would adds a definition of "computer trespasser" to 18 U.S.C. § 2510(20): "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the computer."

[10] 18 U.S.C. § 1030(e)(2).

Expanded Scope of Subpoenas for Records of Electronic Communications

Current law delineates the requirements for law enforcement access to records concerning electronic communications service. A service provider must disclose[11] to a government entity "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service or a subscriber to or customer of such service and the type of services the subscriber or customer utilized."[12] The proposed ATA (Section 107) would expand the type of information that a provider must disclose to include, among other things, records of session times and duration; any temporarily assigned network address; and any means or source of payment. The proposed authority to use subpoenas (rather than court orders) for this broader (and more revealing) class of information would not be limited to investigations of suspected terrorist activity. Because the amendment would broadly apply to all government investigations, its impact on subscriber privacy interests must be closely examined.

Nationwide Application of Surveillance Orders

Current law -- relating to both wiretaps and pen register/trap and trace devices -- authorizes execution of a court order only within the geographic jurisdiction of the issuing court. The proposed ATA (Sections 101 and 108) would expand the jurisdictional authority of a court to authorize the installation of a surveillance device anywhere in the United States. The availability of nationwide orders for the interception and collection of electronic evidence would remove an important legal safeguard by making it more difficult for a distant service provider to appear before the issuing court and object to legal or procedural defects. Indeed, it has become increasingly common for service providers to seek clarification from issuing courts when, in the face of rapidly evolving technological changes, many issues involving the privacy rights of their subscribers require careful judicial consideration.[13] The burden would be particularly acute for smaller providers -- precisely those, for instance, who are most likely (according to the FBI) to be served with orders requiring the installation of the Carnivore system.

Multi-Point ("Roving Wiretap") Authority

The proposed ATA (Section 152) would expand the government's powers under the Foreign Intelligence Surveillance Act ("FISA") to include "roving wiretap" authority,

---

[11] Disclosure is mandated "when the government entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena," or according to a court order or warrant. 18 U.S.C. § 2703(c)(1)(C).

[12] 18 U.S.C. § 2703(c)(1)(C).

[13] *See, e.g., In re Application of the United States for an Order Pursuant to 18 U.S.C. 2703(d*), 36 F. Supp. 2d 430 (D. Mass. 1999)

which would permit the interception of any communications made to or by an intelligence target without specifying the particular telephone line, computer or other facility to be monitored. Current law requires third parties (such as common carriers and others) "specified in court-ordered surveillance" to provide assistance necessary to accomplish the surveillance. The proposed change would extend that obligation to unnamed and unspecified third parties. According to the Justice Department, "Under the proposed amendment, the FBI could simply present the newly discovered carrier, landlord, custodian, or other person with a generic order issued by the Court, and could then effect FISA coverage as soon as technically feasible."[14]

Such "generic" orders could have a significant impact on the privacy rights of large numbers of innocent users, particularly those who access the Internet through public facilities such as libraries, university computer labs and cybercafes. Upon the suspicion that an intelligence target might use such a facility, the FBI could monitor all communications transmitted at the facility. The problem is exacerbated by the fact that the recipient of the assistance order (for instance, a library) would be prohibited from disclosing the fact that monitoring is occurring.

The proposed "generic" roving wiretap orders raise significant constitutional issues, as they do not comport with the Fourth Amendment's requirement that any search warrant "particularly describe the place to be searched." That deficiency becomes even more significant when there is a likelihood that the private communications of law-abiding American citizens could be intercepted incidentally.

Lowered Standard for Foreign Intelligence Surveillance

The proposed legislation (Section 153) would expand the application of FISA to those situations where foreign intelligence gathering is merely "a" purpose of the investigation, rather than, as current law provides, the **sole** or **primary** purpose. The more lenient standards that the government must meet under FISA (as opposed to the stringent requirements of Title III) are justified by the fact that FISA's provisions facilitate the collection of foreign intelligence information, not criminal evidence. Were the lax FISA provisions made applicable to the interception of information relating to a domestic criminal investigation (as it would where foreign intelligence gathering is but one of the purposes of the investigation), this traditional justification would be eliminated. The proposed change would be a significant alteration to the delicate constitutional balance that is reflected in the current legal regime governing electronic surveillance.

