106TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
106–932

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 2000

OCTOBER 4, 2000.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. CANADY, from the Committee on the Judiciary, submitted the following

R E P O R T

[To accompany H.R. 5018]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 5018) amending title 18, United States Code, to modify certain provisions of law relating to the interception of communications, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

TABLE OF CONTENTS

79–006

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 2000".

SEC. 2. USE AS EVIDENCE.

(a) IN GENERAL.—Section 2515 of title 18, United States Code, is amended—

(1) by striking "**wire or oral**" in the heading and inserting "**wire, oral, or electronic**".

(2) by striking "Whenever any wire or oral communication has been intercepted" and inserting "(a) Except as provided in subsection (b), whenever any wire, oral, or electronic communication has been intercepted, or any electronic communication in electronic storage has been disclosed";

(3) by inserting "or chapter 121" after "this chapter"; and

(4) by adding at the end the following:

"(b) Subsection (a) does not apply to the disclosure, before a grand jury or in a criminal trial, hearing, or other criminal proceeding, of the contents of a communication, or evidence derived therefrom, against a person alleged to have intercepted, used, or disclosed the communication in violation of this chapter, or chapter 121, or participated in such violation.".

(b) SECTION 2517.—Paragraphs (1) and (2) of section 2517 are each amended by inserting "or under the circumstances described in section 2515(b)" after "by this chapter".

(c) SECTION 2518.—Section 2518 of title 18, United States Code, is amended—

(1) in subsection (7), by striking "subsection (d)" and inserting "subsection (8)(d)"; and

(2) in subsection (10)—

(A) in paragraph (a)—

(i) by striking "or oral" each place it appears and inserting ", oral, or electronic";

(ii) by striking the period at the end of clause (iii) and inserting a semicolon; and

(iii) by inserting "except that no supresssion may be ordered under the circumstances described in section 2515(b)." before "Such motion"; and

(B) by striking paragraph (c).

(d) CLERICAL AMENDMENT.—The item relating to section 2515 in the table of sections at the beginning of chapter 119 of title 18, United States Code, is amended to read as follows

"2515. Prohibition of use as evidence of intercepted wire, oral, or electronic communications.".

SEC. 3. REPORTS CONCERNING THE DISCLOSURE OF THE CONTENTS OF ELECTRONIC COMMUNICATIONS.

Section 2703 of title 18, United States Code, is amended by adding at the end the following:

"(g) REPORTS CONCERNING THE DISCLOSURE OF THE CONTENTS OF ELECTRONIC COMMUNICATIONS.—

"(1) By January 31 of each calendar year, the judge issuing or denying an order, warrant, or subpoena, or the authority issuing or denying a subpoena, under subsection (a) or (b) of this section during the preceding calendar year shall report on each such order, warrant, or subpoena to the Administrative Office of the United States Courts—

"(A) the fact that the order, warrant, or subpoena was applied for;

"(B) the kind of order, warrant, or subpoena applied for;

"(C) the fact that the order, warrant, or subpoena was granted as applied for, was modified, or was denied;

"(D) the offense specified in the order, warrant, subpoena, or application;

"(E) the identity of the agency making the application; and

"(F) the nature of the facilities from which or the place where the contents of electronic communications were to be disclosed.

"(2) In January of each year the Attorney General or an Assistant Attorney General specially designated by the Attorney General shall report to the Administrative Office of the United States Courts—

"(A) the information required by subparagraphs (A) through (F) of paragraph (1) of this subsection with respect to each application for an order, warrant, or subpoena made during the preceding calendar year; and

"(B) a general description of the disclosures made under each such order, warrant, or subpoena, including—

"(i) the approximate number of all communications disclosed and, of those, the approximate number of incriminating communications disclosed;

"(ii) the approximate number of other communications disclosed; and

"(iii) the approximate number of persons whose communications were disclosed.

"(3) In June of each year, beginning in 2002, the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders, warrants, or subpoenas authorizing or requiring the disclosure of the contents of electronic communications pursuant to subsections (a) and (b) of this section and the number of orders, warrants, or subpoenas granted or denied pursuant to subsections (a) and (b) of this section during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by paragraphs (1) and (2) of this subsection. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by paragraphs (1) and (2) of this subsection.".

SEC. 4. PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) REQUIREMENT FOR SHOWING.—Section 3122(b)(2) of title 18, United States Code, is amended to read as follows:

"(2) a statement of facts showing that the requirements of section 3123 have been met.".

(b) FINDING BY COURT.—Subsection (a) of section 3123 of title 18, United States Code, is amended by striking "the attorney for the Government" and all that follows through the end of such subsection and inserting "specific and articulable facts 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 the investigation of that crime.".

SEC. 5. CIVIL DAMAGES.

Section 2520(c)(2) of title 18, United States Code, is amended—

(1) by striking "court may" and inserting "court shall";

(2) by striking "greater" and inserting "greatest";

(3) in subparagraph (A), by striking "or" after the semicolon;

(4) in subparagraph (B), by striking "whichever is the greater of $100 a day for each day of violation or $10,000." and inserting "$500 a day for each violation; or"; and

(5) by inserting after subparagraph (B), the following:

"(C) statutory damages of $10,000.".

SEC. 6. NOTIFICATION.

Section 2705(a)(4) of title 18, United States Code, is amended by striking "or by certification by a governmental entity, but only in accordance with subsection (b) of this section." and inserting "if the court determines that there is reason to believe that notification of the existence of the court order or subpoena may have an adverse result described in paragraph (2) of this subsection.".

SEC. 7. GOVERNMENT ACCESS TO LOCATION INFORMATION.

(a) COURT ORDER REQUIRED.—Section 2703 of title 18, United States Code, as amended by section 3 of this Act, is further amended by adding at the end the following:

"(h) DISCLOSURE OF LOCATION INFORMATION TO GOVERNMENTAL ENTITIES.—

"(1) DISCLOSURE UPON COURT ORDER.—Except as provided in paragraph (2), a provider of mobile electronic communication service shall provide to a governmental entity information generated by and disclosing the current physical location of a subscriber's equipment only if the governmental entity obtains a court order issued upon a finding that there is probable cause to believe that—

"(A) a person is committing, has committed, or is about to commit a felony offense; and

"(B) the location information sought to be obtained concerns the location of the person believed to have committed, be committing, or be about to commit that offense or a victim of that offense.

"(2) PERMITTED DISCLOSURES WITHOUT COURT ORDER.—A provider of mobile electronic communication service may provide information described in paragraph (1)—

"(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

"(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

"(C) with the express consent of the subscriber or the user of the equipment concerned.

"(3) DEFINITION.—The term 'public safety answering point' means a facility that has been designated to receive emergency calls and route them to emergency service personnel.".

(b) CONFORMING AMENDMENT.—Subsection (c)(1)(A) of section 2703 of title 18, United States Code, is amended by striking "(b) of this section" and inserting "(b), or wireless location information covered by subsection (g)".

SEC. 8. COMPUTER CRIME AMENDMENTS.

(a) GENERALLY.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)(3), by striking "such a computer" and inserting "without or in excess of authorization a computer";

(2) in subsection (a)(5), by inserting after subparagraph (C) the following:

"(B) whose conduct described in clause (i), (ii), or (iii) of subparagraph (A)—

"(i) caused loss to one or more persons during any one-year period (including loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least $5,000;

"(ii) modified or impaired, or potentially modified or impaired, the medical examination, diagnosis, treatment, or care of one or more individuals;

"(iii) caused physical injury to any individual;

"(iv) threatened public health or safety;

"(v) caused damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security; or

"(vi) intentionally defaced, damaged, or destroyed images or information made available to the public and thereby interfered with the rights protected under the First Amendment to the Constitution;".

(3) in subsection (a)(5)(A), by inserting "(i)" after "(5)(A)";

(4) in subsection (a)(5)(B), by striking "(B)" and inserting "(ii)";

(5) in subsection (a)(5)(C)—

(A) by striking "(C)" and inserting "(iii)"; and

(B) by inserting "and" after the semicolon;

(6) in subsection (a)(7), by striking ", firm, association, educational institution, financial institution, government entity, or other legal entity,";

(7) in subsection (b), by adding before the period "as if such person had committed the completed offense";

(8) in subsection (c)(1)(A) and (B), by striking ", or an attempt to commit an offense punishable under this subparagraph";

(9) in subsection (c)(1)(A), by inserting ", (a)(5)(A)(i), or (a)(5)(A)(ii)" after "(a)(1)";

(10) by amending subsection (c)(2)(A) to read as follows:

"(2)(A) except as provided in subsection (c)(2)(B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section;";

(11) by striking subparagraph (C) of subsection (c)(2);

(12) in subsection (c)(3)—

(A) by striking "(3)(A)" and inserting "(3)";

(B) by striking ", (a)(5)(A), (a)(5)(B),";

(C) by striking ", or an attempt to commit an offense punishable under this subparagraph; and" and inserting "; and"; and

(D) by striking subparagraph (B) and inserting:

"(4) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(4), (a)(5), (a)(6), or (a)(7) of this section which occurs after a conviction for another offense under this section.";

(13) in subsection (d)—

(A) by striking "subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of"; and

(B) by striking "which shall be entered into by" and inserting "between";

(14) in subsection (e)(7), by striking "and" after the semicolon;

(15) in subsection (e)(8), by striking all after "information" and inserting a semicolon;

(16) in subsection (e)(9), by striking the period at the end and inserting a semicolon;

(17) by inserting the following after subsection (e)(9):

"(10) the term 'conviction for another offense under this section' includes a State conviction for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

"(11) the term 'loss' means any reasonable cost to any victim, including responding to the offense, conducting a damage assessment, restoring any data, program, system, or information to its condition before the offense, and any revenue lost or costs incurred because of interruption of service; and

"(12) the term 'person' includes any individual, firm, association, educational institution, financial institution, corporation, company, partnership, government entity, or other legal entity.";

(18) by amending subsection (g) to read as follows:

"(g) Except as herein provided, any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive or other equitable relief. A suit for a violation of subsection (a)(5) may be brought only if the conduct involves one or more of the factors enumerated in subsection (a)(5)(B). No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage."; and

(19) by adding the following subsection after subsection (h):

"(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

"(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

"(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

"(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.".

(b) SENTENCING COMMISSION.—Section 805(c) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104–132; 28 U.S.C. 994 note) is amended by striking "shall amend the sentencing guidelines to ensure any individual convicted of a violation of paragraph (4) or (5)" and inserting "shall amend the sentencing guidelines to ensure any individual convicted of a violation of paragraph (4) or a felony violation of paragraph (5)(A)(i) (but not of paragraph (5)(A)(ii) or (5)(A)(iii))".

