Congressional Research Service

Terrorism:

Internet Privacy: Law Enforcement Monitoring of E- Mail and Web Usage

Marcia S. Smith

Issue Definition

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

Current Situation

On October 26, 2001, six weeks after the terrorist attacks, President Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, P.L. 107-56. Among its many provisions, the Act gives law enforcement authorities additional authority to monitor individuals' Internet activity, including e-mail and website visits. Amendments passed the next year as part of the Homeland Security Act (P.L. 107-296) expanded the circumstances under which Internet Service Providers may voluntarily divulge the content of communications, and to whom. The Congress and civil liberties groups are monitoring how the Act is implemented. Some of the Act's provisions, including several related to the Internet, are subject to a December 31, 2005, sunset clause. S. 1695 (Leahy) and S. 1709 (Craig) would sunset more of the sections, while S. 2476 (Kyl) would repeal the sunset clause. The July 2004 "9/11 Commission report" called for a full and informed debate about the PATRIOT Act, and concluded that security and liberty must be reconciled.

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 was using a software program called Carnivore (later renamed DCS 1000) that it installed on the equipment of Internet Service Providers to monitor electronic mail (e-mail) and website visits of suspects. Privacy advocates worried that the software was 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 sought 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. Many of these were provided in the 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.

On July 13, 2004, Attorney General Ashcroft released *Report from the Field: The USA PATRIOT Act At Work* providing an overview of "how the Act has been instrumental in the effort to combat terrorism and make Americans safer." The report cites several instances in which Sec. 210, Sec. 212, and Sec. 216 were instrumental in law enforcement actions. Some critics noted that the report did not address all aspects of the PATRIOT Act, particularly a controversial topic that was the subject of House floor debate in July 2004 (specifically, access to library records, which is outside the scope of this briefing book entry).

On July 22, 2004, the 9/11 Commission issued its report on the terrorist attacks (*Final Report of the National Commission on Terrorist Attacks Upon the United States)*. The Commission concluded (pp. 394-395) that many of the PATRIOT Act provisions appear beneficial, but that "Because of concerns regarding the shifting balance of power to the government, we think that a full and informed debate on the Patriot Act would be healthy." The Commission recommended that "The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use." The Commission also called for creation of a board within the executive branch "to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties." The commissioners went on to say that "We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend."

Options and Implications for U.S. Policy

Attention is focused on oversight of implementation of the PATRIOT Act's provisions, and whether certain provisions should expire ("sunset") after a specified period of time. Sec. 224 of 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 (see below).

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 four-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.

Under the current law, Sec. 212 and Sec. 217 are subject to the December 31, 2005, sunset date in Sec. 224, while Sec. 210 and Sec. 216 are not. S. 1695 (Leahy) would amend the sunset provision such that Sec. 210 and Sec. 216 also would sunset. S. 1709 (Craig) would include Sec. 216 in the sunset clause. By contrast, S. 2476 (Kyl), would repeal Sec. 224 so that none of the provisions 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.*