Privacy from Government
November 15, 2005

- Electronic Communications Privacy Act, as amended by USA PATRIOT Act (read the summaries; the full text of the statutes is included at the end for your convenience, but is not required)
- *Katz v. United States*, 389 U.S. 347 (1967); *Smith v. Maryland*, 442 U.S. 735 (1979); *Kyllo v. United States*, 533 U.S. 27 (2001)
- *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994)
- *Doe v. Ashcroft*, 04-Civ-2614 (S.D.N.Y. Sept. 28, 2004)
- Barton Gellman, "The FBI's Secret Scrutiny," *Washington Post*, Nov. 6, 2005 <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366_pf.html>

Optional further reading

- Deirdre Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1565 (2004)
- Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 46-52 (2004)
- Orin S. Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother that Isn't*, 2003 Nw. U. L. Rev. 607, 616-18 (2003)

The Fourth Amendment anchors our right to privacy from government intrusion:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The meaning of that guarantee has varied with the state of technology, however. Courts must translate the Constitution's text in application to "search" technology unknown to the Framers. Further, as the technology evolves, so do our understandings of it and the "reasonable expectations of privacy" in technologically mediated activities.

The Supreme Court's decisions in *Katz v. United States*, *Smith v. Maryland*, and *Kyllo v. United States* illustrate some of the back-and-forth tugs of technology and privacy, as well as giving us analytical tools to apply to newer Internet technologies. Along with the sweeping pronouncements of constitutional interpretation, we also face more specific questions of statutory application. Even the most recently updated statutes will rarely be a perfect fit with the technology to which they apply, while older law can look like a square peg to a round hole.

Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986), comprised three titles. Title I amended the 1968 federal wiretap statute to cover electronic communications. Title II of ECPA created a new chapter of the criminal code dealing with access to stored communications and transaction records,

commonly known as the "Stored Communications Act" or "SCA." Title III of the ECPA covers pen registers and trap/trace devices.

Wiretap Act

ECPA, Title I, 18 U.S.C. §§ 2510 et seq. ("Wiretap Act") makes it unlawful to listen to or observe the contents of a private communication without the permission of at least one party to the communication and regulates real-time electronic surveillance in federal criminal investigations. 18 U.S.C. §§ 2510-2522 was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is generally (if confusingly) known as "Title III".

Stored Communications Act

ECPA Title II, 18 U.S.C. §§ 2701 et seq. ("Stored Communications Act") generally prohibits the disclosure of the content of electronically stored communications. The Act does not prohibit disclosure of user information to non-government entities.

The Stored Communications Act also strictly limits the information that an electronic communication service may provide to the government. A government entity generally must provide a subpoena, warrant or court order to obtain information about a user that is stored by the communication service provider. The USA PATRIOT Act, see below, amended these provisions to permit disclosure of such information to the government if the service provider has a good faith belief that there is an imminent danger of death or serious physical injury.

Pen/Trap Statute

The Pen Registers and Trap and Trace Devices chapter of Title 18 ("the Pen/Trap statute"), 18 U.S.C. §§ 3121-3127 governs pen registers and trap and trace devices. A "pen register" is a device that records the numbers dialed for outgoing calls made from the target phone. A trap and trace device captures the numbers of calls made to the target phone.

Computer Fraud and Abuse Act

The **Computer Fraud and Abuse Act** ("CFAA"), 18 U.S.C. § 1030 , provides a cause of action against one who, inter alia, "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication." 18 U.S.C. § 1030(a)(2)(C), (g).

The civil remedy extends to "[a]ny person who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g) (emphasis added). The Homeland Security Act, see below, increased the penalties and prison terms for violations of the CFAA.

USA PATRIOT Act

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), PL 107-56. Passed in the wake of the 9/11 terrorist attacks, the controversial Act expands the type of information to which law enforcement officials may obtain access and permits service providers to divulge the contents of communications in emergencies.

1. Section 210 increases the types of information to which law enforcement officials may obtain access by requiring them to meet only the lowest ECPA standard; types of information covered include records of session times and durations, temporary network addresses, and means and source of payments, including credit card and bank account numbers.

2. Section 212 of the Act permits service providers to voluntarily release the contents of communications if they reasonably believe that "an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay." This provision was further modified by the Homeland Security Act to increase the number of governmental agencies to which service providers may disclose communications and to soften the standard by which communications can be disclosed to a "good faith" belief from a "reasonable belief."
3. Section 214 of the Act significantly expands the FBI's electronic surveillance powers under the Foreign Intelligence Surveillance Act (FISA), as well as lowering the standards under which the secret FISA court can authorize the FBI to spy on your phone and Internet communications. In particular, Section 214 makes it easier for the FBI to install "pen registers" and "trap-and-trace devices" (collectively, "pen-traps") in order to monitor the communications of citizens who are not suspected of any terrorism or espionage activities.
4. Section 215 allows the FBI secretly to order anyone to turn over business records or any other "tangible things," so long as the FBI tells the secret Foreign Intelligence Surveillance Act (FISA) court that the information sought is "for an authorized investigation...to protect against international terrorism or clandestine intelligence activities." These demands for records come with a "gag order" prohibiting the recipient from telling anyone, ever, that they received a Section 215 order.
5. Section 217 permits service providers to "invite" law enforcement to assist in tracking and intercepting a computer trespasser's communications.

EFF analysis of the provisions of the USA PATRIOT Act. <http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php>

Homeland Security Act

The Homeland Security Act of 2002, PL 107-296. Provisions of Section 896 and Section 225 ("The Cyber Security Enhancement Act") of the Homeland Security Act increase prison time and penalties for violations of the CFAA, prohibit Internet advertising of illegal surveillance devices, and allow law enforcement agencies to make pen register/trap and trace installations without a court order in the case of "national security interests" or an attack on a protected computer as defined by the CFAA.

The Homeland Security Act Section 225 expanded the power of PATRIOT Section 212 by 1) lowering the relevant standard from "reasonable belief" of a life-threatening emergency to a "good faith belief," 2) allowing communications providers to use the emergency exception to disclose your data to any government entity, not just law enforcement, and 3) dropping the requirement that the threat to life or limb be immediate.

The flip side of privacy concerns is the government worry that the Internet enables criminals to communicate undetected, reducing the effectiveness of offline wiretaps and physical searches. In response, Congress passed the Communications Assistance to Law Enforcement Act ("CALEA") in 1994. CALEA defines the obligation of

telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. As the AskCALEA FAQ describes:

Who must be CALEA-compliant?

All telecommunications carriers as defined by Section 102(8) of CALEA. Basically, this includes all entities engaged in the transmission or switching of wire or electronic communications as a common carrier for hire.

What is "call-identifying information?"

Section 102(2) of CALEA defines call-identifying information as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."

What is "call content?"

Defined in 18 U.S.C. 2510(8) it is an intercept "when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communications."

What is a "safe harbor" under CALEA?

Section 107(a)(2) of CALEA contains a "safe harbor" provision, stating that "[a] telecommunications carrier shall be found to be in compliance with the assistance capability requirements under Section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with Section 106 if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the FCC under subsection (b), to meet the requirements of Section 103."

What is J-STD-025?

Subcommittee TR-45.2 of the Telecommunications Industry Association (TIA), along with Committee T1 of the Alliance for Telecommunications Industry Solutions, developed interim standard J-STD-025 to serve as a CALEA standard for wireline, cellular, and broadband PCS carriers and manufacturers. The standard defines services and features required by wireline, cellular, and broadband PCS carriers to support lawfully-authorized electronic surveillance, and specifies interfaces necessary to deliver intercepted communications and call-identifying information to a law enforcement agency.

What are the Punch List technical requirements?

On August 30, 1999, the FCC found that J-STD-025 was deficient in certain technical respects and remanded the standard to TR-45.2 for revision. The additional requirements (commonly referred to as "punch list" items) must be implemented June 30, 2002, and are stated in the FCC Third Report and Order 99-230, and the Order on Remand, FCC 02-108 as:

> 1) Provide the content of subject-initiated conference calls supported by the subject's service (including the call content of parties on hold).
>
> 2) Identify the active parties of a multiparty call.
>
> 3) Provide access to all dialing and signaling information available from the subject including a subject's use of features (such as the use of flash-hook and other feature keys).
>
> 4) Notify the law enforcement agency when a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy).
>
> 5) Provide timing information to correlate call-identifying information with the call content of a communications interception.
>
> 6) Provide digits dialed by a subject after the initial call "cut-through" is completed to another car

Current debate centers on the application of CALEA tappability requirements to non-traditional telecommunications carriers such as Voice Over Internet Protocol (VOIP) providers whose services may be used to substitute for telephone service. What does it mean to require “VOIP providers” to comply with CALEA?

Katz v. United States, 389 U.S. 347 (1967)

MR. JUSTICE STEWART delivered the opinion of the Court.

The petitioner was convicted in the District Court for the Southern District of California under an eight-count indictment charging him with transmitting wagering information by telephone from Los Angeles to Miami and Boston, in violation of a federal statute. At trial the Government was permitted, over the petitioner's objection, to introduce evidence of the petitioner's end of telephone conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls. In affirming his conviction, the Court of Appeals rejected the contention that the recordings had been obtained in violation of the Fourth Amendment, because "[t]here was no physical entrance into the area occupied by [the petitioner]." We granted certiorari in order to consider the constitutional questions thus presented.

…The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye - it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

The Government contends, however, that the activities of its agents in this case should not be tested by Fourth Amendment requirements, for the surveillance technique they employed involved no physical penetration of the telephone booth from which the petitioner placed his calls. It is true that the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry, *Olmstead v. United States*, 277 U.S. 438, 457 , 464, 466; *Goldman v. United States*, 316 U.S. 129, 134 -136, for that Amendment was thought to limit only searches and seizures of tangible property. But "[t]he premise that property interests control the right of the Government to search and seize has been discredited." *Warden v. Hayden*, 387 U.S. 294, 304 . Thus, although a closely divided Court supposed in Olmstead that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested…. Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people - and not simply "areas" - against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.

We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.

...Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored "the procedure of antecedent justification . . . that is central to the Fourth Amendment," a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case. Because the surveillance here failed to meet that condition, and because it led to the petitioner's conviction, the judgment must be reversed.

Smith v. Maryland, 442 U.S. 735 (1979)

MR. JUSTICE BLACKMUN delivered the opinion of the Court.

[Petitioner Smith was suspected in a robbery. Without a warrant, police requested the telephone company to install a pen register at its central offices to record the numbers dialed from the telephone at Smith's home. Evidence from the pen register showed a call to the victim's home, and Smith was tried and convicted. Smith sought to suppress "all fruits derived from the pen register" on the ground that the police had failed to secure a warrant prior to its installation. The Maryland courts denied his exclusion request, and the Supreme Court granted *certiorari*.]

…In determining whether a particular form of government-initiated electronic surveillance is a "search" within the meaning of the Fourth Amendment, our lodestar is Katz v. United States, 389 U.S. 347 (1967). …

Consistently with Katz, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a "justifiable," a "reasonable," or a "legitimate expectation of privacy" that has been invaded by government action…. This inquiry, as Mr. Justice Harlan aptly noted in his Katz concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy," 389 U.S., at 361 - whether, in the words of the Katz majority, the individual has shown that "he seeks to preserve [something] as private." The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as `reasonable,'" - whether, in the words of the Katz majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances. …

[Petitioner claims] that, notwithstanding the absence of a trespass, the State, as did the Government in Katz, infringed a "legitimate expectation of privacy" that petitioner held. Yet a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications. This Court recently noted:

> "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed - a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." …

Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone. This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize,

moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud, and preventing violations of law." *United States v. New York Tel. Co.*, 434 U.S., at 174 -175. Electronic equipment is used not only to keep billing records of toll calls, but also "to keep a record of all calls dialed from a telephone which is subject to a special rate structure." *Hodge v. Mountain States Tel. & Tel. Co.*, 555 F.2d 254, 266 (9th Cir. 1977) (concurring opinion). Pen registers are regularly employed "to determine whether a home phone is being used to conduct a business, to check for a defective dial, or to check for overbilling." …

Although most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls. … Most phone books tell subscribers, on a page entitled "Consumer Information," that the company "can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls."… Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

…[E]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as `reasonable.'" *Katz v. United States*, 389 U.S., at 361 . This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. e.g., *United States v. Miller*, 425 U.S., at 442 -444…. In Miller, for example, the Court held that a bank depositor has no "legitimate `expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business." 425 U.S., at 442 . The Court explained:

> "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." Id., at 443.

