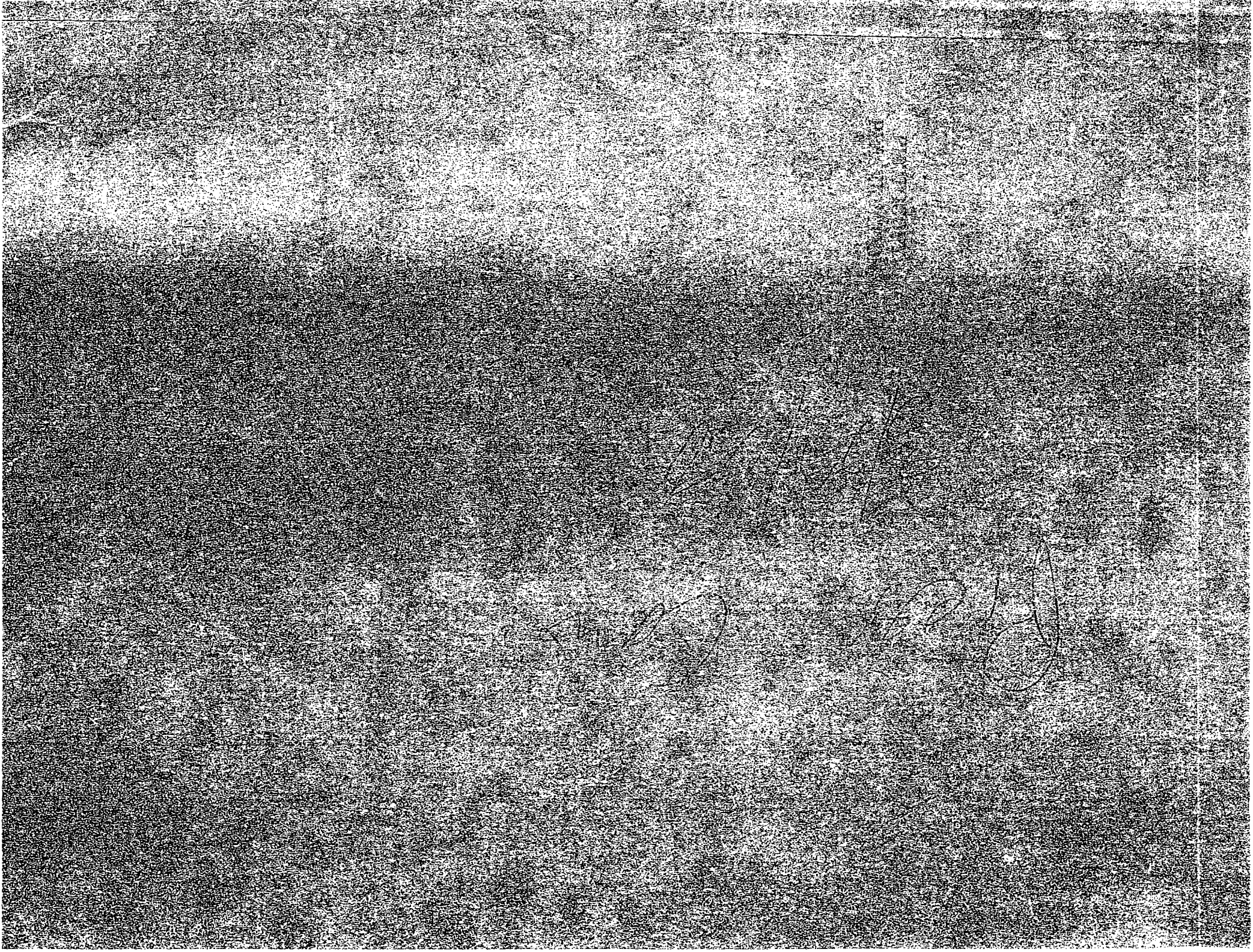




June 30, 2000

Cybersecurity Nominees List

Included in Draft Speech by John Podesta

1. Replace outdated telephone-only language (throughout)
2. Elevating "electronic" to "wire" (p. 31)
3. Cable Communications Policy Act (p. 70)
4. Nationwide trap and trace orders (p. 56)
5. "Shall" to "may" language to add more judicial discretion in trap and trace orders (p. 56)