SEC. 9. INTERCEPTION OF WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS AMENDMENTS.

Chapter 119 of title 18, United States Code, is amended—

(1) in section 2510(10), by striking "153(h)" and inserting "153(10)";

(2) in section 2516(1), by striking "wire or oral" and inserting "wire, oral, or electronic";

(3) in the first paragraph (p) of section 2516(1), by inserting "section 1030 (relating to computer fraud and abuse), section 1362 (relating to destruction of government communications facilities)," after "identification documents),"; and

(4) in section 2516(1), by redesignating the second paragraph (p) as paragraph (q).

SEC. 10. AMENDMENTS TO THE ELECTRONIC COMMUNICATIONS PRIVACY ACT.

(a) PENALTIES FOR UNLAWFUL ACCESS TO STORED COMMUNICATIONS.—Section 2701 of title 18, United States Code, is amended—

(1) in subsection (b)(1)—

(A) by striking "purposes of" and inserting "a tortious or illegal purpose,";

(B) in subparagraph (A), by striking "one year" and inserting "three years"; and

(C) in subparagraph (B), by striking "two" and inserting "five"; and

(2) by amending subsection (b)(2) to read as follows:

"(2) in any other case—

"(A) a fine under this title or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than five years, or both, for any subsequent offense under this subparagraph.".

(b) VOLUNTARY DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS.—Section 2702 of title 18, United States Code, is amended—

(1) by amending the catchline to read as follows:

"§ 2702. Voluntary disclosure of customer communications or records";

(2) in subsection (a)(1)—

(A) by striking "person or entity providing an" and inserting "provider of"; and

(B) by striking "and" at the end;

(3) in subsection (a)(2)—

(A) by striking "person or entity providing" and inserting "provider of"; and

(B) by striking the period at the end and inserting "; and";

(4) in subsection (a), by adding the following paragraph after paragraph (2):

"(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2) of this subsection) to any governmental entity.";

(5) in the heading of subsection (b) by inserting "FOR DISCLOSURE OF COMMUNICATIONS" after "EXCEPTIONS";

(6) in subsection (b), by striking "person or entity" and inserting "provider described in subsection (a)"; and

(7) by adding the following subsection after subsection (b):

"(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2) of this section)—

"(1) as otherwise authorized in section 2703 of this title;

"(2) with the lawful consent of the customer or subscriber;

"(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

"(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

"(5) to any person other than a governmental entity where not otherwise prohibited by law.".

(c) CONFORMING AMENDMENTS.—Section 2703 of title 18, United States Code, as amended by section 7 of this Act, is futher amended—

(1) in subsection (c) by—

(A) redesignating paragraph (2) as paragraph (3); and

(B) redesignating subparagraph (C) of paragraph (1) as paragraph (2);

(2) in subsection (c)(1) by—

(A) striking "(A) Except as provided in subparagraph (B)," and inserting "A governmental entity may require";

(B) striking "may disclose" and inserting "to disclose"; and

(C) striking "to any person other than a governmental entity.";

(D) striking "(B) A provider of" through "to a governmental entity";

(E) redesignating subclauses (i) through (iv) as subparagraphs (A) through (D);

(F) striking "or" at the end of subparagraph (C) as redesignated;

(G) striking the period at the end of subparagraph (D) as redesignated and inserting "; or"; and

(H) adding the following subparagraph after subparagraph (D) as redesignated:

"(E) seeks information pursuant to paragraph (2).";

(3) in subsection (c)(2) as redesignated by—

(A) striking "an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena" and inserting "a Federal or State grand jury or trial subpoena, or a subpoena or equivalent process authorized by a Federal or State statute,"; and

(B) striking "subparagraph (B)." and inserting "paragraph (1).".

(d) CIVIL DAMAGES.—Section 2707(c) of title 18, United States Code, is amended by striking "$1,000" and inserting "$5,000".

(e) CLERICAL AMENDMENT.—The item relating to section 2702 in the table of sections at the beginnning of chapter 121 of title 18, United States Code, is amended to read as follows:

"2702. Voluntary disclosure of customer communications or records.".

SEC. 11. ADDITIONAL PROVISIONS RELATING TO PEN REGISTERS.

(a) EMERGENCY PROVISIONS.—Section 3125 of title 18, United States Code, is amended—

(1) in subsection (a)(1)—

(A) in subparagraph (A), by striking "or" after the semicolon;

(B) in subparagraph (B), by striking the comma after "crime" and inserting a semicolon; and

(C) by inserting after subparagraph (B), the following:

"(C) an immediate threat to a national security interest; or

"(D) an ongoing attack on the integrity or availability of a protected computer in violation of section 1030(a)(5)(A)(i) or 1030(a)(5)(A)(ii) of this title,";

(2) at the end of the matter following subsection (a)(2), by inserting the following: "In the event an application for such order is denied, or in any other case where the installation and use of a pen register or trap and trace device is terminated without an order having been issued, any information obtained by such installation and use shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (b) of this section on the person named in the application.";

(3) by inserting the following after subsection (a):

"(b) Within a reasonable time but not later than 90 days after the filing of an application for an order of approval under subsection (a)(2) of this section which is denied, the denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to the information obtained by such installation and use of a pen register or trap and trace device as the judge may determine in his discretion is in the interest of justice, an inventory which shall include notice of—

"(1) the fact of the entry of the application;

"(2) the date of the entry and the date of the denial of the application; and

"(3) the fact that during the period covered by the application, information was obtained by the installation and use of a pen register or trap and trace device.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the applications as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed."; and

(4) by redesignating subsections (b) through (d) as subsections (c) through (e), respectively.

(b) DEFINITIONS.—Section 3127 of title 18, United States Code, is amended—

(1) in paragraph (6), by striking the period and inserting "; and"; and

(2) by adding the following paragraph after paragraph (6):

"(7) the term 'protected computer' has the meaning set forth in section 1030 of this title.".

SEC. 12. GOVERNMENT ACCESS TO CONTENTS OF STORED ELECTRONIC COMMUNICATIONS.

Section 2703(a) of title 18, United States Code, is amended by striking "one hundred and eighty days" each place it appears and inserting "one year".

SEC. 13. ENHANCED PRIVACY PROTECTION FOR INFORMATION ON COMPUTER NETWORKS.

Section 2510(17) of title 18, United States Code, is amended—

(1) by striking "and" at the end of subparagraph (A); and

(2) by inserting at the end the following:

"(C) any storage of an electronic communication by an electronic communication service without regard to whether the communication has been accessed by the intended recipient; and".

PURPOSE AND SUMMARY

H.R. 5018 balances the need for privacy and effective law enforcement in the digital age. H.R. 5018 protects privacy by raising the standard for the government's access to the transactional data regarding a person's communications obtained with so-called pen register or trap and trace devices; requiring the Federal Govern-

ment to report annually on the number of requests it makes to disclose the contents of stored electronic communications; expanding the statutory exclusionary rule to also exclude from use in evidence at trial electronic communications—including electronic communications such as e-mail that lies in storage with an electronic communications service—obtained in violation of Federal law, just as illegally obtained wire and oral electronic communications are currently excluded, while also allowing the use of such communications against those who illegally obtained them; prohibiting the government from obtaining a mobile phone user's location without first obtaining a court order based on probable cause, except in the case of certain emergency situations; requiring high-level Department of Justice approval for interceptions of electronic communications, as is currently required for interceptions of wire and oral communications; increasing the civil penalties that may be applied to those who illegally intercept electronic communications by raising the daily damages for each violation; making clear that protections of electronic communications in electronic storage cover e-mail messages that have been accessed by the intended recipient but remain stored by an electronic communications service; and extending the protection of a warrant requirement to electronic communications stored for 1 year or less.

H.R. 5018 helps law enforcement capture criminals in the computer age by allowing electronic communications service providers to disclose to law enforcement basic customer records, such as those including names and addresses, in certain emergency situations; allowing law enforcement to use devices that track the source and destination of criminal communications without a court order for up to 48 hours in situations involving national security and ongoing attacks on computer networks, but also requires that, if a court finds law enforcement had an insufficient basis to conduct the monitoring, the judge must order that the person whose communications were wrongfully tracked be notified; adding computer crimes to the enumerated offenses for which interceptions may be ordered; raising the maximum penalty for the most serious computer violations to 10 years in prison; allowing the Federal investigation and prosecution of those who deface or destroy information or images on computer systems without causing $5,000 in damages; amending the Federal sentencing guidelines such that only the most serious computer-related offenses are subject to a mandatory 6-month sentence; increasing criminal and civil penalties for the illegal disclosure of stored electronic communications; and applying criminal asset forfeiture provisions to computer crimes.

BACKGROUND AND NEED FOR THE LEGISLATION

Seventy years ago, Justice Brandeis, in his dissenting opinion in *Olmstead* v. *United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting), predicted that ongoing technological developments would someday enable law enforcement to search people or their property without physical trespass. He also cautioned that courts should be alert to these changes in technology in determining the contours of privacy rights. See *id.* at 472–73. Today, advances in telecommunications technology have dramatically changed people's lives. Internet technology has increased in popularity and has sig-

nificantly changed the way people handle their affairs, and consequently the government's handling of personal communications.[1]

PRIVACY IN THE DIGITAL AGE

The dramatic development of the Internet has transformed methods of gathering, processing and sharing information. In 1981, fewer than 300 computers were linked to the Internet. See *Reno* v. *ACLU*, 929 F. Supp. 824, 831 (E.D. Pa. 1996). In 1986—when the Electronic Communications Privacy Act became law—there were about 50,000. See *id.* By June 1996, there were over 9.4 million host computers worldwide linked to the Internet. A recent report by a White House Working Group states that:

> There can be little doubt that the Internet, a global electronic network of computer networks (including the World Wide Web) that connects people and information, has revolutionized and will continue to revolutionize how we communicate, educate ourselves, and buy and sell goods and services. The Internet has grown from 65 million users in 1998 to over 100 million users in the U.S. in 1999, or half the country's adult population; the number of Internet users in the U.S. is projected to reach 177 million by the end of 2003; and the number of Internet users worldwide is estimated to reach 502 million by 2003. Business-to-business electronic commerce totaled over $100 billion in 1999 (more than doubling from 1998) and is expected to grow to over $1 trillion by 2003.

Report, at 5.

