Order Code RS20693
October 3, 2000

CRS Report for Congress

Congressional Research Service • The Library of Congress

Electronic Communications Privacy Act of 2000 (H.R. 5018): Summary in Brief

Gina Marie Stevens
Legislative Attorney
American Law Division

Summary

The House Judiciary Committee approved the Electronic Communications Privacy Act of 2000 (H.R. 5018) on September 26, 2000. The purpose of H.R. 5018 is to modify certain provisions of Title 18 relating to the interception of electronic communications, and to address some of the legal issues that the Internet raises. H.R. 5018 would (i) amend the laws governing how law enforcement may obtain non-content information under pen register/trap and trace statutes; (ii) extend the statutory exclusionary rule to electronic communications in transit (real-time), and to stored electronic communications; and (iii) extend Title III's (the wiretap statute) reporting requirements to stored electronic communications. H.R. 5018 was amended in Committee. A similar bill has not been introduced in the Senate. Information on amendments to the bill's during markup provisions are derived from published news reports.

The legislation was also prompted in part by privacy concerns over the FBI's "Carnivore" Internet surveillance system. Installed on the network of an Internet service provider, Carnivore monitors communications on the network and records messages sent or received by a targeted user. Carnivore can reportedly also provide the origin and destination of all communications to and from a particular ISP customer. Privacy advocates, civil libertarians, Internet users, and the computer industry expressed concern over Carnivore's threats to the privacy and security of Internet communications. Congressional attention was immediate with hearings on Carnivore held by the House and Senate Judiciary Committees. At the hearings, the Department of Justice urged Congress to update the Electronic Communications Privacy Act and the pen register and trap/trace statutes to address criminal use of the Internet. In July the Clinton Administration, through the Department of Justice, transmitted to Congress proposed legislation to amend the substantive laws defining what conduct is criminal on the Internet, and the procedural laws used to investigate computer crimes (the federal wiretap and electronic privacy laws). This report will be updated when warranted.

The House Judiciary Committee approved the Electronic Communications Privacy Act of 2000 (H.R. 5018) on September 26, 2000 by a 20-1 vote. H.R. 5018's chief sponsor is

CRS Reports are prepared for Members and committees of Congress

Representative Charles Canady, Chairman of the Constitution Subcommittee. Hearings on H.R. 5018 and two other bills (H.R. 4987, the Digital Privacy Act and H.R. 4908, the Notice of Electronic Monitoring Act) were held by the Subcommittee on September 6th.[1] H.R. 5018 was approved by the Subcommittee on September 14th by a unanimous voice vote. A similar bill has not been introduced in the Senate.

The purpose of H.R. 5018 is to modify certain provisions of title 18 (federal criminal laws) relating to the interception of communications. H.R. 5018 was drafted to address some of the legal issues that the Internet raises, and update the statutory framework for conducting digital surveillance on the Internet. The premise for the legislation is that traditional concepts of wiretapping and the Fourth Amendment were developed in an era of centralized telephone networks,[2] not the packetized, decentralized environment of the Internet. According to the FBI, it has encountered an increasing number of criminal investigations in which criminal subjects used the Internet to communicate, for which Internet service providers (ISP) lacked the ability to discriminate communications to identify a particular subject's messages to the exclusion of all others.