Because the depositor "assumed the risk" of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.
This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would

reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.

…We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not "legitimate." The installation and use of a pen register, consequently, was not a "search," and no warrant was required. The judgment of the Maryland Court of Appeals is affirmed.

[Footnote 1] "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." United States v. New York Tel. Co., 434 U.S. 159, 161 n. 1 (1977). A pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached. United States v. Giordano, 416 U.S. 505, 549 n. 1 (1974) (opinion concurring in part and dissenting in part). See also United States v. New York Tel. Co., 434 U.S., at 162 .

Mr. JUSTICE STEWART, with whom MR. JUSTICE BRENNAN joins, dissenting.
I am not persuaded that the numbers dialed from a private telephone fall outside the constitutional protection of the Fourth and Fourteenth Amendments.
In Katz v. United States, 389 U.S. 347, 352 , the Court acknowledged the "vital role that the public telephone has come to play in private communication[s]." The role played by a private telephone is even more vital, and since Katz it has been abundantly clear that telephone conversations carried on by people in their homes or offices are fully protected by the Fourth and Fourteenth Amendments. As the Court said in United States v. United States District Court, 407 U.S. 297, 313 , "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." (Footnote omitted.)
Nevertheless, the Court today says that those safeguards do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes. But that observation no more than describes the basic nature of telephone calls. A telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service. The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled "to assume that the words he utters into the mouthpiece will not be broadcast to the world." *Katz v. United States, supra*, at 352.

…The numbers dialed from a private telephone - although certainly more prosaic than the conversation itself - are not without "content." Most private telephone subscribers may

have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.

Kyllo v. United States, 533 U.S. 27 (2001).
Justice SCALIA.

[Petitioner Kyllo sought the exclusion of marijuana plants discovered when thermal imaging technology showed one side of his house to be significantly warmer than the other, consistent with the use of heat lamps to grow marijuana.]

… It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. For example, as the cases discussed above make clear, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. See *Ciraolo*, *supra*, at 215. The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

The *Katz* test--whether the individual has an expectation of privacy that society is prepared to recognize as reasonable--has often been criticized as circular, and hence subjective and unpredictable. See 1 W. LaFave, Search and Seizure §2.1(d), pp. 393-394 (3d ed. 1996); Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 S. Ct. Rev. 173, 188; *Carter*, *supra*, at 97 (S*calia, J.*, concurring). But see *Rakas*, *supra*, at 143-144, n. 12. While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences are at issue, in the case of the search of the interior of homes--the prototypical and hence most commonly litigated area of protected privacy--there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," *Silverman*, 365 U. S., at 512, constitutes a search--at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.

The Government maintains, however, that the thermal imaging must be upheld because it detected "only heat radiating from the external surface of the house."… But just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house-and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house. We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology--including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude,

the rule we adopt must take account of more sophisticated systems that are already in use or in development. …

…Limiting the prohibition of thermal imaging to "intimate details" would not only be wrong in principle; it would be impractical in application, failing to provide "a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment," *Oliver* v. *United States*, 466 U. S. 170, 181 (1984). To begin with, there is no necessary connection between the sophistication of the surveillance equipment and the "intimacy" of the details that it observes--which means that one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful. The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath--a detail that many would consider "intimate"; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on. We could not, in other words, develop a rule approving only that through-the-wall surveillance which identifies objects no smaller than 36 by 36 inches, but would have to develop a jurisprudence specifying which home activities are "intimate" and which are not. And even when (if ever) that jurisprudence were fully developed, no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up "intimate" details--and thus would be unable to know in advance whether it is constitutional.

…We have said that the Fourth Amendment draws "a firm line at the entrance to the house," *Payton*, 445 U. S., at 590. That line, we think, must be not only firm but also bright--which requires clear specification of those methods of surveillance that require a warrant. While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no "significant" compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward.

"The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens." *Carroll* v. *United States*, 267 U. S. 132, 149 (1925).
Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.

Since we hold the Thermovision imaging to have been an unlawful search, it will remain for the District Court to determine whether, without the evidence it provided, the search warrant issued in this case was supported by probable cause--and if not, whether there is any other basis for supporting admission of the evidence that the search pursuant to the warrant produced.

Steve Jackson Games, Inc. v. United States Secret Service,
36 F.3d 457 (5th Cir. 1994)

RHESA HAWKINS BARKSDALE, Circuit Judge:

The narrow issue before us is whether the seizure of a computer, used to operate an electronic bulletin board system, and containing private electronic mail which had been sent to (stored on) the bulletin board, but not read (retrieved) by the intended recipients, constitutes an unlawful intercept under the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*, as amended by Title I of the Electronic Communications Privacy Act of 1986, …

Appellant Steve Jackson Games, Incorporated (SJG), publishes books, magazines, role-playing games, and related products. Starting in the mid-1980s, SJG operated an electronic bulletin board system, called "Illuminati" (BBS), from one of its computers. SJG used the BBS to post public information about its business, games, publications, and the role-playing hobby; to facilitate play-testing of games being developed; and to communicate with its customers and free-lance writers by electronic mail (E-mail).

Central to the issue before us, the BBS also offered customers the ability to send and receive private E-mail. Private E-mail was stored on the BBS computer's hard disk drive temporarily, until the addressees "called" the BBS (using their computers and modems) and read their mail. After reading their E-mail, the recipients could choose to either store it on the BBS computer's hard drive or delete it. In February 1990, there were 365 BBS users. Among other uses, appellants Steve Jackson, Elizabeth McCoy, William Milliken, and Steffan O'Sullivan used the BBS for communication by private E-mail.

…On February 28, 1990, Agent Foley applied for a warrant to search SJG's premises and Blankenship's residence for evidence of violations of 18 U.S.C. §§ 1030 (proscribes interstate transportation of computer access information) and 2314 (proscribes interstate transportation of stolen property). A search warrant for SJG was issued that same day, authorizing the seizure of, *inter alia*, [computer hardware, software, and documents].

The next day, March 1, the warrant was executed by the Secret Service, including Agents Foley and Golden. Among the items seized was the computer which operated the BBS. At the time of the seizure, 162 items of unread, private E-mail were stored on the BBS, including items addressed to the individual appellants. Despite the Secret Service's denial, the district court found that Secret Service personnel or delegates read and deleted the private E-mail stored on the BBS.

Appellants filed suit in May 1991 against, among others, the Secret Service and the United States, claiming, *inter alia*, violations of the Privacy Protection Act, 42 U.S.C. § 2000aa, *et seq*; the Federal Wiretap Act, as amended by Title I of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2521 (proscribes, *inter alia*, the intentional interception of electronic communications); and Title II of the ECPA, 18 U.S.C. §§ 2701-2711 (proscribes, *inter alia*, intentional access, without authorization, to stored electronic communications). …

The district court held that the Secret Service violated the Privacy Protection Act, and awarded actual damages of $51,040 to SJG; and that it violated Title II of the ECPA by seizing stored electronic communications without complying with the statutory provisions, and awarded the statutory damages of $1,000 to each of the individual appellants. And, it awarded appellants $195,000 in attorneys' fees and approximately $57,000 in costs. But, it held that the Secret Service did not "intercept" the E-mail in violation of Title I of the ECPA, 18 U.S.C. § 2511(1)(a), because its acquisition of the contents of the electronic communications was not contemporaneous with the transmission of those communications.

As stated, the sole issue is a very narrow one: whether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an "intercept" proscribed by 18 U.S.C. § 2511(1)(a).

Section 2511 was enacted in 1968 as part of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, often referred to as the Federal Wiretap Act. Prior to the 1986 amendment by Title I of the ECPA, it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications. In relevant part, § 2511(1)(a) proscribes "intentionally intercept[ing] ... any wire, oral, or electronic communication", unless the intercept is authorized by court order or by other exceptions not relevant here. Section 2520 authorizes, *inter alia,* persons whose electronic communications are intercepted in violation of § 2511 to bring a civil action against the interceptor for actual damages, or for statutory damages of $10,000 per violation or $100 per day of the violation, whichever is greater. 18 U.S.C. § 2520.

The Act 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." 18 U.S.C. § 2510(4). …
Prior to the 1986 amendment by the ECPA, the Wiretap Act defined "intercept" as the "aural acquisition" of the contents of wire or oral communications through the use of a device. 18 U.S.C. § 2510(4) (1968). The ECPA amended this definition to include the "aural *or other* acquisition of the contents of ... wire, *electronic,* or oral communications...." 18 U.S.C. § 2510(4) (1986) (emphasis added for new terms). The significance of the addition of the words "or other" in the 1986 amendment to the definition of "intercept" becomes clear when the definitions of "aural" and "electronic communication" are examined; electronic communications (which include the non-voice portions of wire communications), as defined by the Act, cannot be acquired aurally. *Webster's Third New International Dictionary* (1986) defines "aural" as "of or relating to the ear" or "of or relating to the sense of hearing". *Id.* at 144. And, the Act defines "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. § 2510(18). This definition is extremely important for purposes of understanding the definition of a "wire communication", which is defined by the Act 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) ... *and such term includes any electronic storage of such communication.*

18 U.S.C. § 2510(1) (emphasis added). In contrast, as noted, an "electronic communication" is defined 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, photoelectronic or photooptical system ... but does not include ... any wire or oral communication...." 18 U.S.C. § 2510(12) (emphasis added).

Critical to the issue before us is the fact that, unlike the definition of "wire communication", *the definition of "electronic communication" does not include electronic storage of such communications. See* 18 U.S.C. § 2510(12). See note 4, *supra.* "Electronic storage" is defined 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) (emphasis added). The E-mail in issue was in "electronic storage". Congress' use of the word "transfer" in the definition of "electronic communication", and its omission in that definition of the phrase "any electronic storage of such communication" (part of the definition of "wire communication") reflects that Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage".

[FN6. Wire and electronic communications are subject to different treatment under the Wiretap Act. The Act's exclusionary rule, 18 U.S.C. § 2515, applies to the interception of wire communications, including such communications in electronic storage, *see* 18 U.S.C. § 2510(1), but not to the interception of electronic communications…. And, the types of crimes that may be investigated by means of surveillance directed at electronic communications, 18 U.S.C. § 2516(3) ("any federal felony"), are not as limited as those that may be investigated by means of surveillance directed at wire or oral communications. *See* 18 U.S.C. § 2516(1) (specifically listed felonies).

FN7. Stored wire communications are subject to different treatment than stored electronic communications. Generally, a search warrant, rather than a court order, is required to obtain access to the contents of a stored electronic communication. *See* 18 U.S.C. § 2703(a). But, compliance with the more stringent requirements of § 2518, including obtaining a court order, is necessary to obtain access to a stored wire communication, because § 2703 expressly applies only to stored *electronic* communications, not to stored *wire* communications.]

...Title II generally proscribes unauthorized access to stored wire or electronic communications. Section 2701(a) provides:

> Except as provided in subsection (c) of this section whoever--
> (1) intentionally accesses 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* shall be punished....

18 U.S.C. § 2701(a) (emphasis added).

As stated, the district court found that the Secret Service violated § 2701 when it

> intentionally accesse[d] without authorization a facility [the computer] through which an electronic communication service [the BBS] is provided ... and thereby obtain[ed] [and] prevent[ed] authorized access [by appellants] to a [n] ... electronic communication while it is in electronic storage in such system. 18 U.S.C. § 2701(a).

The Secret Service does not challenge this ruling. We find no indication in either the Act or its legislative history that Congress intended for conduct that is clearly prohibited by Title II to furnish the basis for a civil remedy under Title I as well.