The dramatic development of the Internet as a networked global communications medium, the expansion in the range of transactions that occur "on-line," and the amount of information now stored with third party Internet companies have produced a qualitative change in the nature of communications and, accordingly, in the nature and amount of the information that may be exposed to interception by the government.[2]

In light of these developments, existing statutes should be updated to appropriately balance the concerns of law enforcement—namely, the concern that they have sufficient authority to obtain the information they need in order to keep the public safe—with individuals' concerns that a sufficient degree of privacy and the in-

---

[1] As stated in a recent White House Working Group Report, "Regulation tied to a particular technology may quickly become obsolete and require further amendment. In particular, laws written before the widespread use of the Internet may be based on assumptions regarding then-current technologies and thus may need to be clarified or updated to reflect new technological capabilities or realities." *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, Report by the President's Working Group on Unlawful Conduct on the Internet (hereinafter "Report") at 13.

[2] As stated in the Report:

> Indeed, computers have made it possible for law enforcement agencies to gather some information that may not have been previously even maintained in the physical world. For example, an unsophisticated offender, even after "deleting" computer files (as opposed to destroying paper records), might leave evidence of unlawful activity that a trained computer forensic expert could recover. In addition, because an average computer with several gigabytes of memory can contain millions of pages of information, a law enforcement agent might, pursuant to lawful authority (such as a warrant), find volumes of information in one place. Of course, that information is only useful if there are trained computer experts on hand in a timely fashion, familiar with the relevant computer hardware or software configuration, to search the computer for specific information and to retrieve it in readable form.

Report, at 11.

tegrity of personal information are maintained in an age of modern communications and information storage.

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

Congress initially responded to the emergence of wireless communication services and the digital era by enacting the Electronic Communications Privacy Act ("ECPA") in 1986. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (codified in sections of 18 U.S.C. including §§ 2510–21, 2701–10, 3121–26). The Federal wiretap statute had been limited to voice communications. ECPA extended the wiretap provisions to include wireless voice communications and electronic communications such as e-mail or other computer-to-computer transmissions.[3] ECPA was intended to reestablish the balance between privacy and law enforcement, which Congress found had been upset to the detriment of privacy by the development of communications and computer technology and changes in the structure of the telecommunications industry. Among the developments noted by Congress were "large-scale electronic mail operations, cellular and cordless phones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of digitized networks." H.R. Rep. No. 99–647, at 18 (1986). Privacy, Congress concluded, was in danger of being gradually eroded as technology advanced. S. Rep. No. 99–541, at 2–3, 5 (1986); H.R. Rep. No. 99–647, at 16–19 (1986). See also H.R. Rep. No. 99–647, at 18 (stating that "[l]egal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology. ").

In addition to the goals of privacy and law enforcement, ECPA sought to advance the goal of supporting the development and use of these new technologies and services. See S. Rep. No. 99–541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems "). It was the intent of Congress to encourage the proliferation of new communications technologies, but it recognized that consumers would not trust new technologies if the privacy of those using them was not protected. See S. Rep. No. 99–541, at 5 (1986); H.R. Rep. No. 99–647, at 19 (1986).

ECPA was designed to provide rules for government surveillance in the modern age. However, technology has evolved in unanticipated ways. The interactive nature of the Internet, now including elements such as home banking and telecommuting, has produced an environment in which many people may spend hours each day "on-line." In this context, a person's electronic communications will encompass much more today than it would have in 1986.

A thorough examination of the effects of ECPA's rules governing governmental access to e-mail and other computer communications is made difficult because there is no publicly available data on which to base such an assessment. While the Federal wiretap pro-

[3] ECPA, in fact, did not extend all of the Federal wiretap protections to electronic communications. The court order authorizing the interception of electronic communications can be based upon suspected violations of any Federal felony, rather than the limited list of crimes that can serve as a predicate for telephone interceptions. See 18 U.S.C § 2516(3). In addition, no statutory exclusionary rule applies to non-voice interceptions that violate procedures required by statute. See 18 U.S.C. § 2515 (exclusionary rule only refers to wire or oral communications, not electronic communications).

visions require very detailed reports on interception of voice communications and interception of e-mail in transit, see 18 U.S.C. § 2519, there is no similar requirement for collecting and publishing information on the extent of government access to e-mail and other electronic communications while they are being stored by service providers following their transmission.[4]

GOVERNMENT ACCESS TO ELECTRONIC INFORMATION STORED BY THIRD PARTIES

In regard to e-mail and other electronic communications, ECPA has two purposes. First, ECPA outlaws most unauthorized private access to stored electronic communications. See 18 U.S.C. § 2701. Second, ECPA provides prerequisites for government access. See 18 U.S.C. § 2703.

Although ECPA provides some protection for e-mail and other forms of "electronic communication" held in "electronic storage," the law does not provide stored communications the same level of protection from government access that is afforded to wire or electronic communications in transit. See 18 U.S.C. §§ 2701–2711. Government access to communications in transit requires an intercept order issued pursuant to strict requirements.[5] However, in order for the government to immediately seize any "electronic communications"[6] in "electronic storage"[7] for 180 days or less requires only an ordinary warrant, and seizure of electronic communications in storage for more than 180 days[8] on an "electronic communications service,"[9] requires only a subpoena or an order issued pursuant to an offering of "specific and articulable" facts showing reasonable grounds to believe that the contents of an "electronic communication" are relevant to an ongoing criminal investigation. See 18 U.S.C. §§ 2703(a); 2703(b)(B)(ii); 2703(d). Thus, if the same information were stored in a home file cabinet for more than 180 days, Federal officials would be required to obtain a warrant after a stringent showing of "probable cause" to retrieve the information. 18 U.S.C. § 2703; 18 U.S.C. § 2516. A warrant is also not required

[4] Requirements regarding law enforcement's "interception" of electronic communications apply only to real-time monitoring of communications. As most electronic communications are stored immediately after their transmission, communications recovery of stored electronic communications is by far the easier and presumably the more common means of government's accessing electronic communications.

[5] See 18 U.S.C. § 2518(3) (requiring for a court order that "(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular [enumerated] offense . . .; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) . . . there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person").

[6] See 18 U.S.C. § 2510(12) ("electronic communication" means, with certain exceptions, "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce").

[7] See 18 U.S.C. § 2510(17) ("electronic storage" means "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication"). "[A]ny temporary, intermediate storage" describes an e-mail message that is being held by a third party Internet service provider until it is requested to be read.

[8] If the communication has been in electronic storage for 180 days or less, the government must obtain a warrant. See 18 U.S.C. § 2703(a).

[9] See 18 U.S.C. § 2510(15) ("electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications").

for the government to obtain the contents of electronic communications in a "remote computing service." See 18 U.S.C. §§ 2703(b); 2703(d); 2711(2) (the term "remote computing service" means "the provision to the public of computer storage or processing services by means of an electronic communications system"). Consequently, if the same information is stored by a third party in electronic form—unbeknownst to the deliverer or receiver of the information—rather than in a home file cabinet, Federal officials would be required to obtain a subpoena or an order, see 18 U.S.C. § 2703(b)(B)(ii), following a less rigorous showing of need, to retrieve this same information and subject to a delay in notice to the target for up to 90 days if a court determines that notification may, among other things, "seriously jeopardize an investigation." 18 U.S.C. § 2705.

H.R. 5018 WOULD REQUIRE THE FEDERAL GOVERNMENT TO REPORT BASIC INFORMATION REGARDING ITS REQUESTS FOR THE DISCLOSURE OF STORED ELECTRONIC COMMUNICATIONS

Personal information in people's homes and file cabinets are protected by a warrant requirement and it is clear when the government searches through such materials pursuant to a warrant. Today, as much of that very same information gravitates toward new locations on the Internet's landscape, such as the networks of Internet service providers and other third parties, it is available to law enforcement under lower legal standards, without contemporaneous notice, and often without any notice at all in the case of innocent parties whose stored electronic communications have been disclosed. See 18 U.S.C. §§ 2703; 2705. In order to provide some opportunity for oversight, H.R. 5018 would require the Federal Government to produce annual reports regarding its requests for orders for the disclosure of the contents of electronic communications, such as the contents of stored e-mails, similar to but less detailed than the disclosure requirements the Federal Government must meet under 18 U.S.C. § 2519 regarding the use of electronic wiretaps to intercept telephone conversations. H.R. 5018 provides for the enumeration of basic information relating to requests for the disclosure of the contents of stored electronic communications under 18 U.S.C. §§ 2703(a) and (b)—such as the number of such requests made and the approximate number of incriminating and non-incriminating communications disclosed—to help further Congress' oversight responsibilities and provide the public with a certain level of comfort that the disclosure of the contents of electronic communications is reasonably proportionate to the needs of law enforcement. These reporting requirements will not unduly burden law enforcement.

The committee recognizes that this bill imposes reporting requirements on the Administrative Office of the U.S. Courts that will require the hiring of four additional analysts. This committee urges Congress to appropriate sufficient funds for the Administrative Office of the U.S. Courts to comply with the reporting requirements contained in this bill.

H.R. 5018 RAISES THE STANDARD THE GOVERNMENT MUST MEET TO OBTAIN INFORMATION UNDER THE PEN REGISTER ACT

H.R. 5018 would also amend the standard that must be met by the government before transactional information, such as the numbers dialed to and from a telephone, may be obtained under the Pen Register Act.

The Pen Register Act, enacted when the telephone was the predominant mode of distance communication, currently allows the government to obtain, with a so-called "pen register," the "electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line" and, with a so-called "trap and trace device," the "electronic or other impulses which identify the originating number" of the device from which a wire or electronic communication was transmitted. 18 U.S.C. §§ 3127(3); 3127(4). The government can obtain this information if a government attorney has simply "certified" to the court "that the information likely to be obtained by such installation and use [of the pen register or trap and trace device] is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a). Upon such "certification" by a government official, the court "shall" issue the order. 18 U.S.C. § 3123(a).

Authority under the Pen Register Act is also used by the government to obtain e-mail addresses sent and received.[10] Officials from the Justice Department and the Federal Bureau of Investigation have testified before the Constitution Subcommittee that the Pen Register Act grants the government the authority to capture e-mail addresses as well as telephone numbers. See Hearing Transcript, "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program" (July 24, 2000) at 37–39 (testimony of Dr. Donald Kerr, Director, Lab Division, Federal Bureau of Investigation, and Christopher Painter, Deputy Chief, Computer Crimes and Intellectual Property Section, Department of Justice). Unlike a telephone number, however, an e-mail address often indicates not only the identity of the person communicating, but also their place of work, as in the e-mail address JohnSmith@work.com.

H.R. 5018 would require that, before a pen register or trap and trace device could be ordered installed, the government must first demonstrate to an independent judge that "specific and articulable facts reasonably indicate that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use [of a pen register or trap and trace device] is relevant to an investigation of that crime." The standard that "specific and articulable facts reasonably indicate that a crime has been, is being, or will be committed" is well supported in the law, and in current practice. Indeed, the standard is that which the nation's primary investigative agency, the Federal Bureau of Investigation, must meet each time it initiates an investigation.

