Distributed by Penny Hill Press

BT-1065
Updated Sept. 19, 2002

Congressional Research Service

http://pennyhill.com

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. Amendments to the Act are now being considered by Congress (H.R. 3482). For a detailed legal discussion of all of the Act's provisions, see CRS Report RL31200 For a discussion of the Act's implications for the Internet, see CRS Report RL31289

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 (now renamed DCS 1000) to monitor electronic mail (e-mail) and Web site visits. The FBI must obtain a court order to install the software on the equipment of an Internet Service Provider (ISP), but 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 their 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 is shifting to implementation of its provisions by

law enforcement officials. Attorney General Ashcroft directed federal prosecutors to begin using the new powers immediately; Congress and privacy advocates are monitoring how they are used. House Judiciary Committee Chairman Sensenbrenner and Ranking Member Dingell wrote to Mr. Ashcroft in June 2002 asking a number of questions regarding implementation of the Act. According to press reports, in August 2002, with only partial replies to the questions in hand, Chairman Sensenbrenner threatened to subpoena the Attorney General if the questions were not answered satisfactorily. Senators Leahy, Grassley, and Specter also have been cited in press reports as expressing concern about the Attorney General's unwillingness to provide information about implementation of the Act. Separately, the ACLU, EPIC, and the American Booksellers Foundation have filed Freedom of Information Act requests seeking information on how the surveillance provisions of the Act are being implemented.

Role of Congress/Legislation

As described above, 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.

- 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 for many of the Title II provisions. Among the sections excluded from the sunset are Sections 210 and 216.

A bill (H.R. 3482) that would, *inter alia*, amend Section 212 of the USA PATRIOT Act was reported by the House Judiciary Committee on June 11, 2002 (H. Rept. 107-497) and passed the House on July 15, 2002. It would the lower the threshold for when ISPs may divulge the content of communications and to whom. For more information, see CRS Report RL31408.

Although these provisions provide more latitude to law enforcement officials to monitor Internet activity,

the FY2002 Department of Justice authorization bill (H.R. 2215), as passed by the House and Senate, requires the Justice Department to report *to Congress* on its use of DCS 1000 (Carnivore) or any similar system. Conferees have been named, and the House voted to instruct conferees on May 1, 2002. (As noted above, the USA PATRIOT Act provides for *judicial* oversight of the use of Carnivore-like systems by law enforcement officials.)

CRS Products

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

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

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

CRS Report RL30671 *Personal Privacy Protection: The Legislative Response.*

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