Other Nominees from April Meeting – Not included in Speech

6. Emergency exception to trap and trace for ongoing attacks (p. 59)
7. Computer Fraud and Abuse. Damages less than \$5,000 = new misdemeanor (pp. 3, 5)
8. Can aggregate damages for \$5,000 felony threshold in computer fraud (p. 3)
9. Restrict mandatory sentences for computer fraud to only serious felonies (p. 8)
10. Assistance to state and local law enforcement (no language in proposed bill)
11. Voluntary disclosure of traffic information (pp. 45-46)
12. Application to computers located outside of United States (p. 4)
13. Increase penalties for illegal interceptions (pp. 28, 44)
14. Sentencing Commission to study penalty enhancement for privacy offenses (p. 13)
15. Special provisions for juvenile offenders (p. 5, 62)
16. Access to electronic data by civil investigators (p. 49)
17. Criminal forfeiture (p. 6-7)
18. Clean hands exception to suppression: use against illegal interceptor (cleared) (p. 31)
19. Cyberstalking (cleared) (p. 10)

[REDLINE VERSIONS OF STATUTES AMENDED BY CHECSA]

[Redline-strikeout version: 18 U.S.C. §1030]

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 47 - FRAUD AND FALSE STATEMENTS

Section 1030. Fraud and related activity in connection with computers

(a) Whoever –

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such 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 that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

- (5) (A) 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) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if —

- (A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States;

(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;

(8) knowingly and with intent to commit, or to facilitate the commission of, an act that would constitute a violation of this section, produces, uses, possesses, or traffics (as that term is defined in section 1029 of this Title) in one or more computer intrusion tools.

(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) 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

April 24, 2000

(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) ~~except as provided in subsections (c)(2)(B) and (c)(2)(C),~~ 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), (a)(5), or (a)(6), or (a)(8)~~ 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 5 years, or both, in the case of an offense under subsection (a)(2), if --

Misdemeanor

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000; and

(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 this section, or an attempt to commit an offense punishable under this subparagraph; and a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsections (a)(5)(A) or (a)(5)(B) if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) --~~

(i) 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 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

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

Aggregate to \$5,000

- (3)(A) 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~~

April 24, 2000

~~attempt to commit an offense punishable under this subparagraph; and~~

~~(B)(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), (a)(5)(B), (a)(5)(C), (a)(6), or (a)(7), or (a)(8) 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,~~

(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), (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) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer -

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including computers located outside of the United States;

Application
to computers
outside
U.S.

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means -

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union

April 24, 2000

Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(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;~~

misdemeanor

(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" shall include—

(A) an adjudication of juvenile delinquency for a violation of this section; and

(B) a conviction under the law of any State 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;

Special provision for juveniles

(11) the term "loss" means any reasonable cost to any victim, including responding to the

April 24, 2000

offense, conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any revenue lost or costs incurred because of interruption of service;

(12) the term "computer intrusion tool" means any device, program, information, or code the design of which renders it primarily useful for the purpose of enabling a person to access a computer without authority or exceed authorized access, to cause damage to a computer without authorization, or to conceal any such activity; and

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

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Except as provided below, any 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. A suit for a violation of subsection (a)(5) may be brought only if the conduct involves one of the factors enumerated in subparagraph (c)(2)(C). 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.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i) Criminal Forfeiture: --

(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 property, real or personal, 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

criminal
forfeiture

April 24, 2000

such person obtained, directly or indirectly, as a result of such violation;

*Criminal
forfeiture*

(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.

(i) Civil Forfeiture --

(1) The following shall be subject to forfeiture to the United States and no property right shall exist in them:

(A) any property, real or personal, used or intended to be used to commit or to facilitate the commission of any violation of this section; and

(B) any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section.

(2) The provisions of chapter 46 of this title relating to civil forfeiture shall apply to any seizure or civil forfeiture under this subsection.