The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations ("Guidelines"), as in effect today and last revised by Attorney General Thornburgh in March, 1989, apply to the Federal Bureau of Investigation, which the Guidelines describes as "the primary in-

[10] Although the authority for such use of pen registers is not without doubt, H.R. 5018 does not attempt to resolve this debate.

vestigative agency in the Federal Government." Guidelines, at 1. The Guidelines state:

> Investigations by the FBI are premised upon the important duty of government to protect the public against general crimes, against organized criminal activity, and against those who would engage in political or racial terrorism or would destroy our constitutional system through criminal violence. At the same time, that duty must be performed with care to protect individual rights and to ensure that investigations are confined to matters of legitimate law enforcement interest . . . [I]nvestigations governed by these Guidelines are conducted for the purpose of preventing, detecting, or prosecuting violations of Federal law. They shall be conducted with as little intrusion into the privacy of individuals as the needs of the situation permit.

Id. at 1, 3.

The Guidelines make clear that certain types of investigative techniques "shall not" be used prior to initiating an investigation, including "mail covers" and "[n]onconsensual electronic surveillance." *Id.* at 5. The Guidelines also make clear that "[a] general crimes investigation may be initiated by the FBI" only when "facts or circumstances reasonably indicate that a Federal crime has been, is being, or will be committed." *Id.* at 7.[11] Further, the Guidelines state that "[t]he standard of 'reasonable indication' is substantially lower than probable cause . . . However, the standard does require *specific facts or circumstances* indicating a past, current, or impending violation. There must be an objective, factual basis for initiating the investigation; a mere hunch is insufficient." *Id.* (Emphasis added).[12]

Kevin DiGregory, Deputy Assistant Attorney General, noted in written testimony before the Constitution Subcommittee, that "H.R. 5018 would require such [pen register or trap and trace] applications to contain 'specific and articulable facts' that would justify the collection of the data" and that "the Justice Department *can* comply with the added administrative burdens imposed by increasing this standard [to the standard imposed by H.R. 5018]." Written Testimony of Kevin DiGregory provided to the Constitution

---

[11] Current law requires that an order permitting the installation and use of a pen register or trap and trace device be granted only when there is "an ongoing criminal investigation." 18 U.S.C. § 3123(a).

[12] The phrase "specific and articulable facts" is also a central part of the Supreme Court's opinion in *Terry* v. *Ohio*, 392 U.S. 1, 21 (1968), and it has been seen by subsequent courts as a central part of the *Terry* standard:

> [T]here is no ready test for determining reasonableness other than by balancing the need to search (or seize) against the invasion which the search (or seizure) entails. And in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion . . . Anything less would invite intrusions upon constitutionally guaranteed rights based on nothing more substantial than inarticulate hunches, a result this Court has consistently refused to sanction.

Terry v. *Ohio*, 392 U.S. 1, 21 (1968) (citations and quotation marks omitted).

The footnote at this point of the opinion states, "This demand for specificity in the information upon which police action is predicated is the central teaching of this Court's Fourth Amendment jurisprudence." *Id.* at n.18. Numerous subsequent cases applying and amplifying on the *Terry* standard include the phrase "specific and articulable facts." See, e.g., *Maryland* v. *Buie*, 494 U.S. 325, 327 (1990); *Michigan* v. *Long*, 463 U.S. 1032, 1049–1050 (1983) (quoting *Terry* v. *Ohio*, 392 U.S. 1, 21 (1968)).

Subcommittee, "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program" (July 24, 2000) (Emphasis added.).

H.R. 5018 WOULD REQUIRE HIGH-LEVEL DEPARTMENT OF JUSTICE APPROVAL FOR FEDERAL INTERCEPTIONS OF ELECTRONIC COMMUNICATIONS

H.R. 5018 expands 18 U.S.C. § 2516(1) to apply the existing requirements for authorizing the interception of wire and oral communications to the authorization of the interception of electronic communications. These requirements are that of high-level official approval and the investigation of an enumerated offense. In addition, because the investigation of crimes that involve computers and interstate communications systems often require the interception of electronic communications, H.R. 5018 adds such crimes to the list of predicate offenses in 18 U.S.C. § 2516(1).

H.R. 5018 WOULD REQUIRE THE GOVERNMENT TO OBTAIN A WARRANT TO SEIZE E-MAIL MESSAGES STORED FOR ONE YEAR OR LESS

H.R. 5018 requires that the government obtain a warrant to require the disclosure of electronic communications in electronic storage—namely, an e-mail message stored by an Internet service provider—if the communication sought has been stored for 1 year or less, as opposed to the current requirements for a warrant to disclose electronic communications in electronic storage for 180 days or less. H.R. 5018 also clarifies that an electronic communication in "electronic storage" enjoys the protections provided to such communications regardless of whether or not the communication has been "opened" or otherwise accessed by the intended recipient. This would extend ECPA's protections governing electronic communications in electronic storage, for example, to the electronic communications of those who use Web-based electronic communications services, which often remotely store communications in a third party network even after the messages have been accessed by the recipient.

H.R. 5018 WOULD EXTEND THE STATUTORY EXCLUSIONARY RULE TO COVER ILLEGALLY INTERCEPTED ELECTRONIC COMMUNICATIONS AND ILLEGALLY DISCLOSED ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE

The statutory exclusionary rule provides that "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding . . . if the disclosure of that information would be in violation of this chapter." 18 U.S.C. § 2515. This "exclusionary rule" allows individuals about whom information has been gathered in violation of Federal law to rely on the exclusion of such information from evidence by statute, thereby relieving them of the need to litigate whether or not the action that resulted in the gathering of such information constituted an "unreasonable search or seizure" under the Fourth Amendment. Currently, only illegally obtained "wire and oral communications" are excluded from use as evidence by statute. H.R. 5018 would amend the "statutory exclusionary rule" to also exclude from use as evidence illegally intercepted

"electronic communications" and illegally obtained "electronic communications in electronic storage," namely stored e-mail messages, resulting from violations the Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.*

H.R. 5018 also allows the introduction of intercepted or disclosed communications where an individual violates 18 U.S.C. chapters 119, governing the interception of communications, or 121, governing the disclosure of stored electronic communications, by engaging in illegal communications interception or disclosure and the government seeks to use the communication for the limited purpose of prosecuting that violator. Conforming amendments are also made to 18 U.S.C. §§ 2517 and 2518(10)(a).

Some in the law enforcement community have expressed concern that the statutory exclusionary rule does not contain a good faith exception and therefore could result in the exclusion of evidence based on technical violations. However, even in the context of statutory exclusion, courts have held that when there is a violation of Federal wiretap laws that is of a constitutional magnitude, the good faith exception does apply. Thus, the good faith exception has been applied to the failure of a judge to sign the wiretap order, *United States* v. *Moore*, 41 F.3d 370, 375 (8th Cir. 1994), to inadequacies in the probable cause showing, *United States* v. *Millan*, 817 F.Supp. 1072, 1078 (S.D.N.Y. 1993) ("Even if probable cause is found lacking, the wiretap order should be suppressed only where: (1) the issuing judge abandoned his or her detached, neutral role; (2) the agent was dishonest or reckless in preparing the affidavit supporting the issuance of the wiretap order; or (3) the agent's reliance on the warrant was not objectively reasonable."), and to other defects. See, e.g., *United States* v. *Ferrara*, 771 F.Supp. 1266, 1314 (D. Mass 1991) (finding that even if application for warrant to conduct roving electronic surveillance to intercept certain criminal communications of some members of suspected organization were required to disclose other authorizing electronic surveillance of other members of that same suspected organization, failure to disclose that surveillance would not justify suppression of evidence obtained pursuant to warrant because other authorizing surveillance was not disclosed because affiant had good faith belief such disclosure was not legally required and it was in best interests of investigation not to divulge them gratuitously) (citing 18 U.S.C. § 2518(1)(c), (11)(a)).

Moreover, as to nonconstitutional violations of the Federal wiretap laws, the Supreme Court has held that evidence cannot be excluded under 18 U.S.C. § 2515 for minor or technical violations. The Court held in *United States* v. *Giordano*, 416 U.S. 505, 527 (1994) that suppression under 18 U.S.C. § 2515 is required only for "failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative technique." In determining whether suppression is warranted, courts must examine whether the violated statutory requirement occupies "a central role in the statutory scheme." *Id.* at 528 (holding that, although wiretap application had been approved by the Executive Assistant to the Attorney General rather than by Attorney General himself or a designated Assistant Attorney General, application on its face

identified Assistant Attorney General as authorizing application, and wiretap materials were not subject to statutory exclusionary rule). See also *United States* v. *Chavez*, 416 U.S. 562, 578 (1974) (misidentification of officer authorizing wiretap application did not affect the fulfillment of any of the reviewing or approval functions required by Congress and therefore was not "unlawful" under the Federal wiretap laws and subject to statutory exclusionary rule). Thus, as one leading treatise states, "many violations of the requirements of Title III [the Federal wiretap statute] will lead to either no suppression or only partial suppression . . . In most jurisdictions there are relatively few violations which will lead to the ultimate and absolute sanction of complete suppression of all surveillance evidence . . . In many instances the government has disregarded procedural protections established by Section 2518 without affecting the admissibility of the eavesdropping evidence." James G. Carr, *The Law of Electronic Surveillance*, § 6.3 (1995).

H.R. 5018 WOULD REQUIRE THE GOVERNMENT TO MEET A PROBABLE CAUSE STANDARD TO OBTAIN INFORMATION DISCLOSING THE PHYSICAL LOCATION OF MOBILE PHONE USERS, WITH CERTAIN EXCEPTIONS

Location tracking of users of wireless communications services is an emerging concern. Wireless telephones, which are increasingly used, generate information that can be used to physically track the movement of users. Initially limited to cell site antenna location, this tracking data is becoming more sophisticated with the introduction of new technologies. Still, persons in emergency situations want to be found when they call emergency services such as "911," and the government should have the ability to locate suspected criminals in those circumstances. Currently, there are no clear legal standards governing when the government can collect location information from cell phone companies. Law enforcement now uses its authority under 18 U.S.C. § 2703(d) (requirements for government access to business "records") to obtain location information from mobile phone service providers. However, 18 U.S.C. § 2703(d) does not contain any emergency exceptions to its requirements.

