Internet Surveillance: Recent U.S. Developments

*by Juri Stratford **

The U.S. Federal government has implemented both technologies and policies related to Internet surveillance. While the recent discussion tends to focus on the USA Patriot Act following the September 11 terrorist attacks, the U.S. Congress held hearings addressing Internet surveillance and Fourth Amendment protections as early as April 2000. At this point, Congress criticized the lack of oversight on the Federal Bureau of Investigation's Internet surveillance system, Carnivore.

Congress revisited the issue of Internet surveillance days after the September 11 attacks when the Attorney General presented draft legislation addressing "new surveillance authorities;" the USA Patriot Act developed from this proposal. The executive branch of the Federal government has since pursued a number of policies and strategies dealing with Internet surveillance and data mining.

Many of the difficulties surrounding the question of Internet surveillance center on the analogies between Internet surveillance and telephone surveillance. Are these analogies appropriate; and if we accept that there is a place for telephone surveillance in law enforcement and intelligence activities, does Internet surveillance or data mining naturally follow?

Carnivore (DSC 1000)
Carnivore is a Microsoft Windows based system developed and used by the U.S. Federal Bureau of Investigation that directly connects to an ISP's server. The FBI draws analogies from telephone surveillance to describe the Carnivore system.

Carnivore is used in two ways: as a "content wiretap" and a "trap and trace/pen-register." A telephone "content wiretap" is where law enforcement eavesdrops on a suspect's telephone calls, recording the oral communications on tape. Carnivore provides analogous capabilities for e-mail, capturing all e-mail messages to and from a specific account or all the network traffic to and from a specific IP address.

"Trap and trace" technology tracks all caller IDs of inbound telephone calls, while "pen-register" tracks all outbound telephone numbers dialed. Similar functionality for e-mail consists of capturing all e-mail headers (including e-mail addresses) going to or from an e-mail account, but not the actual contents. For other forms of Internet activity similar functionality consists of listing all the servers (web servers, FTP servers, etc.) accessed but not capturing the content of this communication, tracking everyone who accesses a specific web page or FTP file, or tracking all web pages or FTP files that a suspect accesses (Independent Technical Review of the Carnivore System; Final Report, 2002).

Earthlink
Carnivore first came to public attention through a February 4, 2000 court decision. An Internet service provider, later identified as EarthLink, questioned the legal authority of the court to issue an order requiring the installation of a "device which captures the time, date, source, and destination of electronic mail (e-mail) messages sent to and from an e-mail address maintained by a customer at the ISP." The court found that it had the legal authority under the pen register statute (18 USC 3122) to issue such an order (Court Order Authorizing Carnivore Installation at Earthlink, 2000).

The court decision and an article in the Wall Street Journal prompted congressional hearings on Carnivore in April and July 2000. In testimony before the House Committee on the Judiciary, July 24, 2000, Tom Perrine, on behalf of the San Diego Supercomputer, argued that "[t]he current debate… is really about the risks in naively attempting to simply translate the policies, law, and practices of telephone wiretaps into the digital realm of the Internet" (Perrine, 2000).

While Internet surveillance through Carnivore employed strategies similar to those employed in telephone surveillance, Congress questioned the potential to sift through large quantities of private communications without regard to source or destination. House Majority leader Richard K. Armey (R-TX) stated that "Nobody can dispute the fact that this [Carnivore technology] is not legal… within the context of any current wiretap law" (Poole, 2000).

Patriot Act
Following the September 11 terrorist attacks, Attorney General John Ashcroft submitted a draft of the legislation, the "Mobilization against Terrorism Act" to Congress on September 19, 2001. The Patriot Act developed from this proposal. President Bush signed the bill into Public Law 107-56 on October 26, 2001.

While much of the Patriot Act builds the infrastructure necessary to respond to terrorist activities, a significant section of the Patriot Act deals with "new authorities" that enhance the government's ability to conduct surveillance and share information. Privacy concerns were addressed in part through a sunset provision; many of these new surveillance authorities expire at the end 2005. However, much of the controversy surrounding the Patriot Act continues to focus on these "new authorities."

The FBI highlights these new authorities in their document entitled "Field Guidance on New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation." These highlights include the nationwide effect of court orders for pen registers or trap and trace installations; nationwide search warrants for e-mail; and the use of Carnivore installations. Another interesting point of clarification under the Patriot Act is that computer system administrators, e.g. an ISP, can obtain the assistance of law enforcement to monitor activity on their own computers (Field Guidance on New Authorities [Redacted] Enacted in the 2001 Terrorism Legislation, 2001).

In a Congressional Research Service report on the Patriot Act, Charles Doyle describes Federal communications privacy law as a three tiered system protecting the confidentiality of private telephone, face-to-face, and computer communications while enabling authorities to identify and intercept criminal communications.

First, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 prohibits electronic eavesdropping on telephone conversations, or computer or other forms of electronic communications in most instances. It also gives authorities a narrowly defined process for electronic surveillance to be used as a last resort in serious criminal cases. Next, 18 USC 2701-2709 covers telephone records, e-mail held in third party storage. Finally, 18 USC 3121-3127 governs court orders approving the government's use of trap and trace devices and pen registers which identify the source and destination of calls made to and from a particular telephone. The Patriot Act modifies the procedures at each of these three levels.

- Permits pen register and trap-and-trace orders for electronic communications (e.g. e-mail);

- Authorizes nationwide execution of court orders for pen registers, trap-and trace-devices, and access to stored e-mail or communication records (i.e. Carnivore technology);

- Treats stored voice mail like stored e-mail (rather than telephone conversations);

- Permits authorities to intercept communications to and from a trespasser within a computer system (with permission of the system's owner);

- Adds terrorist and computer crimes to Title III's predicate offense list;

- Reinforces protection for those who help execute Title III, ch. 121 and ch. 206 orders;

- Encourages cooperation between law enforcement and foreign intelligence investigators;

- Establishes a claim against the U.S. for certain communications privacy violations by government personnel

A sunset provision terminates the authority found in many of these provisions and several of the foreign intelligence amendments on December 31, 2005. However, section 216 addressing the use of Carnivore is not subject to the sunset provision (Doyle, 2002).

Total Information Awareness (Terrorist Information Awareness)
The U.S. Department of Defense committed resources to develop data mining capabilities through the Total Information Awareness program. The Defense Advanced Research Projects Agency (DARPA) began work on TIA in 2003. The objective of the program was to integrate information technologies into a prototype that could determine the feasibility of searching vast quantities of data as well as determine links or patterns in the data that are indicative of terrorist activities. The program sought to develop information technology in three areas including language translation, data search with pattern recognition and privacy protection, and advanced collaborative and decision support tools

As DARPA is a research and development agency, the intent was for DARPA to turn over their prototype for adoption to the Department of Defense and other Federal agencies.

While the TIA itself is now defunct, the federal government continues to use "data mining" techniques in other initiatives such as the Multi-State Anti-Terrorism Information Exchange (MATRIX). In a review of the TIA project, the Department of Defense Inspector General reported that the federal government is likely to adopt other versions of "data mining" in the future. (Information

Technology Management: Terrorism Information Awareness Program, 2003).

Recent Developments
The Federal Government continues to implement new policies to incorporate Internet surveillance and data mining into law enforcement and terrorist investigations.

On May 30, 2002, Attorney General John Ashcroft issued new guidelines to permit the FBI to tap commercial databases, employ data mining and search the Internet for evidence of terrorist activity. These new guidelines relax restrictions that were imposed on the FBI in 1976 to curb excesses of the 1950s and 1960s, when the agency actively spied on Americans involved in the civil rights movement, political dissent, and war protests (The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, 2002).

In 2003 and 2004, both President Bush and the Attorney General have made public appeals for the extension of the Patriot Act. These extensions refer to sections of the Title II surveillance authorities set to expire next year under the Act's sunset provisions (U.S. President, 2004).

If we accept that there is any appropriate need for surveillance activities such as telephone wiretapping then we can't dismiss the question of internet surveillance out of hand. While the scope of telephone surveillance is limited by the means of communications, the scope of Internet surveillance is not. Congress needs to revisit the question of Internet surveillance in an impartial setting that protects citizens' privacy while enabling law enforcement and terrorist investigations.

References
The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (2002, May 30), (Retrieved from http://www.usdoj.gov/olp/generalcrimes2.pdf)

Court Order Authorizing Carnivore Installation at Earthlink (2000, February 4), (Retrieved from http://www.epic.org/privacy/carnivore/cd_cal_order.html)

Doyle, Charles (2002, April 15). The USA PATRIOT Act: A Legal Analysis, (Retrieved from http://www.epic.org/privacy/terrorism/usapatriot/RL31377.pdf)

Field Guidance on New Authorities (Redacted) Enacted in the 2001 Terrorism Legislation (2001), (Retrieved from http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf)

Independent Technical Review of the Carnivore System: Final Report (2002, December 8), (Retrieved from http://www.epic.org/privacy/carnivore/carniv_final.pdf)

Perrine, Tom (2000, July 24). Testimony before the U.S. Congress House Committee on the Judiciary, Subcommittee on the Constitution, (Retrieved from http://www.house.gov/judiciary/perr0724.htm)

Poole, Patrick (2000). 'Carnivore' under siege, (Retrieved from http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=20036)

U.S. Department of Defense. Office of the Inspector General (2003, December 12). Information Technology Management: Terrorism Information Awareness Program, (Retrieved from http://www.dodig.osd.mil/audit/reports/FY04/04-033.pdf)

U.S. President (2004, January 20), State of the Union Address, (Retrieved from http://www.whitehouse.gov/news/releases/2004/01/20040120-7.html)

* Paper presented at the IASSIST Conference, Madison, May 2004. Juri Stratford, Government Information and Maps, Shields Library, University of California, Davis, California, 95616. Contact: jtstratford@ucdavis.edu