[Redline strikeout version: Antiterrorism Act of 1996]

ANTITERRORISM ACT OF 1996
PUB. L. NO. 104-132
104TH CONG., 2D SESS. (1996)

....

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

(a) REVIEW. — Not later than 60 calendar days after the date of enactment of this Act, the United States Sentencing Commission shall review the deterrent effect of existing guideline levels as they apply to paragraphs (4) and (5) of section 1030(a) of title 18, United States Code.

(b) REPORT. — The United States Sentencing Commission shall prepare and transmit a report to the Congress on the findings under the study conducted under subsection (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) a felony violation of (5)(A) (but not of (5)(B) or (5)(C))~~ of section 1030(a) of title 18, United States Code, is imprisoned for not less than 6 months.

Restrict
Mandatory
Sentences
for Computer
Fraud to
only serious
felonies

....

April 24, 2000

[redline strikeout version of 47 U.S.C.A. §223]

UNITED STATES CODE ANNOTATED
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5--WIRE OR RADIO COMMUNICATION
SUBCHAPTER II--COMMON CARRIERS
PART I--COMMON CARRIER REGULATION

Section 223. Obscene or harassing ~~telephone calls~~ communications in the District of Columbia or in interstate or foreign communications

(a) Prohibited general purposes

Whoever--

(1) in interstate or foreign communications--

(A) by means of a telecommunications device knowingly--

(i) makes, creates, or solicits, and

(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person;

(B) by means of a telecommunications device knowingly--

(i) makes, creates, or solicits, and

(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

(C) makes a telephone call or utilizes a telecommunications device or interactive computer service, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications;

(D) makes or causes the telephone of another repeatedly or continuously to ring,

with intent to harass any person at the called number; or

(E) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device or interactive computer service, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication; or

(F) with the intent to cause the unavailability of a telecommunications device or interactive computer service, or to cause damage to a protected computer (as such terms are defined in section 1030 of title 18), causes or attempts to cause one or more other persons to initiate communication with such telecommunications device, interactive computer service, or protected computer; or

(G) utilizes a telecommunications device or interactive computer service to transmit information about an individual, including such individual's location, habits, beliefs, or other personal identifying information, or information about that individual's spouse or intimate partner, or family, whether or not such information is true and whether or not such information is obtainable from a public source, with intent thereby to cause --

Cyberstalking

(i) a recipient of the information to inflict bodily injury to that individual, that individual's spouse or intimate partner, or family, or unauthorized damage to the property of that individual, that individual's spouse or intimate partner, or family; or

(ii) reasonable fear to that individual of bodily injury to that individual, that individual's spouse or intimate partner, or family, or reasonable fear to that individual of unauthorized damage to the property that individual, that individual's spouse or intimate partner, or family; or

(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under Title 18, or imprisoned not more than two years, or both.

...

(h) Definitions

For purposes of this section--

- (1) The use of the term "telecommunications device" in this section--
 - (A) shall not impose new obligations on broadcasting station licensees and cable operators covered by obscenity and indecency provisions elsewhere in this chapter; and
 - (B) does not include an interactive computer service.
- (2) The term "interactive computer service" has the meaning provided in section 230(f)(2) of this title.
- (3) The term "access software" means software (including client or server software) or enabling tools that do not create or provide the content of the communication but that allow a user to do any one or more of the following:
 - (A) filter, screen, allow, or disallow content;
 - (B) pick, choose, analyze, or digest content; or
 - (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.
- (4) The term "institution of higher education" has the meaning provided in section 1001 of Title 20.
- (5) The term "library" means a library eligible for participation in State- based plans for funds under title III of the Library Services and Construction Act (> 20 U.S.C. 355e et seq.).
- (6) The term "spouse or intimate partner" has the meaning provided in section 2266 of title 18.
- (7) The term "bodily injury" has the meaning provided in section 2266 of title 18.

**[Funding Authorization for State & Local Cybercrime
Training and for the support of Regional Computer
Forensics Labs**

Pages 12-18]

[redline/strikeout version of directive to Sentencing Commission regarding enhanced penalties for substantial invasions of individual privacy]

SEC. ____ INCREASED PENALTIES FOR VIOLATIONS INVOLVING SUBSTANTIAL
INVASION OF INDIVIDUAL PRIVACY.

Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall review the adequacy of existing penalties for offenses that involve a substantial invasion of individual privacy and, if justified, provide for an appropriate enhancement for such offenses.

Sentencing
Comm'n
Study
of
penalties
for privacy
offenses

[redline strikeout version of wiretap statute]

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND
INTERCEPTION OF ORAL COMMUNICATIONS

Section 2510. Definitions

As used in this chapter--

- (1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce ~~and such term includes any electronic storage of such communication;~~
- (2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;
- (3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;
- (4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device;
- (5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--
 - (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an

April 24, 2000

investigative or law enforcement officer in the ordinary course of his duties;
(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means--

- (a) a judge of a United States district court or a United States court of appeals;
and
- (b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(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;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means 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, but does not include--

- (A) any wire or oral communication;
- (B) any communication made through a tone-only paging device;
- (C) any communication from a tracking device (as defined in section 3117 of this title); or
- (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

- (13) "user" means any person or entity who--
 (A) uses an electronic communication service; and
 (B) is duly authorized by the provider of such service to engage in such use;
- (14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the interim electronic storage of such communications;
- (15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;
- (16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not--
 (A) scrambled or encrypted; ~~;~~
 (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
 (C) carried on a subcarrier or other signal subsidiary to a radio transmission;
 (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
 (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part ~~94~~101 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;
 [(F) Repealed. Pub.L. 104-132, Title VII, S 731(2)(C), Apr. 24, 1996, 110 Stat. 1303]
- (17) "electronic ~~interim~~ storage" means --
 (A) any temporary, intermediate storage by an electronic communication service 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; ~~and~~
- (18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception; ~~;~~

(19) "protected computer" shall have the definition given to it by section 1030 of this title; and

(20) "computer trespasser" means a person who has no reasonable expectation of privacy in any communication transmitted to, through, or from a protected computer because such person is accessing the protected computer without authorization.

Section 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who--

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained

April 24, 2000

through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b) to (c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2) (a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or ~~on an~~ officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic

April 25, 2000

communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter.

(iii) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser, provided that—

(A) the owner or operator of the protected computer expressly authorizes the interception of the computer trespasser's communications on the protected computer;

[(B) the protected computer is not being used to provide commercial electronic communication service to the public;]

(C) the person acting under color of law is lawfully engaged in an ongoing investigation;

(D) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the ongoing investigation; and

(E) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to

April 25, 2000

communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter.

(iii) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser, provided that—

(A) the owner or operator of the protected computer expressly authorizes the interception of the computer trespasser's communications on the protected computer;

[(B) the protected computer is not being used to provide commercial electronic communication service to the public;]

(C) the person acting under color of law is lawfully engaged in an ongoing investigation;

(D) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the ongoing investigation, and

(E) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to

April 24, 2000

such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--

(i) to intercept or access a wire or an electronic communication (other than a radio communication) made through an electronic communications system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted--

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands

allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the
Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which
is causing harmful interference to any lawfully operating station or consumer
electronic equipment, to the extent necessary to identify the source of such
interference; or

(v) for other users of the same frequency to intercept any radio communication
made through a system that utilizes frequencies monitored by individuals engaged
in the provision or the use of such system, if such communication is not
scrambled or encrypted.

(h) It shall not be unlawful under this chapter--

(i) to use a pen register or a trap and trace device (as those terms are defined for
the purposes of chapter 206 (relating to pen registers and trap and trace devices)
of this title); or

(ii) for a provider of electronic communication service to record the fact that a
wire or electronic communication was initiated or completed in order to protect
such provider, another provider furnishing service toward the completion of the
wire or electronic communication, or a user of that service, from fraudulent,
unlawful or abusive use of such service.

(3) (a) Except as provided in paragraph (b) of this subsection, a person or entity providing an
electronic communication service to the public shall not intentionally divulge the contents
of any communication (other than one to such person or entity, or an agent thereof) while
in transmission on that service to any person or entity other than an addressee or intended
recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may
divulge the contents of any such communication--

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient
of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward
such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear
to pertain to the commission of a crime, if such divulgence is made to a law
enforcement agency.