H.R. 5018 provides that the government must show probable cause before it may obtain information disclosing the location of a customer or user of a mobile phone from a mobile phone service provider. Certain exceptions to this provision are provided in the bill for disclosing such information to emergency service providers such as hospitals, or to the legal guardian or members of the user's immediate family in situations involving the risk of death or serious physical harm, or with the express consent of the user of the mobile phone equipment. These exceptions are based on 47 U.S.C. § 222, which already prohibits cell phone companies from disclosing customer location information to marketers and other commercial entities without express customer consent or under other exceptions. See 47 U.S.C. § 222(d).

H.R. 5018 WOULD INCREASE PENALTIES FOR ILLEGALLY INTERCEPTING OR DISCLOSING ELECTRONIC COMMUNICATIONS

H.R. 5018 contains provisions that increase the minimum damages that may be awarded under 18 U.S.C. § 2520 to those whose

electronic communications were illegally intercepted from $100 per day per violation, to $500 per day per violation.

H.R. 5018 also contains provisions raising the minimum criminal penalties under 18 U.S.C. § 2701 for the illegal disclosure of stored electronic communications from one to 3 years for first time offenses, and from two to 5 years for repeat offenses involving the disclosure of stored electronic communications for tortious or illegal purposes, commercial advantage, malicious destruction or damage, or private commercial gain. H.R. 5018 also increases the minimum civil damages available under 18 U.S.C. § 2707 to those whose stored electronic communications are illegally disclosed. from $1,000 to $5,000. An increase in the penalties for such violations is appropriate, considering that more and more sensitive and personal information is gravitating from citizens' file cabinets to computing services on third party networks.

LAW ENFORCEMENT CONCERNS: INVESTIGATING AND PROSECUTING CRIMINALS IN THE DIGITAL AGE

The new digital age has spawned new digital crimes. As stated by a recent White House Working Group Report, "Prior technological advances—the automobile, the telegraph, and the telephone, for example—have brought dramatic improvements for society, but have also created new opportunities for wrongdoing. The same is true of the Internet, which provides unparalleled opportunities for socially beneficial endeavors such as education, research, commerce, entertainment, and debate on public affairs in ways that we may not now even be able to imagine. By the same token, however, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive, and potentially anonymous way to commit unlawful acts, such as fraud, the sale or distribution of child pornography, the sale of guns or drugs or other regulated substances without regulatory protections, and the unlawful distribution of computer software or other creative material protected by intellectual property rights." Report, at 4.

As described in the Report, "These needs and challenges are not theoretical. Law enforcement agencies today, for example, are faced with the need to evaluate and to determine the source, typically on very short notice, of anonymous e-mails that contain bomb threats against a given building or threats to cause serious bodily injury." *Id.* H.R. 5018 contains several provisions that would help law enforcement meet these new needs and challenges.

H.R. 5018 WOULD ALLOW THE DISCLOSURE OF BASIC CUSTOMER RECORDS BY ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS IN EMERGENCY SITUATIONS

H.R. 5018 would grant electronic communications service providers the right, but not impose on them the obligation, to disclose basic customer records in emergency situations. Under current law, an electronic communications service provider may disclose the *contents* of a communication under 18 U.S.C. § 2702(b)—for example, the substance of an e-mail message—to (1) an addressee or intended recipient of such communication; (2) with the lawful consent of the originator or an addressee; (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or

property of the provider of that service; or (4) to a law enforcement agency if the contents appear to pertain to the commission of a crime. Under current law, however, if an Internet service provider's customer receives an e-mail containing a death threat from another customer of the same Internet service provider, the provider is limited in what actions it may take. It may disclose the contents of a communication to law enforcement under 18 U.S.C. § 2703(b)(3), but current law does not expressly authorize a provider to voluntarily provide to law enforcement the identity, home address, and other basic subscriber information of the user making the threat. See 18 U.S.C. § 2703(c)(1)(B) and (C) (permitting disclosure to government entities only in response to legal process).

As law enforcement already has the appropriate authority to disclose the *contents* of customer communications in such circumstances, it is appropriate to allow providers to disclose customer records, which are *not* content, in certain emergency situations, as the right to disclose the contents of communications implies the less intrusive ability to disclose non-content records. H.R. 5018 would allow providers to disclose non-content customer records, including a subscriber's login records, with the lawful consent of the customer or subscriber; as may be necessarily incident to the rendition of service or to the protection of the rights or property of the provider of that service; or to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information. Furthermore, providers should have the right to disclose the facts surrounding attacks on their systems. When an authorized user of an Internet service launches a network intrusion against their Internet service provider, the provider should have the legal right to report the complete details of the crime to law enforcement.

H.R. 5018 WOULD ALLOW LAW ENFORCEMENT TO INSTALL PEN REGISTER AND TRAP AND TRACE DEVICES WITHOUT A COURT ORDER IN EMERGENCY SITUATIONS INVOLVING THREATS TO NATIONAL SECURITY AND ONGOING ATTACKS ON COMPUTER NETWORKS

Existing law empowers law enforcement to use trap and trace devices in emergency situations—such as when it encounters an immediate danger of death or serious bodily injury or when it is investigating organized crime—without getting prior approval from a court. Law enforcement authorities must then obtain court approval within 48 hours. H.R. 5018 would create two more emergency exceptions, those involving immediate threats to national security corresponding to the emergency wiretap provisions at 18 U.S.C. § 2518(7)(a)(ii), and investigations of ongoing intrusions into computer networks. In the latter case, rapid investigative response is made essential by the speed with which, for example, computer viruses are spread through a computer network. In many cases, if investigators cannot trace the computer criminal while the criminal is actively connected to the computers being attacked, it may prove impossible to do so afterwards. Any abuse of these or the other emergency provisions would be deterred by the provisions in H.R. 5018 requiring that when a court determines that law enforcement did not act reasonably under these emergency provisions, the person regarding whom information had been gathered must be noti-

fied, just as such notification is provided for when the emergency provisions of the Federal wiretap law are found by a court to have been exercised inappropriately. See 18 U.S.C. § 2518(7)(b).

H.R. 5018 WOULD RAISE PENALTIES AND EXPAND FEDERAL JURISDICTION OVER SERIOUS COMPUTER CRIMES AND AMEND THE SENTENCING GUIDELINES SUCH THAT ONLY THE MOST SERIOUS COMPUTER CRIME VIOLATIONS ARE SUBJECT TO MANDATORY SIX-MONTH SENTENCES

H.R. 5018 would raise the maximum penalty, from five to 10 years, for computer crime felony violations that are knowingly and intentionally committed and which cause severe damage to governmental and private computer systems. Currently, a first time offense for such felonies could be met with a maximum of 5 years in prison. H.R. 5018 raises that minimum penalty to 10 years. The current 5 year maximum does not adequately take into account the seriousness of these crimes. For example, David Smith recently pled guilty to committing such serious felony offenses for releasing the "Melissa" virus in 1999, which caused massive damage to thousands of computers across the Internet. Although Smith agreed as part of his plea that his conduct caused over $80 million worth of damage—the maximum dollar figure contained in the Sentencing Guidelines—estimates of the real amount of damage have run much higher. See T. Brune, "Cyber-Crooks Elude Justice, Just a Handful Get Punished," *Newsday* (February 25, 2000) at A7. H.R. 5018 also creates a Federal offense when an attack on a protected computer modifies or impairs, or threatens to modify or impair, the medical examination, diagnosis, treatment, or care of one or more individuals, causes physical injury to any individual, or threatens public health or safety. H.R. 5018 also creates a new category of felony violations where a hacker causes damage to a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security. Attacks on computers used in the nation's defense that occur during periods of active military engagement are particularly serious, even if they do not disrupt the military's defense capabilities, because they divert time and attention away from the military's proper objectives.

Further, H.R. 5018 clarifies that damage to multiple protected computers must be aggregated in determining whether a violation has exceeded the $5,000 threshold for a Federal offense. For example, a person may unlawfully access five computers on a network on 10 different dates but cause only $1,000 damage to each computer during each intrusion. H.R. 5018 would allow a count to be brought for the full $50,000 of damage caused by the individual. Aggregating the damage caused to the various computers properly measures an individual's culpability for such conduct. This would bring the statute into harmony with others permitting the aggregation of related conduct in determining the level of culpability. See, e.g., *United States* v. *Griffith*, 17 F.3d 865 (6th Cir. 1994) (value of various shipments of stolen property, none of which was valued at $5,000, was properly aggregated in determining whether government met $5,000 jurisdictional requirement for felony interstate transportation of stolen goods).

H.R. 5018 would also apply the criminal forfeiture rules to computer hacking crimes and require anyone convicted of a violation of the computer crime laws to forfeit to the United States property used or proceeds gained in the commission of the crime. It is the experience of law enforcement that forfeiture of property used in the commission of computer crime or proceeds derived therefrom can provide effective punishment and deterrence, and that it makes little sense to return computers to convicted computer criminals. These criminal forfeiture provisions are based on the familiar forfeiture procedures set forth in section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970, 21 U.S.C. § 853.

H.R. 5018 also expressly defines the term "loss" as used in the statute to account for a wide range of possible harms done to the victims of computer crimes, including reasonable costs of responding to the offense, conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue or costs incurred because of the interruption of service.

H.R. 5018 also allows the Federal Government to investigate and prosecute offenses in which a person intentionally defaced, damaged or destroyed images or information made available to the public, such as the defacing of images or information on Web sites, even if such offenses did not result in more than $5,000 in damages. This provision responds to a serious problem that came to the attention of the committee when the Web site of a non-profit organization became the victim of a computer hacking attack in which educational material was removed and replaced with images of a bomb, skull and crossbones, obscenities, and links to Web sites that espouse contrary points of view. The hackers also violated the privacy of a number of visitors to the Web site by stealing all of the e-mails sent to the site. In response to a request by the committee's ranking member to the Department of Justice, seeking an investigation into the Web site attack, the Department responded that limitations in existing law precluded an investigation because the resulting damage to the site was less than the $5,000 Federal jurisdictional limit. This kind of Web site attack prevents a non-profit organization from using the Internet as a forum for its free expressive activities, and a criminal who carries out such activities in cyberspace should be treated similarly to a criminal who steals a non-profit organization's direct mail shipments or replaces an organization's national radio advertisements with its own. To that end, this provision extends Federal jurisdiction to the investigation and prosecution of intentional efforts to deface, damage, or destroy images or information made available to the public and protected by the first amendment. This provision, however, would not apply to expression on the Internet that does not deface, damage, or destroy other expression, such as e-mails sent which may express views contrary to those expressed elsewhere on a Web site but which do not intentionally deface, damage or destroy such expression.

