

Anti-Terrorism Act Expands Government Surveillance Authorities, Weakens Privacy Protection with No Clear Benefit to Security

Preliminary Analysis
Center for Democracy & Technology
September 21, 2001

The Justice Department's Anti-Terrorism Act of 2001 (ATA) would expand federal government authorities to conduct electronic surveillance and otherwise collect information on US citizens. Some of the changes are quite fundamental. The bill includes numerous, complex provisions extending the surveillance laws (while raising many questions about how they will be implemented) and alters the long-standing distinction between criminal investigations and foreign intelligence investigations. Many of the changes are not related to security concerns raised by the September 11 terrorist attacks. Many are not limited to terrorism cases, but relate to all investigations. Some have been on the Justice Department's wish list for some time.

The FBI already has broad authority to monitor all kinds of communications, including email. Both the criminal wiretap statute and the Foreign Intelligence Surveillance Act already cover terrorism. For some time, it has been recognized that those standards need to strengthen the standards for government surveillance. The changes proposed in the ATA mainly weaken the judicial review.

Here are our top concerns:

- **Sec. 101. Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices.** Expands, in vague and potentially broad terms, the government's ability to get information about Internet communications under a loose standard. Also allows any magistrate in the country to issue a pen register or trap and trace order that can be served multiple times, anywhere in the country.
- **Section 153. Foreign Intelligence Information.** Allows the FBI to collect evidence for criminal cases under the looser standards of foreign intelligence investigations -- an end-run around the relatively stringent requirements for wiretaps in criminal cases and a breach of the understanding that led to enactment of FISA.
- **Section 155. Pen Register and Trap and Trace Authority.** Eliminates the only meaningful statutory control that exists on use of pen register and trap and trace devices in intelligence cases.
- **Section 156. Business records.** Allows access to any business records upon the demand of an FBI agent, with no judicial review or oversight.
- **Sec. 157. Miscellaneous national-security authorities** Amends several key privacy laws, allowing much greater access to banking, credit, and other

consumer records in counter-intelligence investigations, with no judicial review at all.

- Sec. 352. Notice. Allows secret searches through delayed notice for all warrants or court orders.

CDT urges members of Congress to carefully consider these new surveillance proposals, to ensure constitutional liberties and public trust in our communications networks are not sacrificed in a misguided bid for security.

Sec. 101. Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices.

Expands, in vague and potentially broad terms, the government's ability to get information about Internet communications under a loose standard. Also allows any magistrate in the country to issue a pen register or trap and trace order that can be served multiple times, anywhere in the country. – The government claims that it already has authority to collect, under the very weak provisions of the pen register and trap and trace statute, transactional data about Internet communications. But the existing statute, intended to collect telephone numbers, is vague as applied to the Internet. Section 101 compounds the vagueness. It would add the words "addressing" and "routing" to the description of what pen registers and trap and trace devices collect. What do these words mean? We are concerned that the provision would be cited as expanding the scope of what the government collects, creating a more intrusive form of surveillance.

Internet addressing information can be much more revealing than phone numbers and might include information about the content of communications; a URL, for example, which may fit the proposed statutory definition of "addressing" information, may include a specific search term entered into a search engine or the title of a specific book bought at Amazon.com. The bill provides no details on how this content would be separated from other addressing information. *This provision is constitutionally suspect as it could allow government access to content information with minimal judicial oversight, specifically prohibited in a recent DC Circuit Court ruling. (See USTA v. FCC.)*

The standard for pen registers is so low as to be meaningless: people whose communications are targeted need not be suspected of any crime; probable cause is not required, only mere "relevance" to some ongoing investigation; courts have no authority to review these orders. Before extending nationwide scope to these orders, the process for their approval needs to be given some meaningful judicial approval. Congress now should use the language approved by the House Judiciary Committee last year in H.R. 5018.

Subtitle A Electronic Surveillance

Sec. 105. Use of Wiretap Information from Foreign Governments.

Allows use of surveillance information from foreign governments, even if it was seized

in a manner that would have violated the Fourth Amendment. Section 105 makes surveillance information collected about Americans by foreign governments admissible in U.S. courts even if such interceptions would have been illegal in the U.S. (so long as U.S. officials did not participate in the interception.) Such a provision is ripe for abuse and provides unhealthy incentives for more widespread foreign surveillance of U.S. individuals.