First, the substantive and procedural requirements for authorization to intercept electronic communications are quite different from those for accessing stored electronic communications. For example, a governmental entity may gain access to the contents of electronic communications that have been in electronic storage for less than 180 days by obtaining a warrant. *See* 18 U.S.C. § 2703(a). But there are more stringent, complicated requirements for the interception of electronic communications; a court order is required. *See* 18 U.S.C. § 2518.

Second, other requirements applicable to the interception of electronic communications, such as those governing minimization, duration, and the types of crimes that may be investigated, are not imposed when the communications at issue are not in the process of being transmitted at the moment of seizure, but instead are in electronic storage. For example, a court order authorizing interception of electronic communications is required to include a directive that the order shall be executed "in such a way as to minimize the interception of communications not otherwise subject to interception". 18 U.S.C. § 2518(5). Title II of the ECPA does not contain this requirement for warrants authorizing access to stored electronic communications. The purpose of the minimization requirement is to implement "the constitutional obligation of avoiding, to the greatest possible extent, seizure of conversations which have no relationship to the crimes being investigated or the purpose for which electronic surveillance has been authorized". James G. Carr, *The Law of Electronic Surveillance,* § 5.7(a) at 5-28 (1994).

Obviously, when intercepting electronic communications, law enforcement officers cannot know in advance which, if any, of the intercepted communications will be relevant to the crime under investigation, and often will have to obtain access to the contents of the communications in order to make such a determination. Interception thus poses a significant risk that officers will obtain access to communications which have no relevance to the investigation they are conducting. That risk is present to a lesser degree,

and can be controlled more easily, in the context of stored electronic communications, because, as the Secret Service advised the district court, technology exists by which relevant communications can be located without the necessity of reviewing the entire contents of all of the stored communications. For example, the Secret Service claimed (although the district court found otherwise) that it reviewed the private E-mail on the BBS by use of key word searches.

Next, as noted, court orders authorizing an intercept of electronic communications are subject to strict requirements as to duration. An intercept may not be authorized "for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days". 18 U.S.C. § 2518(5). There is no such requirement for access to stored communications.

Finally, as also noted, the limitations as to the types of crimes that may be investigated through an intercept, *see* 18 U.S.C. § 2516, have no counterpart in Title II of the ECPA. *See, e.g.*, 18 U.S.C. § 2703(d) (court may order a provider of electronic communication service or remote computing service to disclose to a governmental entity the contents of a stored electronic communication on a showing that the information sought is "relevant to a legitimate law enforcement inquiry").

In light of the substantial differences between the statutory procedures and requirements for obtaining authorization to intercept electronic communications, on the one hand, and to gain access to the contents of stored electronic communications, on the other, it is most unlikely that Congress intended to require law enforcement officers to satisfy the more stringent requirements for an intercept in order to gain access to the contents of stored electronic communications….

Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004)
(on appeal as *Doe v. Gonzales*)

Plaintiffs in this case challenge the constitutionality of 18 U.S.C. § 2709 ("§ 2709"). That statute authorizes the Federal Bureau of Investigation ("FBI") to compel Communications firms, such as internet service providers ("ISPs") or telephone companies, to produce certain customer records whenever the FBI certifies that those records are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." The FBI's demands under § 2709 are issued in the form of national security letters ("NSLs"), which constitute a unique form of administrative subpoena cloaked in secrecy and pertaining to national security issues. The statute bars all NSL recipients from ever disclosing that the FBI has issued an NSL.

The lead plaintiff, called "John Doe" ("Doe") for purposes of this litigation, is described in the complaint as an internet access firm that received an NSL. The other plaintiffs are the American Civil Liberties Union ("ACLU") and the American Civil Liberties Union Foundation, which is also acting as counsel to Doe (collectively with Doe, "Plaintiffs"). Plaintiffs contend that § 2709's broad subpoena power violates the First, Fourth and Fifth Amendments of the United States Constitution, and that the non-disclosure provision violates the First Amendment. They argue that § 2709 is unconstitutional on its face and as applied to the facts of this case. Plaintiffs' main complaints are that, first, § 2709 gives the FBI extraordinary and unchecked power to obtain private information without any form of judicial process, and, second, that § 2709's non-disclosure provision burdens speech categorically and perpetually, without any case-by-case judicial consideration of whether that speech burden is justified. The parties have cross-moved for summary judgment on all claims. …

A. DOE'S RECEIPT OF AN NSL

After receiving a call from an FBI agent informing him that he would be served with an NSL, Doe received a document, printed on FBI letterhead, which stated that, "pursuant to Title 18, United States Code (U.S.C.), Section 2709" Doe was "directed" to provide certain information to the Government. As required by the terms of § 2709, in the NSL the FBI "certified that the information sought [was] relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." Doe was "further advised" that § 2709(c) prohibited him, or his officers, agents, or employees, "from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions." Doe was "requested to provide records responsive to [the] request personally" to a designated individual, and to not transmit the records by mail or even mention the NSL in any telephone conversation.

After a subsequent conversation with the same FBI agent, Doe decided to consult ACLU lawyers…. Doe has not complied with the NSL request, and has instead engaged counsel to bring the present lawsuit.

B. § 2709 IN GENERAL

…§ 2709 authorizes the FBI to issue NSLs to compel communications firms to produce certain customer records whenever the FBI certifies, that those records are relevant to an authorized international terrorism or counterintelligence investigation, and the statute also categorically bars NSL recipients from disclosing the inquiry. In relevant part, it states:

> (a) Duty to provide. -- A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.
>
> (b) Required certification. -- The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may --
>
> (1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
>
> (2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.
>
> (c) Prohibition of certain disclosure. -- No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

Subsection (d) limits the FBI's ability to disseminate information collected from an NSL, and subsection (e) requires the FBI to periodically report to Congress about its use of NSLs.

Section 2709 is one of only a handful of statutes authorizing the Government to issue NSLs. … In each case, the NSL statutes categorically bar the NSL recipient or its employees or agents from ever disclosing the Government's inquiry. As stated, NSLs are distinguished from other administrative subpoenas in that NSLs pertain to national security issues and are cloaked in secrecy. …

C. LEGISLATIVE HISTORY

Section 2709 was enacted as part of Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), which sought to "protect privacy interests" in "stored wire and electronic communications" while also "protecting the Government's legitimate law enforcement needs." …

Generally speaking, Title II (as amended) allows the Government to obtain stored electronic communications information without the subscriber's permission only through compulsory process, such as a subpoena, warrant, or court order. Section 2709 is a notable exception to these privacy protections because it permits the FBI to request records upon a mere self-certification -- issued to the ISP or telephone company, not to the subscriber or to any court, -- that its request complies with the statutory requirements. As first enacted, § 2709 required electronic communication service providers to produce "subscriber information," "toll billing records information," or "electronic communication transactional records," upon the FBI's internal certification that (1) the information was "relevant to an authorized foreign counterintelligence investigation" and that (2) there were "specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains [was] a foreign power or an agent of a foreign power."…

The… most recent major revision to § 2709 occurred in October 2001, as part of the USA PATRIOT Act of 2001 ("Patriot Act"). In short, the Patriot Act removed the previous requirement that § 2709 inquiries have a nexus to a foreign power, replacing that prerequisite with a broad standard of relevance to investigations of terrorism or clandestine intelligence activities. In hearings before the House Judiciary Committee on September 24, 2001, the Administration submitted the following explanation for the proposed change:

> NSL authority requires both a showing of relevance and a showing of links to an "agent of a foreign power.." In this respect, [it is] substantially more demanding than the analogous criminal authorities, which require only a certification of relevance. Because the NSLs require documentation of the facts supporting the "agent of a foreign power" predicate and because they require the signature of a high-ranking official at FBI headquarters, they often take months to be issued. This is in stark contrast to criminal subpoenas, which can be used to obtain the same information, and are issued rapidly at the local level. In many cases, counterintelligence and counterterrorism investigations suffer substantial delays while waiting for NSLs to be prepared, returned from headquarters, and served. The section would streamline the process of obtaining NSL authority . . . .

The House Judiciary Committee agreed that "such delays are unacceptable" and stated in its October 11, 2001, report that the Patriot Act would "harmonize[]" § 2709 "with existing criminal law where an Assistant United States Attorney may issue a grand jury subpoena for all such records in a criminal case."

D. NSLs AND OTHER INFORMATION-GATHERING AUTHORITY

It is instructive to place the Government's NSL authority in the context of other means by which the Government gathers information of the type covered by § 2709 because Congress (in passing and amending the NSL statutes) and the parties here (in contesting § 2709's constitutionality) have, drawn analogies to those other authorities as grounds for or against its validity. The relationship of § 2709 to other related statutes supplies a backdrop for assessing congressional intent and judging the validity of the law on its face and as applied. In addition, an analysis of these analogous information-gathering methods indicates that NSLs such as the ones authorized by § 2709 provide fewer procedural protections to the recipient than any other information-gathering technique the Government employs to procure information similar to that which it obtains pursuant to § 2709.

…

IV. DISCUSSION

A. SECTION 2709, AS DRAFTED, RAISES SERIOUS CONSTITUTIONAL QUESTIONS

…The NSL statutes, particularly § 2709, present interpretive challenges in at least three respects, the first two of which have a direct bearing on the motions now before the Court. First, while two of the NSL statutes explicitly state that an NSL recipient may disclose the Government's inquiry to persons whose assistance is necessary to comply with the demands of the NSL, the other statutes, including § 2709, appear by their telltale silence on that point, to preclude any disclosures. None of the statutes explain whether consulting an attorney constitutes disclosure, even where an attorney's assistance may be necessary for a recipient to comply with an NSL, and none of the statutes states whether the ban on disclosure may ever be lifted by a court. Second, the statutes contain no explicit provision for the Government to seek judicial enforcement of an NSL against a recipient who refuses to comply, nor is there any provision expressly authorizing an NSL recipient to affirmatively challenge, administratively or judicially, the propriety of an NSL request. Third, there is no explicit provision in the statutes imposing penalties against a person who fails to comply with an NSL.

…Several bills pending in Congress, including H.R. 3179, demonstrate Congress's and the Government's recognition that the NSL statutes could have been drafted with greater particularity and uniformity. H.R. 3279 would address two of the issues listed above by explicitly providing for judicial enforcement of NSLs and by imposing criminal penalties

of up to five years' imprisonment for persons who unlawfully disclose that they have received an NSL. …

As explained below, even if the Court were to agree with the Government that § 2709 should be read to allow: (1) an NSL recipient to consult with an attorney and others necessary to enable compliance with the letter; and (2) an NSL recipient to challenge, or the Government to enforce, an NSL in court, the Court would still hold that the statute; as currently applied by the FBI, exerts an undue coercive effect on NSL recipients. The form language of the NSL served upon Doe, preceded by an FBI phone call, directed him to personally provide the information to the FBI, prohibited him, his officers, agents or employees, from disclosing the existence of the NSL to anyone, and made no mention of the availability of judicial review to quash or otherwise modify the NSL or the secrecy mandated by the letter. Nor did the FBI inform Doe personally that any such judicial review of the issuance of the NSL or the secrecy attaching to it was available. The Court concludes that, when combined, these provisions and practices essentially force the reasonable NSL recipient to immediately comply with the request. This lack of effective process, at least as applied, entails issues far too fundamental for the Court to read as having been sufficiently addressed in the operation of § 2709 in this case. In the court's judgment, as further elaborated below, that absence renders § 2709, as applied, unconstitutional, in violation of the Fourth Amendment.