Finally, H.R. 5018 would give prosecutors more flexibility in charging computer criminals. Section 805 of the Antiterrorism and Effective Death Penalty Act of 1996 transmitted a directive to the Sentencing Commission to ensure that all individuals convicted of a violation of 18 U.S.C. § 1030(a)(4) or (a)(5) be imprisoned for not less than 6 months. A mandatory 6 month sentence, however, may be inappropriate for violations of the least serious computer hack-

ing offenses, which apply to those who have intentionally accessed a protected computer, but did not intend to cause damage. Consequently, prosecutors may be reluctant to charge those committing these less serious hacker violations when the minimum sentence is 6 months in prison. In those cases in which mandatory imprisonment for 6 months might not be the most appropriate remedy, it is nonetheless best that Federal conviction occur. A conviction, even one not resulting in mandatory imprisonment, will become part of a defendant's criminal history and qualify the defendant for the more substantial recidivist provisions of the computer crime laws if the defendant does not reform after the first conviction. H.R. 5018 restricts the 6 month minimum sentence to only the more serious computer crimes and better ensures that the punishment fits the crime.

HEARINGS

The committee's Subcommittee on the Constitution held 3 days of hearings on issues addressed by H.R. 5018 on April 6, 2000, July 24, 2000 and September 6, 2000. On April 6, 2000, testimony was received from several witnesses: James X. Dempsey, Senior Staff Counsel, The Center for Democracy and Technology; Gregory Nojeim, Legislative Counsel, American Civil Liberties Union, Washington National Office; Kevin V. DiGregory, Deputy Associate Attorney General, Department of Justice; accompanied by David Green, Deputy Chief, Computer Crime and Intellectual Property Section, Department of Justice; Stewart Baker, Steptoe & Johnson; Frederick Juergens Baker, Chair, Internet Engineering Task Force; Clifford S. Fishman, Professor of Law, Columbus School of Law, The Catholic University of America; Robert Corn-Revere, Hogan & Hartson; Jeff B. Richards, Executive Director, Internet Alliance; Nicole Wong, Perkins Coie, San Francisco; and Jeffrey Rosen, Associate Professor of Law, The George Washington University Law School.

On July 24, 2000, testimony was received from several witnesses: Dr. Donald M. Kerr, Director, Lab Division, Federal Bureau of Investigation; Larry R. Parkinson, General Counsel, Federal Bureau of Investigation; Kevin V. DiGregory, Deputy Associate Attorney General, Department of Justice; Alan Davidson, Staff Counsel, The Center for Democracy and Technology; Matt Blaze, Research Scientist; Barry Steinhardt, Associate Director, American Civil Liberties Union; Robert Corn-Revere, Attorney, Hogan & Hartson; Stewart Baker, Attorney, Steptoe & Johnson; Peter William Sachs, ICONN, L.L.C.; and Tom Perrine, Principal Investigator, Pacific Institute for Computer Security.

On September 6, 2000, testimony was received from the following witnesses: Kevin DiGregory, Deputy Associate Attorney General, Department of Justice; accompanied by David Green, Deputy Chief, Computer Crime and Intellectual Property Section; James Dempsey, Senior Staff Counsel, The Center for Democracy and Technology; Gregory Nojeim, Legislative Counsel, the American Civil Liberties Union; Robert Corn-Revere, Hogan & Hartson; and Marc Rotenberg, Director, Electronic Privacy Information Center.

COMMITTEE CONSIDERATION

On September 14, 2000, the Subcommittee on the Constitution met in open session and ordered favorably reported the bill H.R.5018 with an amendment in the nature of a substitute, by a voice vote, a quorum being present. On September 20 and 26, 2000, the committee met in open session and ordered favorably reported the bill H.R. 5018 with an amendment in the nature of a substitute by a recorded vote of 20 to 1, a quorum being present.

VOTES OF THE COMMITTEE

1. Mr. Scott Amendment to H.R. 5018 which removed provisions allowing the Federal investigation and prosecution of computer crimes committed by juveniles passed favorably by a voice vote.

2. On September 20, 2000, Mr. Barr offered an amendment that would extend the warrant requirement to the disclosure of electronic communications in electronic storage for 1 year or less. This amendment was defeated by a rollcall vote of 10 to 10.

ROLLCALL NO. 1

	Ayes	Nays	Present
Mr. Sensenbrenner	X		
Mr. McCollum			
Mr. Gekas			
Mr. Coble		X	
Mr. Smith (TX)			
Mr. Gallegly		X	
Mr. Canady		X	
Mr. Goodlatte			
Mr. Chabot		X	
Mr. Barr	X		
Mr. Jenkins	X		
Mr. Hutchinson		X	
Mr. Pease	X		
Mr. Cannon		X	
Mr. Rogan			
Mr. Graham			
Ms. Bono		X	
Mr. Bachus			
Mr. Scarborough	X		
Mr. Vitter			
Mr. Conyers	X		
Mr. Frank			
Mr. Berman			
Mr. Boucher			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt		X	
Ms. Lofgren			
Ms. Jackson Lee	X		
Ms. Waters	X		
Mr. Meehan			
Mr. Delahunt			
Mr. Wexler			
Mr. Rothman		X	
Ms. Baldwin			
Mr. Weiner			
Mr. Hyde, Chairman		X	
Total	10	10	

3. At the next Full Committee meeting, Mr. Cannon moved to reconsider the vote by which the Barr amendment was defeated. The motion to reconsider was agreed to by voice vote, and the Barr amendment was agreed to by voice vote.

4. Mr. Conyers offered an amendment which would make it a Federal offense to deface or destroy information or images on computer systems even if the resulting damage does amount to $5,000 or more. Passed by voice vote.

5. Mr. Nadler, Mr. Conyers and Mr. Barr offered an amendment which would add to the definition of "electronic storage" those communications stored by an electronic communications service without regard to whether they had been accessed by the intended recipient. Passed favorably by voice vote.

6. Mr. Nadler and Mr. Barr offered an amendment which would add provisions to the Federal reporting requirements. This amendment was defeated by a rollcall vote of 9 to 16.

ROLLCALL NO. 2

	Ayes	Nays	Present
Mr. Sensenbrenner			
Mr. McCollum			
Mr. Gekas		X	
Mr. Coble	X		
Mr. Smith (TX)		X	
Mr. Gallegly		X	
Mr. Canady		X	
Mr. Goodlatte		X	
Mr. Chabot		X	
Mr. Barr	X		
Mr. Jenkins		X	
Mr. Hutchinson		X	
Mr. Pease		X	
Mr. Cannon			
Mr. Rogan		X	
Mr. Graham		X	
Ms. Bono			
Mr. Bachus			
Mr. Scarborough			
Mr. Vitter			
Mr. Conyers	X		
Mr. Frank	X		
Mr. Berman			
Mr. Boucher			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren		X	
Ms. Jackson Lee		X	
Ms. Waters	X		
Mr. Meehan			
Mr. Delahunt			
Mr. Wexler			
Mr. Rothman		X	
Ms. Baldwin	X		
Mr. Weiner		X	
Mr. Hyde, Chairman		X	
Total	9	16	

7. Ms. Lofgren offered an amendment which would extend the statutory exclusionary rule to exclude from evidence illegally dis-

closed electronic communications in electronic storage. This amendment was agreed to by a rollcall vote of 9 to 7.

ROLLCALL NO. 3

	Ayes	Nays	Present
Mr. Sensenbrenner			
Mr. McCollum			
Mr. Gekas			
Mr. Coble		X	
Mr. Smith (TX)		X	
Mr. Gallegly			
Mr. Canady		X	
Mr. Goodlatte			
Mr. Chabot			
Mr. Barr	X		
Mr. Jenkins		X	
Mr. Hutchinson		X	
Mr. Pease	X		
Mr. Cannon			
Mr. Rogan			
Mr. Graham		X	
Ms. Bono			
Mr. Bachus			
Mr. Scarborough	X		
Mr. Vitter			
Mr. Conyers			
Mr. Frank			
Mr. Berman	X		
Mr. Boucher			
Mr. Nadler	X		
Mr. Scott			
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters	X		
Mr. Meehan			
Mr. Delahunt			
Mr. Wexler			
Mr. Rothman	X		
Ms. Baldwin			
Mr. Weiner			
Mr. Hyde, Chairman		X	
Total	9	7	

8. Ms. Waters offered an amendment which would require notification to all those whose communications had been traced under an order for the installation of a pen register or trap and trace device. The amendment was defeated by a rollcall vote of 9 to 12.

ROLLCALL NO. 4

	Ayes	Nays	Present
Mr. Sensenbrenner			
Mr. McCollum			
Mr. Gekas			
Mr. Coble		X	
Mr. Smith (TX)		X	
Mr. Gallegly		X	
Mr. Canady		X	
Mr. Goodlatte			
Mr. Chabot		X	
Mr. Barr	X		
Mr. Jenkins		X	

ROLLCALL NO. 4—Continued

	Ayes	Nays	Present
Mr. Hutchinson		X	
Mr. Pease		X	
Mr. Cannon		X	
Mr. Rogan		X	
Mr. Graham			
Ms. Bono			
Mr. Bachus			
Mr. Scarborough	X		
Mr. Vitter			
Mr. Conyers			
Mr. Frank			
Mr. Berman	X		
Mr. Boucher			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters	X		
Mr. Meehan			
Mr. Delahunt			
Mr. Wexler			
Mr. Rothman		X	
Ms. Baldwin			
Mr. Weiner	X		
Mr. Hyde, Chairman		X	
Total	9	12	

9. Motion to report favorably to the House the bill H.R. 5018, with an amendment in the nature of a substitute was agreed to by a rollcall vote of 20 to 1.

ROLLCALL NO. 5

	Ayes	Nays	Present
Mr. Sensenbrenner			
Mr. McCollum			
Mr. Gekas			
Mr. Coble	X		
Mr. Smith (TX)	X		
Mr. Gallegly	X		
Mr. Canady	X		
Mr. Goodlatte			
Mr. Chabot	X		
Mr. Barr	X		
Mr. Jenkins	X		
Mr. Hutchinson	X		
Mr. Pease	X		
Mr. Cannon	X		
Mr. Rogan			
Mr. Graham	X		
Ms. Bono			
Mr. Bachus			
Mr. Scarborough	X		
Mr. Vitter			
Mr. Conyers			
Mr. Frank			
Mr. Berman	X		
Mr. Boucher			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		

ROLLCALL NO. 5—Continued

	Ayes	Nays	Present
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters	X		
Mr. Meehan			
Mr. Delahunt			
Mr. Wexler			
Mr. Rothman	X		
Ms. Baldwin			
Mr. Weiner		X	
Mr. Hyde, Chairman	X		
Total	20	1	

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the committee reports that the findings and recommendations of the committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

COMMITTEE ON GOVERNMENT REFORM FINDINGS

No findings or recommendations of the Committee on Government Reform were received as referred to in clause 3(c)(4) of rule XIII of the Rules of the House of Representatives.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of House Rule XIII is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the committee sets forth, with respect to the bill, H.R. 5018, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 3, 2000.