Sec. 108. Nationwide Service of Search Warrants for Electronic Evidence.

Allows any magistrate in the country to issue an order to seize evidence anywhere in the country. The concept of jurisdiction has due process importance. Traditionally, search orders are limited to the scope of a the issuing judge's jurisdiction. Section 108 would allow the government to obtain from federal judges, even magistrate judges, anywhere in the country orders for seizure of electronic evidence that apply to any communications provider anywhere in the country. Providers could be presented with orders from magistrates thousands of miles away, leaving such providers with less opportunity to question such orders.

Subtitle B. Foreign Intelligence Surveillance and Other Information

The Foreign Intelligence Surveillance Act allows the FBI to conduct electronic surveillance and secret physical searches in the US, including surveillance of US citizens, in international terrorism investigations. The standards are much lower than the standards for criminal wiretaps, and in return, the surveillance is supposed to be focused on the collection of intelligence, not criminal evidence. The FISA court, which now approves about 1000 surveillance requests per year, has denied only one request in its 23 year history. FISA also authorizes court orders for access to travel records.

Section 152 Multi-Point Authority.

Allows roving taps, including against US citizens, in foreign intelligence cases with no limits – ignoring the Constitution's requirement that the place to be searched must be "particularly described." This section purports to afford the FBI "roving tap" authority for intelligence investigations similar to what already exists for criminal investigations. See 18 USC 2518(11). A roving tap allows the government to intercept whatever phone or email account a suspect uses, even if the government cannot specify it in advance. Roving tap authority is constitutionally suspect, at best, since it runs counter to the Fourth Amendment's requirement that any search order "particularly describe the place to be searched." However, the proposed language places no limitation on the exercise of the roving tap authority and offers the FBI no guidance for its exercise. The proposed change merely authorizes the court to issue to any "person" an order commanding them to cooperate with a surveillance request by the government. If roving tap authority is supposed to focus on the targeted person, not on the telephone instrument, then the intercept authority should be limited to the target – it should only allow interception of communications to which the target of the surveillance is a party. Such limitations are absent from this proposal.

Section 153. Foreign Intelligence Information

Allows the FBI to collect evidence for criminal cases under the looser standards of foreign intelligence investigations -- an end-run around the relatively stringent requirements for wiretaps in Title III. This section, which merely changes the word "the" to "a," would actually make a fundamental change in the structure of the wiretap laws. It would permit the government to use the more lenient FISA procedures in criminal investigations which have any counter-intelligence purposes and would destroy the distinctions which justified granting different standards under FISA in the first place. Under existing law, FISA can be used only if foreign intelligence gathering is "the" purpose of the surveillance. The proposed provision would permit FISA's use if this is "a" purpose, even if the primary purpose was to gather evidence for a criminal prosecution. This is an extraordinary change in the law which has no justification.

Section 154. Foreign Intelligence Information Sharing

With no standards, permits the sharing of grand jury information, Title III wiretap information, and any other "foreign intelligence information" acquired in a criminal case with many different federal officials not involved in law enforcement. This is a sweeping change in the law. "Foreign intelligence information" is not defined. The provision places no limits on the purpose for which the information may be shared, and no limit on its reuse or redisclosure. It requires no showing of need and includes no standard of supervisory review or approval. As written, a criminal investigator could share with White House staff information collected about foreign policy critics of the Administration. The provision, at the very least, should be drastically curtailed.

Section 155. Pen Register and Trap and Trace Authority

Eliminates the only meaningful statutory control that exists on use of pen register and trap and trace devices in intelligence cases. The law currently requires a showing that the person being surveilled is a foreign power, an agent of a foreign power or an individual engaged in international terrorism or clandestine intelligence activities. This amendment would eliminate that standard and permit the use of FISA for pen registers whenever the government claimed that it was relevant to an ongoing intelligence investigation. Contrary to the DOJ's assertion in its section-by-section, this is not the same as the standard for pen registers in criminal cases. There, the surveillance must be relevant to an ongoing criminal investigation, which is moored to the criminal law. There is no similar constraint on foreign intelligence investigations, since they can be opened in the absence of any suspicion of criminal conduct. This provision ignores the fact that the government was granted the special rules of FISA only for situations that involved intelligence gathering about foreign powers.

