EBTER135
Updated May 25, 2004

Congressional Research Service

Internet Privacy: Law Enforcement Monitoring of E- Mail and Web Usage
Marcia S. Smith

Issue Definition

To what extent should law enforcement officials be permitted to monitor Internet usage, including electronic mail and Web site visits, and how have the terrorist attacks of September 11, 2001 affected this debate?

Current Situation

In response to the terrorist attacks, Congress passed, and the President signed into law, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), P.L. 107-56. The Homeland Security Act (P.L. 107-296) amends that Act, expanding the circumstances under which Internet Service Providers can voluntarily divulge information about subscribers, and to whom. The 108th Congress is monitoring how law enforcement and other government officials use the new authorities they have been given. A bill has been introduced in the Senate (S. 2476/Kyl) to repeal the section of the USA PATRIOT Act that establishes a sunset date of December 31, 2005, on some provisions in Title II. Another bill (S. 1695, Leahy), conversely, would make more of Title II's provisions subject to the sunset date.

Policy Analysis

The September 11, 2001, terrorist attacks sharpened the debate over how to strike a balance between law enforcement's need to investigate criminals, and protecting what most citizens believe to be their "right" to privacy. Internet privacy is only one part of this debate, but it was highlighted in the summer of 2000 by the revelation that the FBI uses a software program called Carnivore (later renamed DCS 1000) that it installs on the equipment of Internet Service Providers to monitor electronic mail (e-mail) and Web site visits of suspects. Privacy advocates worry that the software is not sufficiently sophisticated to distinguish between the e-mail and Web activity of a suspect and that of other ISP subscribers, thereby violating the latter's privacy.

Prior to the terrorist attacks, congressional attention focused on requiring reports from the Department of Justice on its use of Carnivore or similar systems to help assess whether the FBI was exceeding its authority to monitor Internet usage. However, some policymakers had been seeking expansion, rather than limitation, of law enforcement authority to monitor wire and electronic communications. Following the terrorist attacks, they accelerated efforts to provide law enforcement officials with additional authorities, which were provided in the USA PATRIOT Act. Some Members of Congress and privacy advocates were concerned that, in an emotionally charged climate, Congress was passing legislation too hurriedly. Groups such as the American Civil Liberties Union (ACLU), Center for Democracy and Technology (CDT), and Electronic Privacy Information Center (EPIC) urged caution, fearful that, in an attempt to track down and punish the terrorists who threaten American democracy, one of the fundamental tenets of that democracy -- privacy -- may itself be threatened.

Options and Implications for U.S. Policy

With the enactment of the USA PATRIOT Act, attention has shifted to implementation of its provisions by law enforcement officials and whether certain provisions should expire after a specified period of time ("sunset"). The law includes a sunset date of December 31, 2005, for certain provisions. Some want to repeal the sunset date, while others want to extend it to other provisions of the law.

Role of Congress/Legislation

As described above, in 2001 Congress passed the USA PATRIOT Act (P.L. 107-56) that, *inter alia*, makes it easier for law enforcement officials to monitor Internet activities. Relevant provisions of Title II are:

- Section 210, which expands the scope of subpoenas for records of electronic communications to include records commonly associated with Internet usage, such as session times and duration.

- Section 212, which *allows* ISPs to divulge records or other information (but not the contents of communications) pertaining to a subscriber if they believe there is immediate danger of death or serious physical injury or as otherwise authorized, and *requires* them to divulge such records or information (excluding contents of communications) to a governmental entity under certain conditions. It also allows an ISP to divulge the *contents* of communications to a law enforcement agency if it reasonably believes that an emergency involving immediate danger of death or serious physical injury requires disclosure of the information without delay. [This section was amended by the Cyber Security Enhancement Act, see below.]

- Section 216, which adds routing and addressing information (used in Internet communications) to dialing information, expanding what information a government agency may capture using pen registers and trap and trace devices as authorized by a court order, while excluding the content of any wire or electronic communications. The section also requires law enforcement officials to keep certain records when they use their own pen registers or trap and trace devices and to provide those records to the court that issued the order within 30 days of expiration of the order. To the extent that Carnivore-like systems fall with the new definition of pen registers or trap and trace devices provided in the Act, that language would increase judicial oversight of the use of such systems.

- Section 217, which allows a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from a protected computer under certain circumstances, and

- Section 224, which sets a 4-year sunset period (December 31, 2005) for many of the Title II provisions. Among the sections excluded from the sunset are Sections 210 and 216.

In 2002, Congress passed the Cyber Security Enhancement Act (H.R. 3482) as part of the Homeland Security Act (P.L. 107-296). It amends Section 212, lowering the threshold for when ISPs may divulge the content of communications, and to whom. Now ISPs need only a "good faith" belief (instead of a "reasonable" belief) that there is an emergency involving danger (instead of "immediate" danger) of death or serious physical injury. The contents can be disclosed to "a Federal, state, or local governmental entity" (instead of a "law enforcement agency"). Privacy advocates are concerned about the language for a number of reasons. For example, EPIC noted that allowing such information to be disclosed to any governmental entity not only poses increased risk to personal privacy but also is a poor security strategy and that the language does not provide for judicial oversight of the use of these procedures.

Two bills are pending in the 108th Congress to change the sunset requirements in Sec. 224. One bill (S. 2476/Kyl) would repeal Section 224, so that none of the Title II provisions would sunset. Another (S. 1695, Leahy), conversely, would make more of Title II's provisions subject to the sunset date. For example, Sections 210 and 216 would also sunset.

CRS Products

CRS Report RL31408. *Internet Privacy: Overview and Pending Legislation.*

CRS Report RL31289(pdf). *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government.*

CRS Report RL31200(pdf). *Terrorism: Section by Section Analysis of the USA PATRIOT Act.*

CRS Report 98-326(pdf). *Privacy: an Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping.*