April 24, 2000

- (4) (a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

~~(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then--~~

increasing penalties

- ~~(i) if the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both, and~~
- ~~(ii) if the communication is the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, the offender shall be fined under this title.~~

~~(e)(b)~~ Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

- (i) to a broadcasting station for purposes of retransmission to the general public; or
- (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

- (5) (a) (i) If the communication is--
- (A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection--

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory \$500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than \$500 for each violation of such an injunction.

Section 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally--

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication (including those disseminated by electronic means) any advertisement of--

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for--

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

(4) As used in this section, the phrase "primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications" includes all devices whose manufacture or importation is prohibited under regulations issued by the Federal Communications Commission by reason of such devices' ability to receive, or readily to be altered by the user to receive, frequencies allocated for wireless telephone communications.

April 24, 2000

Section 2513. Confiscation of wire, oral, or electronic communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

[Section 2514. Repealed. Pub.L. 91-452, Title II, S 227(a), Oct. 15, 1970, 84 Stat. 930]

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

(a) Except as provided in subsection (b), Whenever whenever any wire, or oral, or electronic 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 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.

Electronic
to
wire

(b) Subsection (a) shall not apply to the disclosure, before a grand jury or in a criminal trial, hearing, or other proceeding, or, of the contents of a communication, or evidence derived therefrom—

- (1) intercepted by a person not acting under color of law, provided that the party seeking to introduce the contents did not participate directly or indirectly in the interception, or
- (2) against a person alleged to have intercepted the communication, or participated in its

Clean
hands -
exception

interception, in violation of this chapter,

Section 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, 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) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, ~~threat~~ or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or

April 24, 2000

transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), sections 2251 and 2252 (sexual exploitation of children), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), and section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations) with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 1362 (relating to destruction of government communication facilities), section 1992 (relating to wrecking trains), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or naturalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

- (f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;
- (g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions);
- (h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;
- (i) any felony violation of chapter 71 (relating to obscenity) of this title;
- (j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline) or section 46502 (relating to aircraft piracy) of title 49;
- (k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);
- (l) the location of any fugitive from justice from an offense described in this section;
- (m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);
- (n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);
- (o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);
- ~~(p) a felony violation of section 1028 (relating to production of false identification documents), 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);~~
- (p) a felony violation of Title 47, section 223 (relating to abusive communications in interstate or foreign commerce); or
- (q) any conspiracy to commit any offense described in any subparagraph of this paragraph.

April 24, 2000

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers 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 the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of one-way pager electronic communications by an investigative or law enforcement officer 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 any Federal felony.

Section 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)(1) and (b)(2), 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 described in section 2515(b)(1) and (b)(2), 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.

(3) Any person who has received, by any means authorized by this chapter, any information

concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

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

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have

been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that--

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(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) except as provided in subsection (11), 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.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--

- (a) the identity of the person, if known, whose communications are to be intercepted;
- (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
- (c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
- (d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and
- (e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an

order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(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) an emergency situation exists that involves--

- (i) immediate danger of death or serious physical injury to any person,
- (ii) conspiratorial activities threatening the national security interest, or
- (iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(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,

April 24, 2000

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 (8)(d) of this section on the person named in the application.

(8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of--

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

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

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 intercepted communications, applications and orders 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.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

- (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, 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 suppression 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~~ 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.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty

days after the date the order was entered and shall be diligently prosecuted.

~~(e) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for noneconstitutional violations of this chapter involving such communications.~~

...

Section 2520. Recovery of civil damages authorized

(a) In general.--Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) Relief.--In an action under this section, appropriate relief includes--

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c) and punitive damages in appropriate cases; and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of damages.--

(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$50 and not more than \$500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$100 and not more than \$1000.