Carnivore. The legislation was prompted in part by privacy concerns over the FBI's "Carnivore" Internet surveillance system.[3] Widespread knowledge of the existence of the FBI's new surveillance tool for Internet communications – Carnivore – occurred with the publication on July 11th of an article in the Wall Street Journal.[4] Carnivore had been deployed by the FBI in hacker, counterterrorism, and drug-trafficking cases for over a year reportedly to monitor the communications of individuals who were targets of criminal investigations. The FBI must obtain a court order to deploy Carnivore to monitor communications. Carnivore is installed on the network of an ISP. It monitors communications on the network and records messages sent or received by a targeted user. This is presumably designed to respond to an electronic "wiretap" order served on an ISP. Carnivore can also provide the origin and destination of all communications to and from a particular ISP customer. This is designed to be the equivalent of "pen register" and "trap and trace" orders, which in the telephone context provides digits dialed and incoming phone numbers. The FBI dubbed it Carnivore for its ability to get to "the meat" of what would otherwise be an enormous quantity of data. The FBI says the system allows investigators to tailor an intercept operation so it can pluck only the digital traffic of one person from among the stream of millions of other messages. According to the FBI, its design and development of Carnivore "provides the FBI with a 'surgical' ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept."[5] Critics of Carnivore say that the problem with Carnivore is not what the FBI is currently using it for, but rather what it has the capacity to do. Carnivore enables law enforcement officials to

---

[1] [http://www.house.gov/judiciary/cons0906.htm].

[2] For an overview, see, Taps, Bugs & Telephony: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping, Charles Doyle and Gina Stevens, CRS Report 98-326A (Mar. 23, 1998).

[3] Digital surveillance: the Communications Assistance for Law Enforcement Act and FBI Internet monitoring, CRS Report RL30677 by Richard M. Nunno (Sept. 19, 2000).

[4] FBI's Wiretaps To Scan E-Mail Spark Concern, Wall Street Journal (Jul. 11, 2000).

[5] Carnivore Diagnostic Tool, http://www.fbi.gov/programs/carnivore/carnivore2.htm.

sift through all of the traffic that passes through an ISP's network, and is capable of capturing both numbers and a limited amount of content. (e.g., the subject line of emails and the URLs of web sites visited). Because Carnivore's capacity is so broad, critics argue that its use goes beyond the limited wiretapping authority that Congress granted law enforcement officials under the Electronic Communications Privacy Act. ECPA generally requires law enforcement to "minimize" its interceptions of non-incriminating communications. Carnivore, however, has the potential to do the opposite.

Since knowledge of Carnivore's existence became widespread, it has been at the center of controversy. Privacy advocates, civil libertarians, and the computer industry immediately expressed concerns over Carnivore's threats to the privacy and security of Internet communications. The Carnivore system has disturbed many in the Internet industry because, when deployed, it must be hooked directly into Internet service providers' computer networks, and as a result would give the government the ability to eavesdrop on all customers' digital communications, from e-mail to online banking and Web surfing. The system also troubles Internet service providers who are resistant to outside software being plugged into their systems. In many cases, the FBI keeps the secret Carnivore computer system in a locked cage on the provider's premises, and makes daily visits to retrieve the data captured from the provider's network. Legal challenges to the use of Carnivore are few, and judges' rulings remain sealed because of the nature of the investigations.[6]

Congressional attention followed shortly after publication of the Wall Street Journal article on Carnivore with a hearing July 24th held by the House Judiciary Subcommittee on the Constitution on "Carnivore's Challenge to Privacy and Security Online."[7] The Senate Judiciary Committee also held a hearing on "The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age" on September 6th.[8]

Electronic Communications Privacy Act of 2000. H.R. 5018, as introduced, would make three significant changes to the law: (i) it would amend the laws governing how law enforcement may obtain non-content information under pen register/trap and trace statutes; (ii) extend the statutory exclusionary rule to electronic communications in transit (real-time), and to stored electronic communications; and (iii) extend Title III's (the wiretap statute) reporting requirements to stored electronic communications.

Justice Department officials have raised serious concerns about the bill, arguing that it could undermine law enforcement's ability to combat cyberterrorism, Internet-based fraud and theft, online child pornography and many other cybercrimes. The Subcommittee

---

[6] In one case, a federal judge overruled an ISP's refusal to allow the FBI to install Carnivore, and required it to grant the FBI access to its network. The case was resolved when the ISP and the government reached an accommodation in which the device was installed and further assurances were made about network security and about protecting the privacy of subscribers generally. See, "Case History: Installation of a Pen Register and Trap and Trace Device at an ISP" from Testimony of Robert Corn-Revere, Esq. before the Subcommittee on the Constitution of the Committee on the Judiciary on The Fourth Amendment and the Internet (Apr. 6, 2000).