Expansive Sharing of Foreign Intelligence Information

Section 154 of the proposed ATA would facilitate the sharing of any "foreign intelligence" information obtained as part of a criminal investigation. "Foreign intelligence information" is not defined, and the information could be disclosed to federal law enforcement, intelligence, protective, national defense, or immigration agents. The

[14] Anti-Terrorism Act of 2001 Section-by-Section Analysis (Consultation and Discussion Draft 9/19).

provision is not limited to information related to terrorism or national security interests, does not require a showing of necessity, provides for no oversight, and does not limit the purposes for which this information can be shared, used or redisclosed. It is unclear why this provision is contained in an "anti-terrorism" package; in its analysis of the ATA, the Justice Department offers examples of the provision's potential utility in organized crime and computer intrusion investigations, but does not explain the relevance of this broad expansion of authority to the exigent circumstances of anti-terrorism activities.

Liberalized Use of Pen Register/Trap and Trace Devices

The proposed legislation (Section 155) would remove the existing statutory requirement that the government prove the surveillance target is "an agent of a foreign power" before obtaining a pen register/trap and trace order. Therefore, the government could obtain a pen register/trap and trace device "for any investigation to gather foreign intelligence information," without a showing that the device has, is or will be used by a foreign agent or by an individual engaged in international terrorism or clandestine intelligence activities. As with Section 153, the proposed amendment would significantly eviscerate the constitutional rationale for the relatively lax requirements that apply to foreign intelligence surveillance. That laxity is premised on the assumption that the Executive Branch, in pursuit of its national security responsibilities to monitor the activities of foreign powers and their agents, should not be unduly restrained by Congress and the courts. The removal of the "foreign power" predicate for pen register/trap and trace surveillance upsets that delicate balance.

Broad Access to "Any Tangible Things"

Section 156 would grant the government the authority to "by administrative subpoena, require the production of any tangible things (including books, records, papers, documents, and other items) that are relevant" to an intelligence or terrorism investigation. Although the Justice Department has characterized this provision as applying to "business records," the scope of the proposed authority is far broader. The breadth of the power is compounded by the lack of any judicial involvement. Current law permits access to specified records only upon court order; the proposed amendment would allow access under a subpoena issued by investigators. Thus, the amendment removes judicial oversight and a reviewable standard from the process of obtaining access to a broad range of private records.

Removal of Existing Privacy Protections for Consumer and Educational Records

The proposed legislation (Section 157) would amend the National Security Letter authority within the Fair Credit Reporting Act, the Financial Right to Privacy Act, and the Electronic Communications Privacy Act to permit government access to banking, credit, and other records for foreign counterintelligence purposes upon "certification" by an FBI agent. Current law permits government access to such records upon a showing of relevance and that the consumer is an agent of a foreign power. The proposed amendment removes the "agent of a foreign power" requirement, providing government

access to a multitude of private records upon the FBI's certification that "the information sought is relevant to an authorized foreign counterintelligence investigation. Government access to private records would thus be greatly expanded, especially when exercised in conjunction with Section 153's broader application of FISA authority.

Likewise, the ATA (Section 158) would amend the Federal Education Rights and Privacy Act (FERPA) to permit access to educational records in the investigation of domestic or international terrorism, or national security. Current law prohibits the release of personally identifying information about students from education records without the consent of the student or parents, subject to limited exceptions.

Authority to Conduct Secret Searches

The proposed ATA (Section 352) contain a far-reaching provision that would eliminate the current requirement that law enforcement must provide a person subject to a search warrant or order with contemporaneous notice of the search. This significant change in current law would apply to all government searches for material that "constitutes evidence of a criminal offense in violation of the laws of the United States" and is not limited to investigations of terrorist activity. Currently, delayed notification of a search is authorized only under a very small number of circumstances (such as surreptitious electronic surveillance). The expansion of this extraordinary authority to **all** searches would constitute a radical departure from Fourth Amendment standards and could result in routine surreptitious entries (break-ins) by law enforcement agents.

For additional information, contact:

David Sobel or Mikal Condon
(202) 483-1140