B. AS APPLIED HERE, SECTION 2709 LACKS PROCEDURAL PROTECTIONS NECESSARY TO VINDICATE CONSTITUTIONAL RIGHTS

1. Section 2709 And The Fourth Amendment

- - - - - - - - - - - - - - Footnotes - - - - - - - - - - - - - -

To be clear, the Fourth Amendment rights at issue here belong to the person or entity receiving the NSL, not to the person or entity to whom the subpoenaed records pertain. Individuals possess a limited Fourth Amendment interest in records which they voluntarily convey to a third party. See Smith, 442 U.S. at 742-46; Miller, 425 U.S. at 440-43. Nevertheless, as discussed below, many potential NSL recipients may have particular interests in resisting an NSL, e.g., because they have contractually obligated themselves to protect the anonymity of their subscribers or because their own rights are uniquely implicated by what they regard as an intrusive and secretive NSL regime. For example, since the definition of "wire or electronic communication service provider," 18 § 2709(a), is so vague, the statute could (and may currently) be used to seek subscriber lists or other information from an association that also provides electronic communication services (e.g., email addresses) to its members, or to seek records from libraries that many, including the amici appearing in this proceeding, fear will chill speech and use of these invaluable public institutions. Fear that § 2709 may be used as a tool to gain sensitive information from libraries, has led both houses of Congress to introduce bills intended to exclude libraries from the ambit of § 2709. See S. 1709, Security and Freedom Assured ("SAFE") Act of 2003, 108th Cong. § 5 (2003) (proposing to amend § 2709(a) to state that a "library shall not be treated as a wire or electronic communication service provider for purposes of this section"); H.R. 3352,

108th Cong. § 5 (2003) (same).
- - - - - - - - - - - - End Footnotes- - - - - - - - - - - - -

The Fourth Amendment prohibits the Government from conducting "unreasonable searches and seizures," which generally means that any search or seizure must be performed pursuant to a valid warrant based upon probable cause. As the Second Circuit has declared: "It is fundamental that governmental searches and seizures without warrant or probable cause are per se unreasonable under the Fourth Amendment unless they fall within one of the Amendment's few established and well-delineated exceptions." The Fourth Amendment's protection against unreasonable searches applies to administrative subpoenas, even though issuing a subpoena does not involve a literal physical intrusion or search. In so doing, the Supreme Court explained that the Fourth Amendment is not "confined literally to searches and seizures as such, but extends as well to the orderly taking under compulsion of process."

…Plaintiffs contend that § 2709 violates this Fourth Amendment process-based guarantee because it gives the FBI alone the power to issue as well as enforce its own NSLs, instead of contemplating some form of judicial review. Although Plaintiffs appear to concede that the statute does not authorize the FBI to literally enforce the terms of an NSL by, for example, unilaterally seizing documents or imposing fines, Plaintiffs contend that § 2709 has the practical effect of coercing compliance.

Specifically, Plaintiffs stress that the statute has no provision for judicial enforcement or review, and that theoretically any judicial review an NSL recipient sought would violate the express terms of the non-disclosure provision. For example, if an NSL recipient thought that an NSL request was unreasonable or otherwise unlawful - because, for instance, the underlying investigation was not duly "authorized," was initiated "solely on the basis of activities protected by the first amendment to the Constitution of the United States," or did not involve "international terrorism or clandestine intelligence activities," as § 2709 demands - he would have no specific statute under which to challenge the request. More fundamentally, the literal terms of the non-disclosure provision would bar the recipient from even consulting an attorney to file such a challenge. Even if he were to challenge the NSL on his own, the recipient would necessarily have to disclose the fact of the NSL's issuance to the clerk of court and to the presiding judge, again, in violation of the literal terms of the non-disclosure provision.

Rather than dispute the Plaintiffs' interpretation of the relevant constitutional doctrine, the Government's response to these arguments endeavors to heavily repair the statute, essentially by splicing together a string of judicially-sanctioned implications, glosses, or outright patchwork of the various gaps Congress left in the statute, whether inadvertently or purposefully. First, as discussed above, the Government claims that the statute implicitly affords an NSL recipient the opportunity to challenge an NSL on the same terms as would be available to any other subpoena recipient, i.e., to either resist the Government's enforcement action, or to affirmatively file a motion to quash. Second, the Government reads the statute to implicitly permit disclosure to an attorney in connection with such a challenge. Third, the government would recognize an additional exception for

disclosure to other officers, employees, or agents whose assistance may be reasonably necessary for the recipient to comply with the NSL request.

The path that, according to the Government, would lead to the above "correct" reading of § 2709 is as follows. First, concerning the judicial enforcement issue, § 2709 is conspicuously silent on how the Government's demand for records is to be enforced. Plaintiffs concede that § 2709 does not authorize the FBI to resort to "self-help" in enforcing the statute, thus leaving the possibilities that enforcement falls to either the court system, to no one at all, or, worse yet, to other forms of administrative pressures and extra-legal methods that such congressional silences and statutory lacunae may be prone to invite. Following the Government's theory, it is inconceivable that Congress intended compliance with § 2709 to be a mere courtesy in light of § 2709's mandatory phrases, such as "duty" and "shall comply." The obvious purpose of the statute - to obtain important records quickly - would be eviscerated, the argument goes, if an NSL recipient could treat the NSL as if it were a piece of junk mail to be tossed in the trash can and ignored without consequence. Furthermore, courts have long recognized the "sharp distinction between agency power to issue subpoenas and judicial power to enforce them." Accordingly, the Government concludes that it would make sense that an NSL, which is in the family of administrative subpoenas, would follow that ordinary course. …. As the Supreme Court has also instructed, the courts "cannot press statutory construction 'to the point of disingenuous evasion' even to avoid a constitutional question." … [T]he more and the deeper the interstices in a law a judge is called upon to fill, the more what the enterprise demands is not construction of a statute but its emendation by the court, effectively an exercise of judicial legislation in order to repair and rescue the enactment by furnishing through this back channel the missing terms Congress itself did not provide.

…Despite these severe reservations, in the final analysis the Court need not resolve Plaintiffs' facial challenge to § 2709 on Fourth Amendment grounds for two reasons. First, even if the Court were to accept that the FBI's authority to issue and enforce NSLs pursuant to § 2709 means what the Government says it means, the Court's inquiry would not end there with a ruling in favor of the Government. Investing those provisions with the reading the Government accords them does not address the Plaintiffs' distinct claim that in practice § 2709 in all or the vast majority of actual cases, by virtue of the statute's unwarranted application by the FBI, operates otherwise. The Court concludes that the operation of § 2709 renders it unconstitutional, notwithstanding that, at least in a theoretical sense, a possible reading of portions of the statute as the Government propounds, through extensive judicial tinkering with its silences, may be posited to withstand a Fourth Amendment facial challenge. In particular, deficiencies in the application of § 2709 pertain to the very core issues -- access to legal advice and availability of judicial process to enforce and contest the law -- upon which Plaintiffs' Fourth Amendment facial challenge is grounded. Because the Court agrees that those protections are vital to satisfy Fourth Amendment standards, it finds the manner in which § 2709 has been applied unwarranted.

The crux of the problem is that the form NSL, like the one issued in this case, which is preceded by a personal call from an FBI agent, is framed in imposing language on FBI letterhead and which, citing the authorizing statute, orders a combination of disclosure in person and in complete secrecy, essentially coerces the reasonable recipient into immediate compliance. Objectively viewed, it is improbable that an FBI summons invoking the authority of a certified "investigation to protect against international terrorism or clandestine intelligence activities," and phrased in tones sounding virtually as biblical commandment, would not be perceived with some apprehension by an ordinary person and therefore elicit passive obedience from a reasonable NSL recipient. The full weight of this ominous writ is especially felt when the NSL's plain language, in a measure that enhances its aura as an expression of public will, prohibits disclosing the issuance of the NSL to "any person." Reading such strictures, it is also highly unlikely that an NSL recipient reasonably would know that he may have a right to contest the NSL, and that a process to do so may exist through a judicial proceeding.

Because neither the statute, nor an NSL, nor the FBI agents dealing with the recipient say as much, all but the most mettlesome and undaunted NSL recipients would consider themselves effectively barred from consulting an attorney or anyone else who might advise them otherwise, as well as bound to absolute silence about the very existence of the NSL. Furthermore, it is doubtful that an NSL recipient, not necessarily a lawyer, would be willing to undertake any creative exercises in statutory construction to somehow reach the Government's proposed reading of § 2709, especially because that construction is not apparent from the plain language of the statute, the NSL itself, or accompanying government communications, and any penalties for noncompliance or disclosure are also unspecified in the NSL or in the statute. For the reasonable NSL recipient confronted with the NSL's mandatory language and the FBI's conduct related to the NSL, resistance is not a viable option.

The evidence in this case bears out the hypothesis that NSLs work coercively in this way. The ACLU obtained, via the Freedom of Information Act ("FOIA"), and presented to the Court in this proceeding, a document listing all the NSLs the Government issued from October 2001 through January 2003. Although the entire substance of the document is redacted, it is apparent that hundreds of NSL requests were made during that period. Because § 2709 has been available to the FBI since 1986 (and its financial records counterpart in RFPA since 1978), the Court concludes that there must have been hundreds more NSLs issued in that long time span. The evidence suggests that, until now, none of those NSLs was ever challenged in any court. First, the Department of Justice explicitly informed the House Judiciary Committee in May 2003 that there had been no challenges to the propriety or legality of any NSLs. Second, the Government's evidence in this case conspicuously lacks any suggestion either that the Government has ever had to resort to a judicial enforcement proceeding for any NSL, or that any recipient has ever resisted an NSL request in such a proceeding or via any motion to quash.

To be sure, the Court recognizes that many other reasons may exist to explain the absence of challenges to NSLs: the communications provider who receives the NSL ordinarily

would have little incentive to contest the NSL on the subscriber's behalf; the standard of review for administrative subpoenas similar to NSLs is so minimal that most such NSLs would likely be upheld in court; litigating these issues is expensive; and many citizens may feel a civic duty to help the FBI's investigation and thus may willingly comply. Nevertheless, the Court finds it striking that, in all the years during which the FBI has been serving NSLs, the evidence suggests that, until now, no single NSL recipient has ever sought to quash such a directive. The Court thus concludes that in practice NSLs are essentially unreviewable because, as explained, given the language and tone of the statute as carried into the NSL by the FBI, the recipient would consider himself, in virtually every case, obliged to comply, with no other option but to immediately obey and stay quiet.
...Here, the Court concludes it would be … naive to conclude that § 2709 NSLs, given their commandeering warrant, do anything short of coercing all but the most fearless NSL recipient into immediate compliance and secrecy. …

Recognizing from the preceding discussion the reality that § 2709 effectively keeps § 2709 NSLs out of litigation altogether, the Court concludes that supplying a judicial gloss to § 2709 but failing to address the practical effects of the unparalleled level of secrecy and coercion fostered by the FBI's implementation of the statute would be completely academic. That is, the Court is reluctant to fashion a "remedy" which has no effect beyond being printed in the Federal Supplement.
…
Accordingly, the Court concludes that § 2709, as applied here, must be invalidated because in all but the exceptional case it has the effect of authorizing coercive searches effectively immune from any judicial process, in violation of the Fourth Amendment. The Court next turns to other reasons that compel the more drastic conclusion that § 2709 must be invalidated on its face. First, however, the Court examines Plaintiffs' arguments that § 2709 violates communications service subscribers' First Amendment rights. It concludes that the absence of meaningful judicial review created by § 2709's coercive implementation may also lead to violations of subscribers' own constitutional rights.

2. NSLs May Violate ISP Subscribers' Rights.

Plaintiffs have focused on the possibility that § 2709 could be used to infringe subscribers' First Amendment rights of anonymous speech and association. Though it is not necessary to precisely define the scope of ISP subscribers' First Amendment rights, the Court concludes that § 2709 may, in a given case, violate a subscriber's First Amendment privacy rights, as well as other legal rights, if judicial review is not readily available to an ISP that receives an NSL. This conclusion buttresses the Court's holding that, at least as applied, § 2709 does not permit sufficient judicial review to preserve individual subscribers' rights, where impairment of such rights may be implicated by a given NSL.

The Supreme Court has recognized the First Amendment right to anonymous speech at least since Talley v. California, which invalidated a California law requiring that handbills distributed to the public contain certain identifying information about the

source of the handbills. The Court stated that the "identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression" The Supreme Court has also invalidated identification requirements pertaining to persons distributing campaign literature, persons circulating petitions for state ballot initiatives, and persons engaging in door-to-door religious advocacy.