(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~~ \$500 a day for each day of violation ~~or \$10,000; or~~

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

(d) Defense.--A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation.--A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

[redline strikeout version of amendments to ECPA]

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 121--STORED WIRE AND ELECTRONIC COMMUNICATIONS AND
TRANSACTIONAL RECORDS ACCESS

Section 2701. Unlawful access to stored communications

(a) Offense.--Except as provided in subsection (c) of this section whoever--

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in interim electronic storage in such system shall be punished as provided in subsection (b) of this section.

(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~~ five 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~~ ten years, or both, for any subsequent offense under this subparagraph; and

(2) ~~in any other case--~~

~~(A) a fine under this title or imprisonment for not more than six months~~ one year, or both, in ~~any other case~~ 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.

Increasing
penalties

(c) Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized--

(1) by the person or entity providing a wire or electronic communication service;

(2) by a user of that service with respect to a communication of or intended for that user;
or

(3) in section 2703, or 2704 ~~or 2518~~ of this title.

April 24, 2000

Section 2702. Voluntary disclosure ~~Disclosure of contents~~ 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 interim electronic storage by that service; and

(2) ~~a person or entity providing an~~ 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 subsection (a)(1) or (a)(2) of this section) 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) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section ~~2517, 2511(2)(a), or~~ 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) 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

Voluntary
disclosure
of traffic
information

April 24, 2000

(6) to a law enforcement agency—

(A) if such contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

(B) if required by section 113 of the Child Protection and Sexual Predator Punishment Act of 1998; or

(C) 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.

Voluntary
disclosure
of traffic
information

(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.

Section 2703. Requirements for governmental access Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in interim electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or an electronic communication, that is in interim electronic storage in an electronic communications system for one hundred and eighty days 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 communication services of the contents of a wire or an electronic communication that has been in interim electronic storage in an electronic communications system for more than one hundred and eighty

April 24, 2000

days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

~~(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or~~

~~(ii) obtains a court order for such disclosure under subsection (d) of this section;~~

~~except that delayed notice may be given pursuant to section 2705 of this title.~~

(i) uses a Federal or State grand jury subpoena, or a subpoena or equivalent process authorized by a Federal or State statute (except a subpoena pursuant to subparagraph (ii)), or obtains a court order for such disclosure under subsection (d) of this section, except that delayed notice may be given pursuant to section 2705(a) of this title; or

(ii) uses a Federal or State trial subpoena, or a subpoena duces tecum pursuant to Rule 34 of the Federal Rules of Civil Procedure or equivalent State procedure.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held 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 remote computing 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.

(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) 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~~

~~(D) with prior notice to the customer or subscriber, serves on the provider a Federal or State grand jury or trial subpoena, a subpoena authorized by a Federal or State statute, or a subpoena duces tecum pursuant to Rule 34 of the Federal Rules of Civil Procedure or equivalent State procedure; or~~
~~(E) seeks information pursuant to subparagraph (2) or (3).~~

~~(iv) 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).~~

~~(C)(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the~~

~~(A) name;~~

~~(B) address;~~

~~(C) local and long distance telephone connection records, or records of session times and durations;~~

~~(D) length and types of service utilized;~~

~~(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and~~

~~(F) means and source of payment (including any credit card or bank account number)~~

~~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~~

April 24, 2000

statute; or a Federal or State grand jury or trial subpoena; a subpoena duces tecum pursuant to Rule 34 of the Federal Rules of Civil Procedure or equivalent State procedure; or any means available under subparagraph (B)(1).

(3) A provider of electronic communication service or remote computing service shall, in response to a written request from a law enforcement agency, disclose the city, state, and country associated with a customer or subscriber. Such a request shall be made only for purposes of referring suspected criminal activity to a law enforcement agency in an appropriate jurisdiction.

(2)(4) Except as otherwise provided, a governmental entity receiving requesting records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c)(1) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation or to a Federal or State administrative investigation within the authority of the requesting Federal or State governmental entity. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Access to
electronic
data by
civil
investig-
ators

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence already in its possession pending the issuance of a court order or other process.

April 24, 2000

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(3) Remedies.--If a provider of wire or electronic communication services or a remote computing service knowingly fails to comply with a request under this subsection, the requesting governmental entity shall have a cause of action, in addition to any other remedy or cause of action, against such provider pursuant to section 2707 of this chapter.