Section 156. Business records

Allows access to any business records upon the demand of an FBI agent, with no judicial review or oversight. This section would permit the use of administrative subpoenas rather than an application to a court to get any business records under FISA. An administrative subpoena is a piece of paper signed by an investigator. There is no judicial review, no standard of justification, not oversight.

Sec. 157. Miscellaneous national-security authorities

Allows much greater access to banking, credit, and other consumer records in counter-intelligence investigations - The Fair Credit Reporting Act, the Financial Right to Privacy Act, and the Electronic Communications Privacy Act allow access to credit records, financial records, and telephone and Internet communication records, for counterintelligence investigations - but only if there is specific and articulable evidence that the consumer is an agent of a foreign power. ATA removes this essential requirement, mandating disclosure of this sensitive consumer data simply if an FBI official certifies that they are needed for a counterintelligence investigation. This is a major change of basic privacy legislation.

Section 158. Disclosure of educational records

Amends the law protecting education records to permit access to them. While this might be justified in terrorism cases, the provision covers all cases involving “national security” and is far too sweeping.

Section 159. Presidential Authority.

Does not appear to permit judicial challenge to seizure of property. At the very least, there must be such opportunity. A second provision allows the use of secret evidence. Use of such evidence, if ever permitted, must be on a much higher standard than that the information is properly classified, as provided here. The government must be required to persuade a court that the disclosure to the party would result in imminent and serious harm and the court must require the government to provide sanitized information to the party.

Sec. 351. Single-Jurisdiction Search Warrants for Terrorism.

Allows any magistrate in the country to issue an order to seize evidence anywhere in the country - The concept of jurisdiction has due process importance. Traditionally, search orders are limited to the scope of a the issuing judge's jurisdiction. Sec. 351 allows a judge in a district where activities related to terrorism have occurred to issue search warrants with effect anywhere in the county, raising similar concerns about due process.

Sec. 352. Notice.

Allows secret searches through delayed notice for all warrants or court orders. For any warrant or court order to search or seize property relating to a federal criminal offense, notice of the search or seizure could be delayed if it could interfere with lawful investigations. Notice is a bedrock Fourth Amendment protection from mistaken or abusive searches and

seizures. Delayed notice has been allowed in only the most extraordinary circumstances, such as wiretapping, and only with substantial judicial supervision. Section 352 represents a major erosion of this key Fourth Amendment requirement of notice.

Other new surveillance authorities granted to the government would include:

- the ability to seize voicemail messages with a warrant rather than a wiretap order (Sec. 102);
- allows the disclosure of wiretapping information to any executive branch employee - potentially millions of people. (Sec. 103)
- allows interception of "computer trespasser" communications with the permission of the operator of a protected computer (Sec. 106)
- allows subpoenas for records of electronic communications to also demand the credit card or bank account number of the subject of the subpoena (Sec. 107)
- allows emergency disclosure of electronic communications without a judicial order in situations of immediate danger of death or serious injury (Sec. 110).

Taken together, these changes to the law would erode already weak protections for individual privacy on the Internet. They risk increased surveillance and disclosure of the online activities of many U.S. citizens. They could impose new costs on industry, as Internet companies are forced to comply with a range of new demands for information from the government. And they risk eroding public trust in and chilling use of the information infrastructure that has become such an essential tool for promoting commerce, communication, and democratic values.

What Congress Should Do

- **Hold hearings.** Congress should have at least some investigation before passing sweeping new surveillance laws that will alter the individual privacy rights for years to come.
- **Act carefully.** Congress should take care not to sacrifice precious constitutional freedoms, particularly without a clear relationship to the goal of countering terrorism.
- **Focus on real efforts to enhance computer security.** None of the provisions of the ATA address the core issue of how to provide better security in our increasingly important IT infrastructure. Computer security experts have for years highlighted the difficult task of making infrastructure security a higher priority for the Internet. As a starting point, the Federal government has a tremendous job to do in keeping its own house in order, and should also focus on what it can do to facilitate better security in the infrastructure.

For further information, contact:

Jim Dempsey, jdempsey@cdt.org
Alan Davidson, abd@cdt.org
Mike Godwin, godwin@cdt.org
(202) 637-9800