In a related doctrine, the Supreme Court has held that "compelled disclosure, of affiliation with groups engaged in advocacy" amounts to a "restraint on freedom of association" where disclosure could expose the members to "public hostility." Laws mandating such disclosures will be upheld only where the Government interest is compelling.
The Court concludes that such First Amendment rights may be infringed by application of § 2709 in a given case. For example, the FBI theoretically could issue to a political campaign's computer systems operator a § 2709 NSL compelling production of the names of all persons who have email addresses through the campaign's computer systems. The FBI theoretically could also issue an NSL under § 2709 to discern the identity of someone whose anonymous online web log, or "blog," is critical of the Government. Such inquiries might be beyond the permissible scope of the FBI's power under § 2709 because the targeted information might not be relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, or because the inquiry might be conducted solely on the basis of activities protected by the First Amendment. These prospects only highlight the potential danger of the FBI's self-certification process and the absence of judicial oversight.

Other rights may also be violated by the disclosure contemplated by the statute; the statute's reference to "transactional records" creates ambiguity regarding the scope of the information required to be produced by the NSL recipient. If the recipient -- who in the NSL is called upon to exercise judgment in determining the extent to which complying materials constitute transactional records rather than content -- interprets the NSL broadly as requiring production of all e-mail header information, including subject lines, for example, some disclosures conceivably may reveal information protected by the subscriber's attorney-client privilege, e.g., communication with an attorney where the subject line conveys privileged or possibly incriminating information. Indeed, the practical absence of judicial review may lead ISPs to disclose information that is protected from disclosure by the NSL statute itself, such as in a case where the NSL was initiated solely in retaliation for the subscriber's exercise of his First Amendment rights, as prohibited by § 2709(b)(1)-(2). Only a court would be able to definitively construe the statutory and First Amendment rights at issue in the "First Amendment retaliation" provision of the statute, and to strike a proper balance among those interests.

The Government asserts that disclosure of the information sought under § 2709 could not violate a subscriber's rights (and thus demands no judicial process) because the information which a § 2709 NSL seeks has been voluntarily conveyed to the ISP who receives the NSL. According to the Government, an internet speaker relinquishes any interest in any anonymity, and any protected claim to that information, as soon as he releases his identity and other information to his ISP. In support of its position, the

Government cites the Supreme Court's holding that, at least in the Fourth Amendment context involving the Government installing a pen register or obtaining bank records, when a person voluntarily conveys information to third parties, he assumes the risk that the information will be turned over to the Government.

The Court rejects the Government's reasoning. Every court that has addressed the issue has held that individual internet subscribers have a right to engage in anonymous internet speech, though anonymity may be trumped in a given case by other concerns. No court has adopted the Government's argument here that anonymous internet speech or associational activity ceases to be protected because a third-party ISP is in possession of the identifying information.

Moreover, the Court notes that the implications of the Government's position are profound. Anonymous internet speakers could be unmasked merely by an administrative, civil, or trial subpoena, or by any state or local disclosure regulation directed at their ISP, and the Government would not have to provide any heightened justification for revealing the speaker. The same would be true for attempts to compile membership lists by seeking the computerized records of an organization which uses a third-party electronic communications provider. Considering, as is undisputed here, the importance of the internet as a forum for speech and association, the Court rejects the invitation to permit the rights of internet anonymity and association to be placed at such grave risk.

The Court reaches this conclusion by determining that NSLs issued pursuant to § 2709 may seek information about or indirectly obtained from subscribers that may be protected from disclosure by the First Amendment, or other rights-protecting constitutional provisions or statutes. Echoing the Supreme Court's observation that "differences in the characteristics of new media justify differences in the First Amendment standards applied to them," the Court concludes that even though Smith and Miller might suggest that there is no First Amendment interest at stake in compelling the disclosure by telephone companies and banks of certain transactional information derived from customer records, in deciding this case the Court must take account of the unique features of internet communications that may warrant application of different rules. The Court is persuaded that, for First Amendment purposes, internet records of the type obtained via a § 2709 NSL could differ substantially from transactional bank or phone records.

The evidence on the record now before this Court demonstrates that the information available through a § 2709 NSL served upon an ISP could easily be used to disclose vast amounts of anonymous speech and associational activity. For instance, § 2709 imposes a duty to provide "electronic communication transactional records," a phrase which, though undefined in the statute, certainly encompasses a log of email addresses with whom a subscriber has corresponded and the web pages that a subscriber visits. Those transactional records can reveal, among other things, the anonymous message boards to which a person logs on or posts, the electronic newsletters to which he subscribes, and the advocacy websites he visits. Moreover, § 2709 imposes a duty on ISPs to provide the names and addresses of subscribers, thus enabling the Government to specifically identify

someone who has written anonymously on the internet. As discussed above, given that an NSL recipient is directed by the FBI to turn over all information "which you consider to be an electronic communication transactional record," the § 2709 NSL could also reasonably be interpreted by an ISP to require, at minimum, disclosure of all e-mail header information, including subject lines.

In stark contrast to this potential to compile elaborate dossiers on internet users, the information obtainable by a pen register is far more limited. As the Supreme Court in Smith was careful to note:
[Pen registers] disclose only the telephone numbers that have been dialed -- a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.

The Court doubts that the result in Smith would have been the same if a pen register operated as a key to the most intimate details and passions of a person's private life.

The more apt Supreme Court case for evaluating the assumption of risk argument at issue here is Katz v. United States, the seminal decision underlying both Smith and Miller. Katz held that the Fourth Amendment's privacy protections applied where the Government wiretapped a telephone call placed from a public phone booth. Especially noteworthy and pertinent to this case is the Supreme Court's remark that: "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." The Supreme Court also stated that a person entering a phone booth who "shuts the door behind him" is "surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," and held that, "to read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."

Applying that reasoning to anonymous internet speech and associational activity is relatively straightforward. A person who signs onto an anonymous forum under a pseudonym, for example, is essentially "shut[ting] the door behind him,"and is surely entitled to a reasonable expectation that his speech, whatever form the expression assumes, will not be accessible to the Government to be broadcast to the world absent appropriate legal process. To hold otherwise would ignore the role of the internet as a remarkably powerful forum for private communication and association. Even the Government concedes here that the internet is an "important vehicle for the free exchange of ideas and facilitates associations."

To be sure, the Court is keenly mindful of the Government's reminder that the internet may also serve as a vehicle for crime. The Court equally recognizes that circumstances exist in which the First Amendment rights of association and anonymity must yield to a

more compelling Government interest in obtaining records from internet firms. To this end, the Court re-emphasizes that it does not here purport to set forth the scope of these First Amendment rights in general, or define them in this or any other case. The Court holds only that suchfundamental rights are certainly implicated in some cases in which the Government may employ § 2709 broadly to gather information, thus requiring that the process incorporate the safeguards of some judicial review to ensure that if an infringement of those rights is asserted, they are adequately protected through fair process in an independent neutral tribunal. Because the necessary procedural protections are wholly absent here, the Court finds on this ground additional cause for invalidating § 2709 as applied.

C. CONSTITUTIONALITY OF THE NON-DISCLOSURE PROVISION

Finally, the Court turns to the issue of whether the Government may properly enforce § 2709(c), the non-disclosure provision, against Doe or any other person who has previously received an NSL. Section 2709(c) states: "No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."

A threshold question concerning this issue is whether, as Plaintiffs contend, § 2709(c) is subject to strict scrutiny as either a prior restraint on speech or a content-based speech restriction, or whether, as the Government responds, § 2709(c) is subject to the more relaxed judicial review of intermediate scrutiny. The difference is crucial. A speech restriction which is either content-based or which imposes a prior restraint on speech is presumed invalid and may be upheld only if it is "narrowly tailored to promote a compelling Government interest." If "less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve," then the speech restriction is not narrowly tailored and may be invalidated. Under intermediate scrutiny, a speech restriction may be upheld as long as "it advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests."

The Court agrees with Plaintiffs that § 2709(c) works as both a prior restraint on speech and as a content-based restriction, and hence, is subject to strict scrutiny.

…. The Government's argument …fails to recognize that even a viewpoint-neutral restriction can be content-based, if the restriction pertains to an entire category of speech. The Supreme Court has clearly expressed this principle: "The First Amendment's hostility to content-based regulation extends not only to restrictions on particular viewpoints, but also to prohibition of public discussion of an entire topic." Section 2709(c) prohibits any discussion of the first-hand experiences of NSL recipients, and of their officers, employees, and agents, and thus closes off that "entire topic" from public discourse. Those persons are forever barred from speaking to anyone about their knowledge and role in the underlying events pertaining to the issuance of an NSL, however substantively limited or temporally remote that role may be, even at a time when disclosure of the

occurrence of the investigation may have ceased to generate legitimate national security concerns and instead may hold historical or scholarly value then bearing relatively greater interest to the general public. The restriction would also categorically bar the recipient and its agents from ever discussing their roles even if other persons may be free to do so -- because, for example, the matter may have become public or the FBI itself may have revealed the information or publicly brought the investigation to closure. The absolute and permanent ban on disclosure § 2709(c) commands forecloses an objective weighing of these competing public policy interests by a neutral arbiter even as the relative merits of the respective claims may alter over time.

…[T]he Court …acknowledges that the Government's interest in protecting the integrity and efficacy of international terrorism and counterintelligence investigations is a compelling one. The Supreme Court has so acknowledged: "This Court has recognized the Government's 'compelling interest' in withholding national security information from unauthorized persons in the course of executive business." A suspected terrorist or foreign intelligence operative who is alerted that the Government is conducting an investigation may destroy evidence, create false leads, alert others, or otherwise take steps to avoid detection. More generally, such disclosures can reveal the Government's intelligence-gathering methods, from which foreign intelligence operatives or terrorists could learn better how to avoid detection.

Nonetheless, Plaintiffs contend that § 2709(c)'s categorical, perpetual, and automatic ban on disclosure is not a narrowly-tailored means to advance those legitimate public interests. Plaintiffs suggest that a more precisely-calibrated statute, which would equally advance the Government's compelling interests, would prohibit disclosure only on a case-by-case basis, for a limited time, and with prior judicial approval. Without detailing the degree of narrow tailoring which the First Amendment demands with respect to § 2709, the Court concludes that § 2709 is not sufficiently narrow.

…

Viewed from another perspective, however, the restraint imposed under § 2709(c) is as thorough as is conceivable. The statute permanently prohibits not only the recipient but its officers, employees or agents, from disclosing the NSL's existence to "any person," in every instance in which an NSL is issued and irrespective of the circumstances prevailing at any given point in time. In this respect, § 2709(c) as well as the other NSL statutes, are uniquely extraordinary. …[W]hen the Government conducts a secret investigation, it ordinarily must apply for a court order before restricting third-party participants from revealing the inquiry, and those restrictions are generally temporary.

….

Furthermore, these provisions are not quite as severe as those contained in the NSL statutes because, with one narrow exception for certain FISA surveillance orders, they apply in contexts in which a court authorizes the investigative method in the first place. Thus, even in these statutes, the silenced party, at least theoretically, would almost always have a forum in which to contest the continuing validity of the non-disclosure obligation or to seek a modified secrecy order. The FISA limits the potential for abuse in yet another way by requiring a clear connection to a foreign power and by sharply

limiting the degree to which any United States citizen may be subject to surveillance under a secret FISA order; such protections are not present in § 2709, particularly after the significant broadening of the statute's scope effectuated by the Patriot Act. The NSL statutes, including § 2709(c), thus stand virtually alone in providing for blanket secrecy entirely outside the context of judicial process.

In synthesizing the broad and narrow features of § 2709(c) explained above, and in considering how closely those features are tailored to the Government's compelling interests, the Government makes convincing points in showing that it would be consistent with the First Amendment to impose a certain amount of limited secrecy in many cases involving a § 2709 NSL. The Government also persuasively demonstrates how that secrecy, under certain circumstances, might continue for longer periods of time, consistent with the First Amendment. The Court acknowledges those arguments so far as they go, but concludes in the end that the Government cannot cast § 2709 -- a blunt agent of secrecy applying in perpetuity to all persons affected in every case -- as narrowly-tailored.