Hon. HENRY J. HYDE, *Chairman,*
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5018, the Electronic Communications Privacy Act of 2000.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Hadley, who can be reached at 226–2860.

Sincerely,

Enclosure

cc: Honorable John J. Conyers Jr.
Ranking Democratic Member

H.R. 5018—Electronic Communications Privacy Act of 2000.

Based on information from the Department of Justice, CBO estimates that implementing the reporting requirements of H.R. 5018 would cost federal law enforcement agencies about $1 million a year. Enacting H.R. 5018 could affect direct spending and receipts; therefore, pay-as-you-go procedures would apply to the bill. However, CBO estimates that any impact on direct spending and receipts would not be significant.

H.R. 5018 would require greater judicial oversight when law enforcement officials monitor the electronic communications (such as e-mail) of suspected criminals. The bill would require law enforcement officials who request court orders to monitor these communications to provide evidence of a crime and show that information related to the crime is likely to be contained in such communications. (Under current law, officials need to certify that these communications are related to a criminal investigation.) The bill would prohibit illegally obtained electronic communications from being used as evidence in trials. In addition, the bill would require federal law enforcement agencies to report annually to the Congress on the number and nature of their requests for such orders.

The bill would increase penalties for certain crimes, and establish federal crimes related to the unauthorized disclosure or distruction of certain electronic information. As a result, the federal government might be able to pursue cases that it otherwise would not be able to prosecute. CBO expects that any increase in federal costs for law enforcement, court proceedings, or prison operations would not be significant, however, because of the small number of cases likely to be involved. Any such additional costs would be subject to the availability of appropriated funds.

Because those prosecuted and convicted under H.R. 5018 could be subject to criminal fines, and increased fines and penalties, the federal government might collect additional fines if the bill is enacted. Collections of such fines are recorded in the budget as governmental receipts (revenues), which are deposited in the Crime Victims Fund and spent in subsequent years. CBO expects that any additional receipts and direct spending would be less than $500,000 each year.

H.R. 5018 also would increase judicial oversight of efforts by state and local law enforcement agencies to monitor certain electronic communications. Such requirements would constitute intergovernmental mandates (on both courts and law enforcement agencies) as defined in th Unfunded Mandates Reform Act (UMRA). Based on information from state and local public safety officials, however, CBO estimates that the costs of complying with these new requirements would not likely be significant, and would not exceed the threshold established in UMRA ($55 million in 2000, adjusted annually for inflation). The bill contains no new private-sector mandates as defined by UMRA.

The CBO staff contacts are Mark Hadley (for federal costs), who can be reached at 226–2860, and Theresa Gullo (for the impact on state and local governments), who can be reached at 225–3220.

This estimate was approved by Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the committee finds the authority for this legislation in Article I, section 8, clauses 3 and 18 of the Constitution.

SECTION-BY-SECTION ANALYSIS AND DISCUSSION

Section 1—Short Title

Section 1 states that the act may be cited as the "Electronic Communications Privacy Act of 2000."

Section 2—Use as Evidence

Section 2 extends the statutory exclusionary rule to also exclude from use in evidence at trial electronic communications—including electronic communications such as e-mail that lies in storage with an electronic communications service—obtained in violation of Federal law, just as illegally obtained wire and oral electronic communications are excluded, while also allowing the use of such communications against those who illegally obtained them.

Section 3—Reports Concerning the Disclosure of the Contents of Electronic Communications

Section 3 requires the Federal Government to report annually basic information regarding the requests it makes to disclose the contents of stored electronic communications under 18 U.S.C. §§ 2703(a) and (b).

Section 4—Pen Registers and Trap and Trace Devices

Section 4 raises the standard for the government's access, under the Pen Register Act, to transactional information regarding a person's communications by requiring that a court find that "specific and articulable facts reasonably indicate that crime has been, is being, or will be committed, and information likely to be obtained by such installation and use is relevant to the investigation of that crime."

Section 5—Civil Damages

Section 5 increases the civil penalties that may be applied to those who illegally intercept electronic communications by raising the daily damages for each violation from $100 a day to $500 a day.

Section 6—Notification

Section 6 makes clear that only a court may decide whether delays in notifying those whose stored electronic communications are disclosed are appropriate.

Section 7—Government Access to Location Information

Section 7 prohibits the government from obtaining a mobile phone user's location without first obtaining a court order based on probable cause, except in certain emergency situations. Certain exceptions to this provision are provided for disclosing such informa-

tion to emergency service providers such as hospitals, or to the legal guardian or members of the user's immediate family in situations involving the risk of death or serious physical harm, or with the express consent of the user of the mobile phone equipment.

Section 8—Computer Crime Amendments

Section 8 raises the maximum penalty for the most serious computer violations to 10 years in prison and extends Federal jurisdiction to those computer crimes involving an attack on a protected computer that modifies or impairs, or threatens to modify or impair, the medical examination, diagnosis, treatment, or care of one or more individuals, causes physical injury to any individual, or threatens public health or safety. Section 8 also creates a new category of felony violations where a hacker causes damage to a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

Section 8 also clarifies that damage to multiple protected computers must be aggregated in determining whether a violation has exceeded the $5,000 threshold for an offense and applies the criminal forfeiture rules to computer hacking crimes.

Section 8 also expressly defines the term "loss" as used in the statute to account for a wide range of possible harms done to the victims of computer crimes, including reasonable costs of responding to the offense, conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue or costs incurred because of the interruption of service.

Section 8 also allows the Federal Government to investigate and prosecute offenses in which a person intentionally defaced, damaged or destroyed images or information made available to the public, such as the defacing of images or information on computer systems, even if such offenses did not result in more than $5,000 in damages.

Finally, Section 8 restricts the 6 month minimum sentence under the Federal Sentencing Guidelines to only the more serious computer crimes and better ensures that the punishment fits the crime.

Section 9—Interception of Wire, Oral, and Electronic Communications Amendments

Section 9 requires high-level Department of Justice approval for interceptions of electronic communications, as is currently required for interceptions of wire and oral communications, and also adds computer crimes to the enumerated offenses for which interceptions may be ordered.

Section 10—Amendments to the Electronic Communications Privacy Act

Section 10 increases the criminal penalties for the illegal disclosure of stored electronic communications and allows electronic communications service providers to disclose to law enforcement basic customer records, such as name and address, with the lawful consent of the customer or subscriber; as may be necessarily incident to the rendition of service or to the protection of the rights or property of the provider of that service; or to a governmental entity, if the provider reasonably believes that an emergency involving im-

mediate danger of death or serious physical injury to any person justifies disclosure of the information.

Section 10 also raises the minimum civil damage award for the illegal disclosure of stored electronic communications to $5,000.

Section 11—Additional Provisions Relating to Pen Registers

Section 11 allows law enforcement to use devices that track the source and destination of criminal communications without a court order for up to 48 hours in situations involving national security and ongoing attacks on computer networks, but also requires that, if a court finds law enforcement had an insufficient basis to conduct the monitoring, the judge must order that the person whose communications were wrongfully tracked be notified.

Section 12—Government Access to Contents of Stored Electronic Communications

Section 12 extends the protection of a warrant requirement to electronic communications stored by electronic communications services for 1 year or less.

Section 13—Enhanced Privacy Protection for Information on Computer Networks

Section 13 makes clear that protections of electronic communications in electronic storage cover e-mail messages that have been accessed by the intended recipient but remain stored by an electronic communications service.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

* * * * * * *

CHAPTER 47—FRAUD AND FALSE STATEMENTS

* * * * * * *

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) * * *

* * * * * * *

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses [such a computer] *without or in excess of au-*

thorization a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects;

* * * * * * *

(5)(A)*(i)* knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

[(B)**]** *(ii)* intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

[(C)**]** *(iii)* intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; *and*

(B) whose conduct described in clause (i), (ii), or (iii) of subparagraph (A)—

(i) caused loss to one or more persons during any one-year period (including loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least $5,000;

(ii) modified or impaired, or potentially modified or impaired, the medical examination, diagnosis, treatment, or care of one or more individuals;

(iii) caused physical injury to any individual;

(iv) threatened public health or safety;

(v) caused damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security; or

(vi) intentionally defaced, damaged, or destroyed images or information made available to the public and thereby interfered with the rights protected under the First Amendment to the Constitution;

* * * * * * *

(7) with intent to extort from any person**[**, firm, association, educational institution, financial institution, government entity, or other legal entity,**]** any money or other thing of value,

transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section *as if such person had committed the completed offense*.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1)*, (a)(5)(A)(i), or (a)(5)(A)(ii)* of this section which does not occur after a conviction for another offense under this

section[, or an attempt to commit an offense punishable under this subparagraph]; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section[, or an attempt to commit an offense punishable under this subparagraph];

[(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and]

(2)(A) except as provided in subsection (c)(2)(B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section;

* * * * * * *

[(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and]

[(3)(A)] *(3)* a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4)[, (a)(5)(A), (a)(5)(B),] or (a)(7) of this section which does not occur after a conviction for another offense under this section[, or an attempt to commit an offense punishable under this subparagraph; and]*; and*

[(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and]

(4) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(4), (a)(5), (a)(6), or (a)(7) of this section which occurs after a conviction for another offense under this section.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under [subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of] this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement [which shall be entered into by] *between* the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) * * *

* * * * * * *

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the

executive departments enumerated in section 101 of title 5; [and]

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information[, that—

[(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

[(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

[(C) causes physical injury to any person; or

[(D) threatens public health or safety; and]*;*

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country[.]*;*

(10) the term "conviction for another offense under this section" includes a State conviction for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including responding to the offense, conducting a damage assessment, restoring any data, program, system, or information to its condition before the offense, and any revenue lost or costs incurred because of interruption of service; and

(12) the term "person" includes any individual, firm, association, educational institution, financial institution, corporation, company, partnership, government entity, or other legal entity.

* * * * * * *

[(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.]

(g) Except as herein provided, any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive or other equitable relief. A suit for a violation of subsection (a)(5) may be brought only if the conduct involves one or more of the factors enumerated in subsection (a)(5)(B). No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

* * * * * * *

(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

* * * * * * *

CHAPTER 119—WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec.
2510. Definitions.

* * * * * * *

[2515. Prohibition of use as evidence of intercepted wire or oral communications.]
2515. Prohibition of use as evidence of intercepted wire, oral, or electronic communications.