[7] [http://www.house.gov/judiciary/con0724.htm].

[8] [http://www.senate.gov/~judiciary/w196200f.htm].

worked closely with Justice Department officials to address some of these concerns during markup.

Extension of Reporting Requirement. Section 3 of H.R. 5018 amends section 2703 of title 18 to require the compilation and publication of annual reports of data regarding government acquisition of stored data, such as email. In 1968, when Congress adopted Title III, the wiretap statute, it required the Administrative Office of the United States Courts to compile and publish annually a report on wiretap activity.[9] In 1986, when Congress adopted the Electronic Communications Privacy Act (ECPA), real-time interception of email (electronic communications in transit) was included under Title III, so that interception of email is reported under the Title III reporting provisions of section 2519. However, ECPA created a new chapter 121 for government access to email and other electronic communications "in storage."[10] Section 2703 is the main section setting out standards for government access to electronic communications in storage. However, Congress did not include a reporting requirement in the stored records chapter, and therefore no data is collected on the amount of email seized under the stored communications chapter. Section 3 of H.R. 5018 requires the compilation and reporting of basic information on the activity of federal, state, and local agencies in seizing email and other customer records. Privacy advocates and civil libertarians support the extension of the reporting requirements to stored electronic communications as a method to improve government accountability, and as a means to assess the scope and effectiveness of government wiretapping. The Department of Justice testified that the bill's reporting requirements would place a "significant burden" on law enforcement officials. According to published reports,[11] the reporting requirement was simplified in committee.[12]

Extension of Statutory Exclusionary Rule. Section 2 of H.R. 5018 creates two new statutory suppression remedies, by bringing electronic communications within the scope of the statutory suppression rule of Title III, 18 U.S.C. § 2515. Current law provides that illegally intercepted voice communications cannot be used in court or in agency hearings. When Congress adopted Title III in 1968, it established certain protections for interception of communications that went beyond Fourth Amendment requirements. Congress then established a statutory suppression rule, to exclude evidence seized in material violation of those protections, 18 U.S.C. § 2515. In 1986, when Congress passed the Electronic Communications Privacy Act, and added the word "electronic" to most of Title III's provisions, it did not do so in section 2515. Section 2 of H.R. 5018 addresses this omission. H.R. 5018 extends the statutory exclusionary rule to electronic communications in transit (real-time), and also extends the statutory exclusionary rule to stored electronic communications. In addition, section 2 adds a reference to stored electronic communications disclosed in violation of chapter 121, extending the statutory suppression rule to illegal seizures of email in violation of chapter 121. In other words, section 2 makes clear that the exclusionary rule apples to "electronic communication," the term

---

[9] 18 U.S.C. § 2519.

[10] 18 U.S.C. § 2701 et seq.

[11] House Panel Mulls Tougher Standards for Electronic Wiretap Warrants, 106 Markup H.R. 5018, National Journal Committee Markups and Votes (Sep. 20, 2000).

[12] Electronic Wiretap Bill Clears House Panel, 106 Markup H.R. 5018, National Journal Markup Reports (Sep. 26, 2000).

introduced in 1986, as well as to "wire and oral communication," the original phrase from the 1968 Act.

According to published reports, a manager's amendment offered by the bill's chief sponsor eliminated stored email from the exclusionary rule amendment.[13] Several committee members opposed the elimination of stored email. The panel voted 9-7 to bar that provision, and to include stored email under the statutory exclusionary rule.