…

The Government's claim to perpetual secrecy surrounding the FBI's issuance of NSLs, by its theory as advanced here an authority neither restrained by the FBI's own internal discretion nor reviewable by any form of judicial process, presupposes a category of information, and thus a class of speech, that, for reasons not satisfactorily explained, must forever be kept from public view, cloaked by an official seal that will always overshadow the public's right to know. In general, as our sunshine laws and judicial doctrine attest, democracy abhors undue secrecy, in recognition that public knowledge secures freedom. Hence, an unlimited government warrant to conceal, effectively a form of secrecy per se, has no place in our open society. Such a claim is especially inimical to democratic values for reasons borne out by painful experience. Under the mantle of secrecy, the self-preservation that ordinarily impels our government to censorship and secrecy may potentially be turned on ourselves as a weapon of self-destruction. When withholding information from disclosure is no longer justified, when it ceases to foster the proper aims that initially may have supported confidentiality, a categorical and uncritical extension of non-disclosure may become the cover for spurious ends that government may then deem too inconvenient, inexpedient, merely embarrassing, or even illicit to ever expose to the light of day. At that point, secrecy's protective shield may serve not as much to secure a safe country as simply to save face.

-The Government does not deny that there are plausible situations in which little or no reason may remain for continuing the secrecy of the fact that an NSL was issued. To cite an example, a case may arise in which the Government's investigation has long since been completed and information about it has become public through Government sources or otherwise, in which the material obtained through an NSL revealed that there was no basis whatsoever to pursue the subject or target of the Government's investigation, or in which the disclosure may have been made by a person in the chain of information, such as an employee or agent of the NSL recipient, who was not informed in any way of the secrecy requirement. Section 2709(c) does not countenance the possibility that the FBI

could permit modification of the NSL's no-disclosure order even in those or any other similar situations no longer implicating legitimate national security interests and presenting factual or legal issues that any court could reasonably adjudicate. Bluntly stated, the statute simply does not allow for that balancing of competing public interests to be made by an independent tribunal at any point. In this regard, it is conceivable that "less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve." For instance, Congress could require the FBI to make at least some determination concerning need before requiring secrecy, and ultimately it could provide a forum and define at least some circumstances in which an NSL recipient could ask the FBI or a court for a subsequent determination whether continuing secrecy was still warranted.

…In response to this standard, the Government's main contention, quite understandably, is that international terrorism and counterintelligence investigations justify more secrecy than other types of investigations. The Court agrees with that basic point so far as it goes. However, under the exacting demands of the First Amendment, the argument does not carry far enough.

…

VI. CONCLUSION

To summarize, the Court concludes that the compulsory, secret, and unreviewable production of information required by the FBI's application of 18 U.S.C. § 2709 violates the Fourth Amendment, and that the non-disclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment. The Government is therefore enjoined from issuing NSLs under § 2709 or from enforcing the non-disclosure provision in this or any other case, but enforcement of the Court's judgment will be stayed pending appeal, or if no appeal is filed, for 90 days.

washingtonpost.com

The FBI's Secret Scrutiny

In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans

By Barton GellmanWashington Post Staff WriterSunday, November 6, 2005; A01

The FBI came calling in Windsor, Conn., this summer with a document marked for delivery by hand. On Matianuk Avenue, across from the tennis courts, two special agents found their man. They gave George Christian the letter, which warned him to tell no one, ever, what it said.

Under the shield and stars of the FBI crest, the letter directed Christian to surrender "all subscriber information, billing information and access logs of any person" who used a specific computer at a library branch some distance away. Christian, who manages digital records for three dozen Connecticut libraries, said in an affidavit that he configures his system for privacy. But the vendors of the software he operates said their databases can reveal the Web sites that visitors browse, the e-mail accounts they open and the books they borrow.

Christian refused to hand over those records, and his employer, Library Connection Inc., filed suit for the right to protest the FBI demand in public. The Washington Post established their identities -- still under seal in the U.S. Court of Appeals for the 2nd Circuit -- by comparing unsealed portions of the file with public records and information gleaned from people who had no knowledge of the FBI demand.

The Connecticut case affords a rare glimpse of an exponentially growing practice of domestic surveillance under the USA Patriot Act, which marked its fourth anniversary on Oct. 26. "National security letters," created in the 1970s for espionage and terrorism investigations, originated as narrow exceptions in consumer privacy law, enabling the FBI to review in secret the customer records of suspected foreign agents. The Patriot Act, and Bush administration guidelines for its use, transformed those letters by permitting clandestine scrutiny of U.S. residents and visitors who are not alleged to be terrorists or spies.

The FBI now issues more than 30,000 national security letters a year, according to government sources, a hundredfold increase over historic norms. The letters -- one of which can be used to sweep up the records of many people -- are extending the bureau's reach as never before into the telephone calls, correspondence and financial lives of ordinary Americans.

Issued by FBI field supervisors, national security letters do not need the imprimatur of a prosecutor, grand jury or judge. They receive no review after the fact by the Justice Department or Congress. The executive branch maintains only statistics, which are incomplete and confined to classified reports. The Bush administration defeated legislation and a lawsuit to require a public accounting, and has offered no example in which the use of a national security letter helped disrupt a terrorist plot.

The burgeoning use of national security letters coincides with an unannounced decision to deposit all the

information they yield into government data banks -- and to share those private records widely, in the federal government and beyond. In late 2003, the Bush administration reversed a long-standing policy requiring agents to destroy their files on innocent American citizens, companies and residents when investigations closed. Late last month, President Bush signed Executive Order 13388, expanding access to those files for "state, local and tribal" governments and for "appropriate private sector entities," which are not defined.

National security letters offer a case study of the impact of the Patriot Act outside the spotlight of political debate. Drafted in haste after the Sept. 11, 2001, attacks, the law's 132 pages wrought scores of changes in the landscape of intelligence and law enforcement. Many received far more attention than the amendments to a seemingly pedestrian power to review "transactional records." But few if any other provisions touch as many ordinary Americans without their knowledge.

Senior FBI officials acknowledged in interviews that the proliferation of national security letters results primarily from the bureau's new authority to collect intimate facts about people who are not suspected of any wrongdoing. Criticized for failure to detect the Sept. 11 plot, the bureau now casts a much wider net, using national security letters to generate leads as well as to pursue them. Casual or unwitting contact with a suspect -- a single telephone call, for example -- may attract the attention of investigators and subject a person to scrutiny about which he never learns.

A national security letter cannot be used to authorize eavesdropping or to read the contents of e-mail. But it does permit investigators to trace revealing paths through the private affairs of a modern digital citizen. The records it yields describe where a person makes and spends money, with whom he lives and lived before, how much he gambles, what he buys online, what he pawns and borrows, where he travels, how he invests, what he searches for and reads on the Web, and who telephones or e-mails him at home and at work.

As it wrote the Patriot Act four years ago, Congress bought time and leverage for oversight by placing an expiration date on 16 provisions. The changes involving national security letters were not among them. In fact, as the Dec. 31 deadline approaches and Congress prepares to renew or make permanent the expiring provisions, House and Senate conferees are poised again to amplify the FBI's power to compel the secret surrender of private records.

The House and Senate have voted to make noncompliance with a national security letter a criminal offense. The House would also impose a prison term for breach of secrecy.

Like many Patriot Act provisions, the ones involving national security letters have been debated in largely abstract terms. The Justice Department has offered Congress no concrete information, even in classified form, save for a partial count of the number of letters delivered. The statistics do not cover all forms of national security letters or all U.S. agencies making use of them.

"The beef with the NSLs is that they don't have even a pretense of judicial or impartial scrutiny," said

former representative Robert L. Barr Jr. (Ga.), who finds himself allied with the American Civil Liberties Union after a career as prosecutor, CIA analyst and conservative GOP stalwart. "There's no checks and balances whatever on them. It is simply some bureaucrat's decision that they want information, and they can basically just go and get it."

'A Routine Tool'

Career investigators and Bush administration officials emphasized, in congressional testimony and interviews for this story, that national security letters are for hunting terrorists, not fishing through the private lives of the innocent. The distinction is not as clear in practice.

Under the old legal test, the FBI had to have "specific and articulable" reasons to believe the records it gathered in secret belonged to a terrorist or a spy. Now the bureau needs only to certify that the records are "sought for" or "relevant to" an investigation "to protect against international terrorism or clandestine intelligence activities."

That standard enables investigators to look for conspirators by sifting the records of nearly anyone who crosses a suspect's path.

"If you have a list of, say, 20 telephone numbers that have come up . . . on a bad guy's telephone," said Valerie E. Caproni, the FBI's general counsel, "you want to find out who he's in contact with." Investigators will say, " 'Okay, phone company, give us subscriber information and toll records on these 20 telephone numbers,' and that can easily be 100."

Bush administration officials compare national security letters to grand jury subpoenas, which are also based on "relevance" to an inquiry. There are differences. Grand juries tend to have a narrower focus because they investigate past conduct, not the speculative threat of unknown future attacks. Recipients of grand jury subpoenas are generally free to discuss the subpoenas publicly. And there are strict limits on sharing grand jury information with government agencies.

Since the Patriot Act, the FBI has dispersed the authority to sign national security letters to more than five dozen supervisors -- the special agents in charge of field offices, the deputies in New York, Los Angeles and Washington, and a few senior headquarters officials. FBI rules established after the Patriot Act allow the letters to be issued long before a case is judged substantial enough for a "full field investigation." Agents commonly use the letters now in "preliminary investigations" and in the "threat assessments" that precede a decision whether to launch an investigation.

"Congress has given us this tool to obtain basic telephone data, basic banking data, basic credit reports," said Caproni, who is among the officials with signature authority. "The fact that a national security letter is a routine tool used, that doesn't bother me."

If agents had to wait for grounds to suspect a person of ill intent, said Joseph Billy Jr., the FBI's deputy

assistant director for counterterrorism, they would already know what they want to find out with a national security letter. "It's all chicken and egg," he said. "We're trying to determine if someone warrants scrutiny or doesn't."

Billy said he understands that "merely being in a government or FBI database . . . gives everybody, you know, neck hair standing up." Innocent Americans, he said, "should take comfort at least knowing that it is done under a great deal of investigative care, oversight, within the parameters of the law."

He added: "That's not going to satisfy a majority of people, but . . . I've had people say, you know, 'Hey, I don't care, I've done nothing to be concerned about. You can have me in your files and that's that.' Some people take that approach."

'Don't Go Overboard'

In Room 7975 of the J. Edgar Hoover Building, around two corners from the director's suite, the chief of the FBI's national security law unit sat down at his keyboard about a month after the Patriot Act became law. Michael J. Woods had helped devise the FBI wish list for surveillance powers. Now he offered a caution.

"NSLs are powerful investigative tools, in that they can compel the production of substantial amounts of relevant information," he wrote in a Nov. 28, 2001, "electronic communication" to the FBI's 56 field offices. "However, they must be used judiciously." Standing guidelines, he wrote, "require that the FBI accomplish its investigations through the 'least intrusive' means. . . . The greater availability of NSLs does not mean that they should be used in every case."

Woods, who left government service in 2002, added a practical consideration. Legislators granted the new authority and could as easily take it back. When making that decision, he wrote, "Congress certainly will examine the manner in which the FBI exercised it."

Looking back last month, Woods was struck by how starkly he misjudged the climate. The FBI disregarded his warning, and no one noticed.

"This is not something that should be automatically done because it's easy," he said. "We need to be sure . . . we don't go overboard."

One thing Woods did not anticipate was then-Attorney General John D. Ashcroft's revision of Justice Department guidelines. On May 30, 2002, and Oct. 31, 2003, Ashcroft rewrote the playbooks for investigations of terrorist crimes and national security threats. He gave overriding priority to preventing attacks by any means available.