* * * * * * *

§ 2510. Definitions

As used in this chapter—

(1) * * *

* * * * * * *

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section [153(h)] *153(10)* of title 47 of the United States Code;

* * * * * * *

(17) "electronic storage" means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; [and]

* * * * * * *

(C) any storage of an electronic communication by an electronic communication service without regard to whether the communication has been accessed by the intended recipient; and

* * * * * * *

§ 2515. Prohibition of use as evidence of intercepted [wire or oral] *wire, oral, or electronic* communications

[Whenever any wire or oral communication has been intercepted] *(a) Except as provided in subsection (b), whenever any wire, oral, or electronic communication has been intercepted, or any electronic communication in electronic storage has been disclosed*, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing,

or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter *or chapter 121.*

(b) Subsection (a) does not apply to the disclosure, before a grand jury or in a criminal trial, hearing, or other criminal proceeding, of the contents of a communication, or evidence derived therefrom, against a person alleged to have intercepted, used, or disclosed the communication in violation of this chapter, or chapter 121, or participated in such violation.

§ 2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of ⟦wire or oral⟧ *wire, oral, or electronic* communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) * * *

* * * * * * *

(p) a felony violation of section 1028 (relating to production of false identification documents), *section 1030 (relating to computer fraud and abuse), section 1362 (relating to destruction of government communications facilities),* section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens); or

⟦(p)⟧ *(q)* any conspiracy to commit any offense described in any subparagraph of this paragraph.

* * * * * * *

§ 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter *or under the circumstances described in section 2515(b)*, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter *or under the circumstances de-*

scribed in section 2515(b), has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

§ 2518. Procedure for interception of wire, oral, or electronic communications

(1) * * *

* * * * * * *

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) * * *

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in **[**subsection (d)**]** *subsection (8)(d)* of this section on the person named in the application.

* * * * * * *

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire **[**or oral**]***, oral, or electronic* communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval**[**.**]***;*

except that no supresssion may be ordered under the circumstances described in section 2515(b). Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire **[**or oral**]***, oral, or electronic* communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the

intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

* * * * * * *

[(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.]

* * * * * * *

§ 2520. Recovery of civil damages authorized

(a) * * *

* * * * * * *

(c) COMPUTATION OF DAMAGES.—(1) * * *

(2) In any other action under this section, the court [may] *shall* assess as damages whichever is the [greater] *greatest* of—

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; [or]

(B) statutory damages of [whichever is the greater of $100 a day for each day of violation or $10,000.] *$500 a day for each violation; or*

(C) statutory damages of $10,000.

* * * * * * *

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

* * * * * * *

§ 2701. Unlawful access to stored communications

(a) * * *

(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for [purposes of] *a tortious or illegal purpose,* commercial advantage, malicious destruction or damage, or private commercial gain—

(A) a fine under this title or imprisonment for not more than [one year] *three years*, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than [two] *five* years, or both, for any subsequent offense under this subparagraph; and

[(2) a fine under this title or imprisonment for not more than six months, or both, in any other case.]

(2) in any other case—

(A) a fine under this title or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than five years, or both, for any subsequent offense under this subparagraph.

* * * * * * *

[§ 2702. Disclosure of contents]

§ 2702. Voluntary disclosure of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b)—

(1) a **[**person or entity providing an**]** *provider of* electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; **[**and**]**

(2) a **[**person or entity providing**]** *provider of* remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing**[**.**]***; and*

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2) of this subsection) to any governmental entity.

(b) EXCEPTIONS *FOR DISCLOSURE OF COMMUNICATIONS*.—A **[**person or entity**]** *provider described in subsection (a)* may divulge the contents of a communication—

(1) * * *

* * * * * * *

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2) of this section)—

(1) as otherwise authorized in section 2703 of this title;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

(5) to any person other than a governmental entity where not otherwise prohibited by law.

§ 2703. Requirements for governmental access

(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for [one hundred and eighty days] *one year* or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than [one hundred and eighty days] *one year* by the means available under subsection (b) of this section.

* * * * * * *

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1)[(A) Except as provided in subparagraph (B),] *A governmental entity may require* a provider of electronic communication service or remote computing service [may] *to* disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or [(b) of this section] *(b), or wireless location information covered by subsection (g))* [to any person other than a governmental entity.]

[(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity] only when the governmental entity—

[(i)] *(A)* obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;

[(ii)] *(B)* obtains a court order for such disclosure under subsection (d) of this section;

[(iii)] *(C)* has the consent of the subscriber or customer to such disclosure; [or]

[(iv)] *(D)* submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title)[.]*; or*

(E) seeks information pursuant to paragraph (2).

[(C)] *(2)* A provider of electronic communication service or remote computing service shall disclose to a governmental entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized, when the governmental entity uses [an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena] *a Federal or State grand jury or trial subpoena,*

or a subpoena or equivalent process authorized by a Federal or State statute, or any means available under ⟦subparagraph (B).⟧ *paragraph (1).*

⟦(2)⟧ *(3)* A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

* * * * * * *

(g) REPORTS CONCERNING THE DISCLOSURE OF THE CONTENTS OF ELECTRONIC COMMUNICATIONS.—

(1) By January 31 of each calendar year, the judge issuing or denying an order, warrant, or subpoena, or the authority issuing or denying a subpoena, under subsection (a) or (b) of this section during the preceding calendar year shall report on each such order, warrant, or subpoena to the Administrative Office of the United States Courts—

(A) the fact that the order, warrant, or subpoena was applied for;

(B) the kind of order, warrant, or subpoena applied for;

(C) the fact that the order, warrant, or subpoena was granted as applied for, was modified, or was denied;

(D) the offense specified in the order, warrant, subpoena, or application;

(E) the identity of the agency making the application; and

(F) the nature of the facilities from which or the place where the contents of electronic communications were to be disclosed.

(2) In January of each year the Attorney General or an Assistant Attorney General specially designated by the Attorney General shall report to the Administrative Office of the United States Courts—

(A) the information required by subparagraphs (A) through (F) of paragraph (1) of this subsection with respect to each application for an order, warrant, or subpoena made during the preceding calendar year; and

(B) a general description of the disclosures made under each such order, warrant, or subpoena, including—

(i) the approximate number of all communications disclosed and, of those, the approximate number of incriminating communications disclosed;

(ii) the approximate number of other communications disclosed; and

(iii) the approximate number of persons whose communications were disclosed.

(3) In June of each year, beginning in 2002, the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders, warrants, or subpoenas authorizing or requiring the disclosure of the contents of electronic communications pursuant to subsections (a) and (b) of this section and the number of orders, warrants, or subpoenas granted or denied pursuant to subsections (a) and (b) of this section during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by paragraphs (1) and (2) of this

subsection. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by paragraphs (1) and (2) of this subsection.

(h) DISCLOSURE OF LOCATION INFORMATION TO GOVERNMENTAL ENTITIES.—

(1) DISCLOSURE UPON COURT ORDER.—Except as provided in paragraph (2), a provider of mobile electronic communication service shall provide to a governmental entity information generated by and disclosing the current physical location of a subscriber's equipment only if the governmental entity obtains a court order issued upon a finding that there is probable cause to believe that—

(A) a person is committing, has committed, or is about to commit a felony offense; and

(B) the location information sought to be obtained concerns the location of the person believed to have committed, be committing, or be about to commit that offense or a victim of that offense.

(2) PERMITTED DISCLOSURES WITHOUT COURT ORDER.—A provider of mobile electronic communication service may provide information described in paragraph (1)—

(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(C) with the express consent of the subscriber or the user of the equipment concerned.

(3) DEFINITION.—The term "public safety answering point" means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

* * * * * * *

§ 2705. Delayed notice

(a) DELAY OF NOTIFICATION.—(1) * * *

* * * * * * *

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, **[**or by certification by a governmental entity, but only in accordance with subsection (b) of this section.**]** *if the court determines that there is reason to believe that notification of the existence of the court order or subpoena may have an adverse result described in paragraph (2) of this subsection.*

* * * * * * *

§ 2707. Civil action

(a) * * *

* * * * * * *

(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of [$1,000] *$5,000*. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

* * * * * * *

PART II—CRIMINAL PROCEDURE

* * * * * * *

CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES

* * * * * * *

§ 3122. Application for an order for a pen register or a trap and trace device

(a) * * *

(b) CONTENTS OF APPLICATION.—An application under subsection (a) of this section shall include—

(1) * * *

[(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.]

(2) a statement of facts showing that the requirements of section 3123 have been met.

§ 3123. Issuance of an order for a pen register or a trap and trace device

(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that [the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.] *specific and articulable facts 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 the investigation of that crime.*

* * * * * * *

§ 3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General,

or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(1) an emergency situation exists that involves—

(A) immediate danger of death or serious bodily injury to any person; [or]

(B) conspiratorial activities characteristic of organized crime[,]*;*

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on the integrity or availability of a protected computer in violation of section 1030(a)(5)(A)(i) or 1030(a)(5)(A)(ii) of this title,

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use;

may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title. *In the event an application for such order is denied, or in any other case where the installation and use of a pen register or trap and trace device is terminated without an order having been issued, any information obtained by such installation and use shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (b) of this section on the person named in the application.*

(b) Within a reasonable time but not later than 90 days after the filing of an application for an order of approval under subsection (a)(2) of this section which is denied, the denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to the information obtained by such installation and use of a pen register or trap and trace device as the judge may determine in his discretion is in the interest of justice, an inventory which shall include notice of—

(1) the fact of the entry of the application;

(2) the date of the entry and the date of the denial of the application; and

(3) the fact that during the period covered by the application, information was obtained by the installation and use of a pen register or trap and trace device.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the applications as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

[(b)] *(c)* In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

[(c)] *(d)* The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.

[(d)] *(e)* A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

* * * * * * *

§ 3127. Definitions for chapter

As used in this chapter—

(1) * * *

* * * * * * *

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States[.]; *and*

(7) the term "protected computer" has the meaning set forth in section 1030 of this title.

* * * * * * *

SECTION 805 OF THE ANTITERRORISM AND EFFECTIVE DEATH PENALTY ACT OF 1996

SEC. 805. DETERRENT AGAINST TERRORIST ACTIVITY DAMAGING A FEDERAL INTEREST COMPUTER.

(a) * * *

* * * * * * *

(c) AMENDMENT OF GUIDELINES.—Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission [shall amend the sentencing guidelines to ensure any individual convicted of a violation of paragraph (4) or (5)] *shall amend the sentencing guidelines to ensure any individual convicted of a violation of paragraph (4) or a felony violation of paragraph (5)(A)(i) (but not of paragraph (5)(A)(ii) or (5)(A)(iii))* of section 1030(a) of title 18, United States Code, is imprisoned for not less than 6 months.

○