CIVIL LIBERTIES CONCERNS IN TERRORISM BILLS
As of October 8, 2001

- **Pen Registers/ Trap and Trace Devices for the Internet (House 101, Senate 216) – Allows gov't to collect unspecified, undefined information about Web browsing and e-mail without meaningful judicial review.**

  - Expands "rubber-stamp" authority of the pen register statute (designed to collect telephone dialing information) to "dialing, routing, addressing and signaling information" regarding e-mail, Web browsing and other Internet use.

  - Excludes "content," but no one knows what that means on the Internet, where packets combine content and non-content, and signaling data reveal much more than telephone numbers do. No definition is given to the terms "routing, addressing and signaling."

  - Will be cited by FBI in imposing Carnivore on ISPs and others.

  - In the House, members of the Judiciary Committee agreed to work for clarifying language. **At the least, it needs to be made clear that URL information after the host name (everything after cnn.com or amazon.com) is content that cannot be intercepted by pen register.**

- **Interception of computer trespasser communications (House 105, Senate 217) – Allows ISPs, universities, network administrators to authorize surveillance on others without judicial order.**

  - Says that anyone accessing a computer "without authorization" has no privacy rights and can be tapped by the government without a court order, if the operator of the computer system says its okay. "Without authorization" is not defined.

  - Under the House version, relatively minor violations - like downloading a copyrighted mp3 file - would allow an ISP to authorize the government to tap all of that person's communications. With no judicial permission, oversight, or supervision.

  - No time limit – the extrajudicial wiretapping could go on for ever.

  - Senate bill states "computer trespasser" does **not** include any person with a "preexisting contractual agreement" with the computer operator, thus exempting ISP users. **Senate language is better and should be expanded to deal with workplaces, universities, libraries, or other network operators who do not necessarily have a contractual relationship with their users. Provision also needs to be given a time limitation of 48 hours, the limit on other emergency wiretap authorities.**

- **Roving taps in FISA cases (House 152, Senate 206) – Allows FBI to go from phone to phone, computer to computer, without assurance that device is used by suspected terrorist**

  - Gives FBI multi-point or "roving" tap authority in FISA cases. But does not limit tap top phone or computer while suspect is using it.

  - **Could allow government to tap all the computers in a library if suspect is using one of them.** If a FISA target is using payphones, the government could tap all payphones in the neighborhood, all day long.

  - **House Judiciary Committee Members agreed to work to include the so-called ascertainment guideline, which is in the roving tap provision applicable in criminal cases, specifying that the government can tap a particular payphone or computer when it ascertains that the target is using it.**

- **FISA Business Records Provision (House156, Senate 215)** -- Overrides existing privacy laws for sensitive categories of records, including medical, educational and library.

  - Would give intelligence agency access to "any tangible thing" - including sensitive medical, financial, or library records - from any person, with minimal judicial review, if "sought for" an intelligence investigation.

  - **A simple change – "Unless existing federal or state law provides otherwise as to the criteria for obtaining an order to produce records," – would avoid preemption of existing privacy laws.**

- **Eliminating FISA's "primary purpose" test (House 153, Senate 218) --** Criminal wiretaps could be conducted under the lower standards for foreign intelligence, without showing probable cause of a crime -- **an end-run around the relatively more stringent requirements for wiretaps in Title III.**

  - Eliminates the requirement that FISA procedures only be used when the government's purpose is the gathering of foreign intelligence -- allows wiretaps and secret searches in criminal investigations under the weaker FISA standards thereby circumventing the relatively stricter requirements for criminal investigations.

  - The current language in the bills – which add the word "significant" – is characterized as a compromise but would in fact have the same effect as the administration proposal. It would authorize the use of FISA procedures in <u>all</u> criminal investigations involving international terrorism or espionage, because they will always have "a significant' foreign intelligence gathering purpose. Destroys the distinction between intelligence and law enforcement agencies, which made the lower standards of FISA constitutional in the first place.