Ashcroft remained bound by Executive Order 12333, which requires the use of the "least intrusive means" in domestic intelligence investigations. But his new interpretation came close to upending the

mandate. Three times in the new guidelines, Ashcroft wrote that the FBI "should consider . . . less intrusive means" but "should not hesitate to use any lawful techniques . . . even if intrusive" when investigators believe them to be more timely. "This point," he added, "is to be particularly observed in investigations relating to terrorist activities."

'Why Do You Want to Know?'

As the Justice Department prepared congressional testimony this year, FBI headquarters searched for examples that would show how expanded surveillance powers made a difference. Michael Mason, who runs the Washington field office and has the rank of assistant FBI director, found no ready answer.

"I'd love to have a made-for-Hollywood story, but I don't have one," Mason said. "I am not even sure such an example exists."

What national security letters give his agents, Mason said, is speed.

"I have 675 terrorism cases," he said. "Every one of these is a potential threat. And anything I can do to get to the bottom of any one of them more quickly gets me closer to neutralizing a potential threat."

Because recipients are permanently barred from disclosing the letters, outsiders can make no assessment of their relevance to Mason's task.

Woods, the former FBI lawyer, said secrecy is essential when an investigation begins because "it would defeat the whole purpose" to tip off a suspected terrorist or spy, but national security seldom requires that the secret be kept forever. Even mobster "John Gotti finds out eventually that he was wiretapped" in a criminal probe, said Peter Swire, the federal government's chief privacy counselor until 2001. "Anyone caught up in an NSL investigation never gets notice."

To establish the "relevance" of the information they seek, agents face a test so basic it is hard to come up with a plausible way to fail. A model request for a supervisor's signature, according to internal FBI guidelines, offers this one-sentence suggestion: "This subscriber information is being requested to determine the individuals or entities that the subject has been in contact with during the past six months."

Edward L. Williams, the chief division counsel in Mason's office, said that supervisors, in practice, "aren't afraid to ask . . . 'Why do you want to know?' " He would not say how many requests, if any, are rejected.

'The Abuse Is in the Power Itself'

Those who favor the new rules maintain -- as Sen. Pat Roberts (R-Kan.), chairman of the Senate Select Committee on Intelligence, put it in a prepared statement -- that "there has not been one substantiated allegation of abuse of these lawful intelligence tools."

What the Bush administration means by abuse is unauthorized use of surveillance data -- for example, to blackmail an enemy or track an estranged spouse. Critics are focused elsewhere. What troubles them is not unofficial abuse but the official and routine intrusion into private lives.

To Jeffrey Breinholt, deputy chief of the Justice Department's counterterrorism section, the civil liberties objections "are eccentric." Data collection on the innocent, he said, does no harm unless "someone [decides] to act on the information, put you on a no-fly list or something." Only a serious error, he said, could lead the government, based on nothing more than someone's bank or phone records, "to freeze your assets or go after you criminally and you suffer consequences that are irreparable." He added: "It's a pretty small chance."

"I don't necessarily want somebody knowing what videos I rent or the fact that I like cartoons," said Mason, the Washington field office chief. But if those records "are never used against a person, if they're never used to put him in jail, or deprive him of a vote, et cetera, then what is the argument?"

Barr, the former congressman, said that "the abuse is in the power itself."

"As a conservative," he said, "I really resent an administration that calls itself conservative taking the position that the burden is on the citizen to show the government has abused power, and otherwise shut up and comply."

At the ACLU, staff attorney Jameel Jaffer spoke of "the profound chilling effect" of this kind of surveillance: "If the government monitors the Web sites that people visit and the books that they read, people will stop visiting disfavored Web sites and stop reading disfavored books. The FBI should not have unchecked authority to keep track of who visits [al-Jazeera's Web site] or who visits the Web site of the Federalist Society."

Links in a Chain

Ready access to national security letters allows investigators to employ them routinely for "contact chaining."

"Starting with your bad guy and his telephone number and looking at who he's calling, and [then] who they're calling," the number of people surveilled "goes up exponentially," acknowledged Caproni, the FBI's general counsel.

But Caproni said it would not be rational for the bureau to follow the chain too far. "Everybody's connected" if investigators keep tracing calls "far enough away from your targeted bad guy," she said. "What's the point of that?"

One point is to fill government data banks for another investigative technique. That one is called "link

analysis," a practice Caproni would neither confirm nor deny.

Two years ago, Ashcroft rescinded a 1995 guideline directing that information obtained through a national security letter about a U.S. citizen or resident "shall be destroyed by the FBI and not further disseminated" if it proves "not relevant to the purposes for which it was collected." Ashcroft's new order was that "the FBI shall retain" all records it collects and "may disseminate" them freely among federal agencies.

The same order directed the FBI to develop "data mining" technology to probe for hidden links among the people in its growing cache of electronic files. According to an FBI status report, the bureau's office of intelligence began operating in January 2004 a new Investigative Data Warehouse, based on the same Oracle technology used by the CIA. The CIA is generally forbidden to keep such files on Americans.

Data mining intensifies the impact of national security letters, because anyone's personal files can be scrutinized again and again without a fresh need to establish relevance.

"The composite picture of a person which emerges from transactional information is more telling than the direct content of your speech," said Woods, the former FBI lawyer. "That's certainly not been lost on the intelligence community and the FBI."

Ashcroft's new guidelines allowed the FBI for the first time to add to government files consumer data from commercial providers such as LexisNexis and ChoicePoint Inc. Previous attorneys general had decided that such a move would violate the Privacy Act. In many field offices, agents said, they now have access to ChoicePoint in their squad rooms.

What national security letters add to government data banks is information that no commercial service can lawfully possess. Strict privacy laws, for example, govern financial and communications records. National security letters -- along with the more powerful but much less frequently used secret subpoenas from the Foreign Intelligence Surveillance Court -- override them.

'What Happens in Vegas'

The bureau displayed its ambition for data mining in an emergency operation at the end of 2003.

The Department of Homeland Security declared an orange alert on Dec. 21 of that year, in part because of intelligence that hinted at a New Year's Eve attack in Las Vegas. The identities of the plotters were unknown.

The FBI sent Gurvais Grigg, chief of the bureau's little-known Proactive Data Exploitation Unit, in an audacious effort to assemble a real-time census of every visitor in the nation's most-visited city. An average of about 300,000 tourists a day stayed an average of four days each, presenting Grigg's team with close to a million potential suspects in the ensuing two weeks.

A former stockbroker with a degree in biochemistry, Grigg declined to be interviewed. Government and private sector sources who followed the operation described epic efforts to vacuum up information.

An interagency task force began pulling together the records of every hotel guest, everyone who rented a car or truck, every lease on a storage space, and every airplane passenger who landed in the city. Grigg's unit filtered that population for leads. Any link to the known terrorist universe -- a shared address or utility account, a check deposited, a telephone call -- could give investigators a start.

"It was basically a manhunt, and in circumstances where there is a manhunt, the most effective way of doing that was to scoop up a lot of third party data and compare it to other data we were getting," Breinholt said.

Investigators began with emergency requests for help from the city's sprawling hospitality industry. "A lot of it was done voluntary at first," said Billy, the deputy assistant FBI director.

According to others directly involved, investigators turned to national security letters and grand jury subpoenas when friendly persuasion did not work.

Early in the operation, according to participants, the FBI gathered casino executives and asked for guest lists. The MGM Mirage company, followed by others, balked.

"Some casinos were saying no to consent [and said], 'You have to produce a piece of paper,' " said Jeff Jonas, chief scientist at IBM Entity Analytics, who previously built data management systems for casino surveillance. "They don't just market 'What happens in Vegas stays in Vegas.' They want it to be true."

The operation remained secret for about a week. Then casino sources told Rod Smith, gaming editor of the Las Vegas Review-Journal, that the FBI had served national security letters on them. In an interview for this article, one former casino executive confirmed the use of a national security letter. Details remain elusive. Some law enforcement officials, speaking on the condition of anonymity because they had not been authorized to divulge particulars, said they relied primarily on grand jury subpoenas. One said in an interview that national security letters may eventually have been withdrawn. Agents encouraged voluntary disclosures, he said, by raising the prospect that the FBI would use the letters to gather something more sensitive: the gambling profiles of casino guests. Caproni declined to confirm or deny that account.

What happened in Vegas stayed in federal data banks. Under Ashcroft's revised policy, none of the information has been purged. For every visitor, Breinholt said, "the record of the Las Vegas hotel room would still exist."

Grigg's operation found no suspect, and the orange alert ended on Jan. 10, 2004."The whole thing washed out," one participant said.

'Of Interest to President Bush'

At around the time the FBI found George Christian in Connecticut, agents from the bureau's Charlotte field office paid an urgent call on the chemical engineering department at North Carolina State University in Raleigh. They were looking for information about a former student named Magdy Nashar, then suspected in the July 7 London subway bombing but since cleared of suspicion.

University officials said in interviews late last month that the FBI tried to use a national security letter to demand much more information than the law allows.

David T. Drooz, the university's senior associate counsel, said special authority is required for the surrender of records protected by educational and medical privacy. The FBI's first request, a July 14 grand jury subpoena, did not appear to supply that authority, Drooz said, and the university did not honor it. Referring to notes he took that day, Drooz said Eric Davis, the FBI's top lawyer in Charlotte, "was focused very much on the urgency" and "he even indicated the case was of interest to President Bush."

The next day, July 15, FBI agents arrived with a national security letter. Drooz said it demanded all records of Nashar's admission, housing, emergency contacts, use of health services and extracurricular activities. University lawyers "looked up what law we could on the fly," he said. They discovered that the FBI was demanding files that national security letters have no power to obtain. The statute the FBI cited that day covers only telephone and Internet records.

"We're very eager to comply with the authorities in this regard, but we needed to have what we felt was a legally valid procedure," said Larry A. Neilsen, the university provost.

Soon afterward, the FBI returned with a new subpoena. It was the same as the first one, Drooz said, and the university still had doubts about its legal sufficiency. This time, however, it came from New York and summoned Drooz to appear personally. The tactic was "a bit heavy-handed," Drooz said, "the implication being you're subject to contempt of court." Drooz surrendered the records.

The FBI's Charlotte office referred questions to headquarters. A high-ranking FBI official, who spoke on the condition of anonymity, acknowledged that the field office erred in attempting to use a national security letter. Investigators, he said, "were in a big hurry for obvious reasons" and did not approach the university "in the exact right way."

'Unreasonable' or 'Oppressive'

The electronic docket in the Connecticut case, as the New York Times first reported, briefly titled the lawsuit *Library Connection Inc. v. Gonzales* . Because identifying details were not supposed to be left in the public file, the court soon replaced the plaintiff's name with "John Doe."

George Christian, Library Connection's executive director, is identified in his affidavit as "John Doe 2." In that sworn statement, he said people often come to libraries for information that is "highly sensitive, embarrassing or personal." He wanted to fight the FBI but feared calling a lawyer because the letter said he could not disclose its existence to "any person." He consulted Peter Chase, vice president of Library Connection and chairman of a state intellectual freedom committee. Chase -- "John Doe 1" in his affidavit -- advised Christian to call the ACLU. Reached by telephone at their homes, both men declined to be interviewed.

U.S. District Judge Janet C. Hall ruled in September that the FBI gag order violates Christian's, and Library Connection's, First Amendment rights. A three-judge panel heard oral argument on Wednesday in the government's appeal.

The central facts remain opaque, even to the judges, because the FBI is not obliged to describe what it is looking for, or why. During oral argument in open court on Aug. 31, Hall said one government explanation was so vague that "if I were to say it out loud, I would get quite a laugh here." After the government elaborated in a classified brief delivered for her eyes only, she wrote in her decision that it offered "nothing specific."

The Justice Department tried to conceal the existence of the first and only other known lawsuit against a national security letter, also brought by the ACLU's Jaffer and Ann Beeson. Government lawyers opposed its entry into the public docket of a New York federal judge. They have since tried to censor nearly all the contents of the exhibits and briefs. They asked the judge, for example, to black out every line of the affidavit that describes the delivery of the national security letter to a New York Internet company, including, "I am a Special Agent of the Federal Bureau of Investigation ('FBI')."