Pen Registers and Trap and Trace Amendments. Section 4 of H.R. 5018 would amend the pen register and trap and trace statute for email to require a showing of "specific and articulable facts [that] reasonably indicate that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use is relevant to an investigation of that crime." This evidentiary standard tracks the current standard for a court order authorizing the acquisition of stored electronic data under 18 U.S.C. § 2703(d). Current law provides that the court *shall* issue an order authorizing the placement of a pen register or trap and trace device whenever any attorney for the Government or an investigative officer certifies in an ex parte proceeding that information likely to be obtained through the Order is relevant to an ongoing criminal investigation. There is widespread agreement that the current legal standard does not offer meaningful privacy protection.

The legal standard that law enforcement agencies must satisfy to obtain authorization to secure a list of the telephone numbers of incoming and outgoing calls on a surveillance subject's line are less demanding than the standards for interception of telephone conversations. The Electronic Communications Privacy Act establishes less demanding standards for capturing telephone numbers through the use of pen registers and trap and trace devices. Pen registers record telephone numbers of outgoing calls;[14]trap and trace devices record telephone numbers from which incoming calls originate.[15] ECPA requires law enforcement agencies to obtain court orders to install and use these devices. Rather than the strict probable cause showing necessary for wiretaps, pen register orders require only certification from a law enforcement officer that "the information likely to be obtained is relevant to an ongoing criminal investigation."[16]

H.R. 5018 would introduce the requirement of judicial review of the factual basis for such orders. Specifically, H.R. 5018 would require such applications to contain "specific and articulable facts" that would justify the collection of the data. H.R. 5018 would apply the heightened standard only to devices that identify "an email address." The Justice Department had several concerns about these changes. Specifically, it was concerned with the technology-specific manner in which the bill would implement this change, the lack of an emergency exception, and the geographic limitations that restrict such orders in the present law. The fact that H.R. 5018 would apply the heightened standard only to devices that identify an email address does not take into account other ways that electronic

---

[13] Panel Vote Emphatically Backs Limits on Electronic Tracking, CQ Daily Monitor 11 (Sep. 27, 2000).

[14] 18 U.S.C. § 3127(3).

[15] 18 U.S.C. § 3127(4).

[16] 18 U.S.C. § 3122(b)(2).

communications are sent over computer networks. Justice prefers the use of technology neutral language, and desires authorization for law enforcement to use pen/trap devices in emergency situations without getting approval from a court, so long as they obtain court approval within 48 hours. Finally, the Department of Justice would like the wiretap statute to be amended to ensure that federal courts have the authority to order all telecommunications carriers providing service in the United States to provide law enforcement authorities the information needed to trace both voice and electronic communications to their source.

Some hearing witnesses have criticized section 4 of H.R. 5018 because it explicitly authorizes access to email address information under the "reasonable indication" standard, and leaves in place the lower standard of "relevancy" for issuing a pen register or trap and trace order for voice communications. Instead, they recommend strengthening the standards for issuing pen register and trap and trace orders by requiring a finding that factual evidence "reasonably indicates" that a crime has been, is being, or will be committed." They would defer for the time being the question of whether that standard is appropriate for email addresses and other electronic communications, in order for full debate to occur on whether the pen register statute should apply to the Internet and if so what information should be collected and what the standard should be.

Other Provisions. It was also reported that the committee approved an amendment that would require police to get a warrant to obtain a suspect's email, whether stored or "real-time."[17] The committee also approved an amendment that would extend from six months to one year, the period of time in which a warrant would be needed to access a suspect's stored email from an Internet service provider.[18] Published reports also indicate that the committee approved an amendment that would make it more difficult for law enforcement officials to get location information from cell phone providers, except in emergency circumstances.[19] Another amendment the committee adopted would make it illegal to deface or destroy a website, even if the damage amounts to less than $5,000.[20]

---

[17] Electronic Wiretap Bill Clears House Panel, 106 Markup H.R. 5018, National Journal Markup Reports (Sep. 26, 2000).

[18] Id.

[19] Panel Vote Emphatically Backs Limits on Electronic Tracking, CQ Daily Monitor 11 (Sep. 27, 2000).

[20] Id.