- **Sharing of Intelligence Information (House 103, 154, 353; Senate 203) – Allows intelligence agencies to receive – mainly with no judicial controls - information collected domestically in criminal cases.**

  - The House bill allows disclosure of the following information to any intelligence, national security, national defense, immigration or protective official, when such information constitutes "foreign intelligence" (undefined):

    - wiretap results (House 103),
    - grand jury information and any other information collected in a criminal case (House 154).

  - House bill allows disclosure of grand jury information that is not foreign intelligence to any intelligence, national security, national defense, immigration or protective personnel or to the President or Vice President, when permitted by the court upon a showing that the matters pertain to international or domestic terrorism or national security (House 353).

  - Senate bill allows disclosure of grand jury information, wiretap results, and any other information collected in a criminal investigation to any intelligence, national security, national defense, immigration or protective official, when such information involves "foreign intelligence" or "counterintelligence" (as defined in the National Security Act) or "foreign intelligence information" (Senate 203).

- **Secret Searches (not in the House bill, Senate 213) -- Allows law enforcement agencies to search homes and offices without notifying the owner right away.**

  - Not limited to terrorism cases - emerged last year in an anti-methamphetamine bill. Applies to citizens. Allows seizure of things and of wire and electronic communications (thereby seeming to supercede Title III.)

  - Government could enter your house, apartment or office with a search warrant when you are away, search through your property and take photographs, and in some cases seize physical property and electronic communications, and not tell you until later.

  - The Senate made changes to the broad Administration proposal, but secret searches remain a fundamental departure for traditional police practice and strict adherence to the Fourth Amendment.

  - **This provision should be dropped.**

Other Areas of Privacy Concern

- **Disclosure of educational records (Senate 508 and 509, not in House bill) --** Section 508 puts holes in the Family Educational Rights and Privacy Act – Senate language is an improvement over the Administration draft but it still should come out.

Section 509 deals with surveys (containing individually identifiable information) of post-secondary students.

- **Lowering standard for FISA pen registers (House 154, Senate 214)--** Both bills delete the "agent of a foreign power" standard for FISA pen registers and trap and trace devices. Leaving essentially no standard. Senate bill limits use to protection against international terrorism or clandestine intelligence activities. Senate bill bars use based solely on First Amendment activities.

- **Definition of federal crime of terrorism (House 309, Senate 810)**-- the Senate bill is better on this issue. Many of the property related offenses were removed from the list of predicate offenses (the computer predicate offenses were narrowed), and the section on releasing information about secret agents was removed. Furthermore, the statute of limitations and the penalty sections were significantly narrowed. **At this point, the terrorism definition, statute of limitation and penalty sections are all better in the Senate than in the House.**

- **Duration of FISA taps and searches (House 151, Senate 207) -- The House version allows secret searches and electronic surveillance of the homes and apartments of non-US citizens for up to one year without judicial supervision.**

  - Under current law, the FISA Court can order a wiretap of a "non-US person" for a period of 90 days, after which the government must report to the court on the progress of the surveillance and justify the need for further surveillance. The court can authorize physical searches for up to 45 days.

  - The House bill would extend both time frames to one year, meaning that after the government's initial ex parte showing there would be no judicial review for one year. This is too long.

  - **The Senate bill is better – it retains the current time frames for the initial approval. If, after 90 days, the government can show a continuing justification for the surveillance or search authority, then the court could authorize surveillance for one year.** (The Senate bill also extends the initial period for physical searches from 45 to 90 days.)

- **Miscellaneous national-security authorities (House 157, Senate 506)-- Allows greater access to banking, credit, and other consumer records in counter-intelligence investigations.**

  - Current law allows the federal government to use a "national security letter" to obtain sensitive banking, credit, and other consumer records under the relaxed and secretive oversight of FISA - but only when there are "specific and articulable" facts showing that the target consumer is "a foreign power or the agent of a foreign power."

- Bill would eliminate this "agent of a foreign power" standard, mandating disclosure of sensitive consumer data simply if an FBI official certifies that they are needed for an intelligence investigation.

- Applies to Fair Credit Reporting Act, allowing access to records from consumer reporting agencies (including the names of all financial institutions where accounts are held, all past addresses and employers, and credit reports); Right to Financial Privacy Act, broadly allowing access to bank records; Electronic Communications Privacy Act, allowing access to communications billing records.