U.S. District Judge Victor Marrero, in a ruling that is under appeal, held that the law authorizing national security letters violates the First and Fourth Amendments.

Resistance to national security letters is rare. Most of them are served on large companies in highly regulated industries, with business interests that favor cooperation. The in-house lawyers who handle such cases, said Jim Dempsey, executive director of the Center for Democracy and Technology, "are often former prosecutors -- instinctively pro-government but also instinctively by-the-books." National security letters give them a shield against liability to their customers.

Kenneth M. Breen, a partner at the New York law firm Fulbright & Jaworski, held a seminar for corporate lawyers one recent evening to explain the "significant risks for the non-compliant" in government counterterrorism investigations. A former federal prosecutor, Breen said failure to provide the required information could create "the perception that your company didn't live up to its duty to fight terrorism" and could invite class-action lawsuits from the families of terrorism victims. In extreme cases, he said, a business could face criminal prosecution, "a 'death sentence' for certain kinds of companies."

The volume of government information demands, even so, has provoked a backlash. Several major

business groups, including the National Association of Manufacturers and the U.S. Chamber of Commerce, complained in an Oct. 4 letter to senators that customer records can "too easily be obtained and disseminated" around the government. National security letters, they wrote, have begun to impose an "expensive and time-consuming burden" on business.

The House and Senate bills renewing the Patriot Act do not tighten privacy protections, but they offer a concession to business interests. In both bills, a judge may modify a national security letter if it imposes an "unreasonable" or "oppressive" burden on the company that is asked for information.

'A Legitimate Question'

As national security letters have grown in number and importance, oversight has not kept up. In each house of Congress, jurisdiction is divided between the judiciary and intelligence committees. None of the four Republican chairmen agreed to be interviewed.

Roberts, the Senate intelligence chairman, said in a statement issued through his staff that "the committee is well aware of the intelligence value of the information that is lawfully collected under these national security letter authorities," which he described as "non-intrusive" and "crucial to tracking terrorist networks and detecting clandestine intelligence activities." Senators receive "valuable reporting by the FBI," he said, in "semi-annual reports [that] provide the committee with the information necessary to conduct effective oversight."

Roberts was referring to the Justice Department's classified statistics, which in fact have been delivered three times in four years. They include the following information: how many times the FBI issued national security letters; whether the letters sought financial, credit or communications records; and how many of the targets were "U.S. persons." The statistics omit one whole category of FBI national security letters and also do not count letters issued by the Defense Department and other agencies.

Committee members have occasionally asked to see a sampling of national security letters, a description of their fruits or examples of their contribution to a particular case. The Justice Department has not obliged.

In 2004, the conference report attached to the intelligence authorization bill asked the attorney general to "include in his next semiannual report" a description of "the scope of such letters" and the "process and standards for approving" them. More than a year has passed without a Justice Department reply.

"The committee chairman has the power to issue subpoenas" for information from the executive branch, said Rep. Zoe Lofgren (D-Calif.), a House Judiciary Committee member. "The minority has no power to compel, and . . . Republicans are not going to push for oversight of the Republicans. That's the story of this Congress."

In the executive branch, no FBI or Justice Department official audits the use of national security letters to

assess whether they are appropriately targeted, lawfully applied or contribute important facts to an investigation.

Justice Department officials noted frequently this year that Inspector General Glenn A. Fine reports twice a year on abuses of the Patriot Act and has yet to substantiate any complaint. (One investigation is pending.) Fine advertises his role, but there is a puzzle built into the mandate. Under what scenario could a person protest a search of his personal records if he is never notified?

"We do rely upon complaints coming in," Fine said in House testimony in May. He added: "To the extent that people do not know of anything happening to them, there is an issue about whether they can complain. So, I think that's a legitimate question."

Asked more recently whether Fine's office has conducted an independent examination of national security letters, Deputy Inspector General Paul K. Martin said in an interview: "We have not initiated a broad-based review that examines the use of specific provisions of the Patriot Act."

At the FBI, senior officials said the most important check on their power is that Congress is watching.

"People have to depend on their elected representatives to do the job of oversight they were elected to do," Caproni said. "And we think they do a fine job of it."

Researcher Julie Tate and research editor Lucy Shackelford contributed to this report.

ECPA Title I, Wiretap Act, 18 U.S.C. §§ 2510-2522

§ 2510. Definitions

As used in this chapter--

(1) "wire communication" means 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;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means 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.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--

> **(a)** any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;
>
> **(b)** a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means--

> **(a)** a judge of a United States district court or a United States court of appeals; and
>
> **(b)** a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" has the meaning given that term in section 3 of the Communications Act of 1934;
(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;
(12) "electronic communication" means 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, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who--

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;
(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;
(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not--

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means--

(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) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;
(19) "foreign intelligence information", for purposes of section 2517(6) of this title, means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser"--

(A) means 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 protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter 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 when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(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;

(d) intentionally uses, or endeavors to use, 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

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the

existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted--

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter--

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

[**(c)** Redesignated (b)]

(5)(a)(i) If the communication is--

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection--

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable

in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

§ 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally--

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of--

(i) any electronic, mechanical, or other device knowing the content of the advertisement and knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications,

knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined under this title or imprisoned not more than five years, or both.

…

§ 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

§ 2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of--

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344

(relating to bank fraud), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 1992 (relating to wrecking trains), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline) or section 46502 (relating to aircraft piracy) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);
(l) the location of any fugitive from justice from an offense described in this section;
(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);
(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);
(o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);
(p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens);
(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2332f, 2339A, 2339B, or 2339C of this title (relating to terrorism); or
(r) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

§ 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this

chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents 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.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign 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, and foreign investigative or law enforcement officers may use or

disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

§ 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any

judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that--

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person

whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(a) an emergency situation exists that involves--

(i) immediate danger of death or serious physical injury to any person,
(ii) conspiratorial activities threatening the national security interest, or
(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of--

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted

communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that--

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if--

(a) in the case of an application with respect to the interception of an oral communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;
(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and
(iii) the judge finds that such specification is not practical; and
(b) in the case of an application with respect to a wire or electronic communication--
(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;
(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;
(iii) the judge finds that such showing has been adequately made; and
(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.
(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

§ 2519. Reports concerning intercepted wire, oral, or electronic communications
(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts--

(a) the fact that an order or extension was applied for;
(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title);
(c) the fact that the order or extension was granted as applied for, was modified, or was denied;
(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
(e) the offense specified in the order or application, or extension of an order;
(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts--

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

§ 2520. Recovery of civil damages authorized

(a) In general.--Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.--In an action under this section, appropriate relief includes--

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of damages.--(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of--

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense.--A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation.--A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly

initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper disclosure is violation.--Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

§ 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

§ 2522. Enforcement of the Communications Assistance for Law Enforcement Act

(a) Enforcement by court issuing surveillance order.--If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) Enforcement upon application by Attorney General.--The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

(c) Civil penalty.--

(1) In general.--A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

(2) Considerations.--In determining whether to impose a civil penalty and in determining its amount, the court shall take into account--

(A) the nature, circumstances, and extent of the violation;
(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and
(C) such other matters as justice may require.
(d) Definitions.--As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

ECPA Title II. Stored Communications Act, 18 U.S.C. §§ 2701-2711

§ 2701. Unlawful access to stored communications

(a) Offense.--Except as provided in subsection (c) of this section whoever--

(1) intentionally accesses 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 shall be punished as provided in subsection (b) of this section.

(b) Punishment.--The punishment for an offense under subsection (a) of this section is--

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case--

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized--

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

§ 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.--Except as provided in subsection (b)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and
(ii) appear to pertain to the commission of a crime; or

[**(B)** Repealed. Pub.L. 108-27, Title V, § 508(b)(1)(A), April 30, 2003, 117 Stat. 650]

[**(C)** Repealed. Pub.L. 107-296, Title II, § 225(d)(1)(C), Nov. 25, 2002, 116 Stat. 2157]

(8) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or

(6) to any person other than a governmental entity.

§ 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing

service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure; or

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or

electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90- day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

§ 2704. Backup preservation

(a) Backup preservation.--**(1)** A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of--

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider--

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer challenges.--(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement--

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are

maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

§ 2705. Delayed notice

(a) Delay of notification.--(1) A governmental entity acting under section 2703(b) of this title may--

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is--

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that--

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber--

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access.--A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§ 2706. Cost reimbursement

(a) Payment.--Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount.--The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception.-- The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

§ 2707. Civil action

(a) Cause of action.--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.--In a civil action under this section, appropriate relief includes--

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination."

(e) Defense.--A good faith reliance on--3

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) Limitation.--A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) Improper disclosure.--Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the

official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

§ 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

> **(1)** request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
>
> **(2)** request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of certain disclosure.--No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by bureau.--The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of

Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed.--On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

§ 2710. Wrongful disclosure of video tape rental or sale records

(a) Definitions.--For purposes of this section--

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term "ordinary course of business" means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) Video tape rental and sale records.--**(1)** A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer--

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if--

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if--

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) Civil action.--(1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award--

(A) actual damages but not less than liquidated damages in an amount of $2,500;

(B) punitive damages;

(C) reasonable attorneys' fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) Personally identifiable information.--Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.

(e) Destruction of old records.--A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (b)(2) or (c)(2) or pursuant to a court order.

(f) Preemption.--The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

§ 2711. Definitions for chapter

As used in this chapter--

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system; and

(3) the term "court of competent jurisdiction" has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.

§ 2712. Civil actions against the United States

(a) In general.--Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U. S.C. 1801 et seq.) may commence an action in United States District Court against the United States to

recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

(1) actual damages, but not less than $10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) Procedures.--**(1)** Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General

with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) Exclusive remedy.--Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) Stay of proceedings.--**(1)** Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

> **(2)** In this subsection, the terms "related criminal case" and "related investigation" mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.
>
> **(3)** In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.

ECPA Title III. Pen Register Act, 18 U.S.C. §§ 3121-3127

§ 3121. General prohibition on pen register and trap and trace device use; exception

(a) In general.--Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception.--The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.

(c) Limitation.--A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

(d) Penalty.--Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

§ 3122. Application for an order for a pen register or a trap and trace device

(a) Application.--**(1)** An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of application.--An application under subsection (a) of this section shall include--

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

§ 3123. Issuance of an order for a pen register or a trap and trace device
(a) In general.--

(1) Attorney for the Government.--Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

(2) State investigative or law enforcement officer.--Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify--

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

(b) Contents of order.--An order issued under this section--

(1) shall specify--

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and".

(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

(c) Time period and extensions.--**(1)** An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) Nondisclosure of existence of pen register or a trap and trace device.--An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that--

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached, or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of

the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

§ 3124. Assistance in installation and use of a pen register or a trap and trace device

(a) Pen registers.--Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

(b) Trap and trace device.--Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line or other facility and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123(b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

(c) Compensation.--A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

(d) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter or request pursuant to section 3125 of this title.

(e) Defense.--A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(f) Communications assistance enforcement orders.--Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

§ 3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(1) an emergency situation exists that involves--

(A) immediate danger of death or serious bodily injury to any person;

(B) conspiratorial activities characteristic of organized crime;

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year;

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use;

may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title.

(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.

(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

§ 3126. Reports concerning pen registers and trap and trace devices

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which report shall include information concerning--

(1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
(2) the offense specified in the order or application, or extension of an order;
(3) the number of investigations involved;
(4) the number and nature of the facilities affected; and
(5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

§ 3127. Definitions for chapter

As used in this chapter--

(1) the terms "wire communication", "electronic communication", "electronic communication service", and "contents" have the meanings set forth for such terms in section 2510 of this title;
(2) the term "court of competent jurisdiction" means--
(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or
(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;
(3) the term "pen register" means 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, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;
(4) the term "trap and trace device" means 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 reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;
(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and
(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the Unite