Section 2705. Delayed notice

(a) Delay of notification.--

(1) A governmental entity acting under section 2703(b) of this title may--

- (A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or
- (B) where ~~an administrative subpoena authorized by a Federal or State statute or where a Federal or State grand jury subpoena~~ a Federal or State grand jury subpoena or a subpoena or equivalent process authorized by a Federal or State statute (except a subpoena pursuant to subparagraph (ii)) is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is--

- (A) endangering the life or physical safety of an individual;
- (B) flight from prosecution;
- (C) destruction of or tampering with evidence;
- (D) intimidation of potential witnesses; or
- (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph(1)(B).

April 24, 2000

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

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that--

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber--

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access.--A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

...

Section 2707. Civil action

(a) Cause of action.--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) Relief.--In a civil action under this section, appropriate relief includes--

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c); and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(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. 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.

(d) Disciplinary actions for violations.--If a court determines that any agency or department of the United States has violated this chapter and the court finds that the circumstances surrounding the violation raise the question whether or not an officer or employee of the agency or department acted willfully or intentionally with respect to the violation, the agency or department concerned shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the officer or employee.

(e) Defense.--A good faith reliance on--

- (1) a court warrant or order, a grand jury subpoena, a request of a governmental entity under section 2703(f) of this chapter, a legislative authorization, or a statutory authorization;
- (2) a request of an investigative or law enforcement officer under section 2518(7) of this

title; or
(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;
is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) Limitation.--A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

Section 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

...

Section 2711. Definitions for chapter

As used in this chapter--

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; ~~and~~

(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; ~~and~~

(3) the term "court of competent jurisdiction" has the meaning assigned by section 3127 of this title, and includes any federal court within that definition, without geographic limitation.

[Redline Strikeout Version of Amendments to CEOS Admin Subpoenas]

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II--CRIMINAL PROCEDURE
CHAPTER 223--WITNESSES AND EVIDENCE

Section 3486A. Administrative subpoenas in cases involving child abuse and child sexual exploitation

(a) Authorization.--

(1) In general.--In any investigation relating to any act or activity involving a violation of section 1201, 2241(c), 2242, 2243, 2251, 2251A, 2252, 2252A, 2260, 2421, 2422, or 2423 of this title in which the victim is an individual who has not attained the age of 18 years, the Attorney General, or the designee of the Attorney General, may issue in writing and cause to be served a subpoena--

(A) requiring a provider of electronic communication service or remote computing service to disclose ~~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~~ the information specified in subsection 2703(c)(2) of this Title, which may be relevant to an authorized law enforcement inquiry; or

(B) requiring a custodian of records to give testimony concerning the production and authentication of such records or information.

(2) Attendance of witnesses.--Witnesses summoned under this section shall be paid the same fees and mileage that are paid witnesses in the courts of the United States.

(b) Procedures applicable.--The same procedures for service and enforcement as are provided with respect to investigative demands in section 3486 apply with respect to a subpoena issued under this section.

[redline strikeout version: Trap and Trace Statute]

18 U.S.C.A. §3123
UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II--CRIMINAL PROCEDURE
CHAPTER 206--PEN REGISTERS AND TRAP AND TRACE DEVICES

Section 3121. General prohibition on pen register and trap and trace device use; exception

(a) In general.--Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception.--The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.

(c) Limitation.--A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in call processing the processing and transmitting of wire and electronic communications.

(d) Penalty.--Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

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

(a) Application.--

April 24, 2000

(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of application.--An application under subsection (a) of this section shall include--

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(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.

Section 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.~~

(a) In general. --

(1) Upon an application made under section 3122(a)(1) 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 if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. Such order shall, upon service of such order, apply to any entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order.

shall to may
Nationwide
trap
and trace

(2) Upon an application made under section 3122(a)(2) 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 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.

(b) Contents of order.--An order issued under this section--

(1) shall specify--

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, such as the number or other identifier and, if known, physical location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device authorized under paragraph (a)(2) of this section, the geographic limits of the trap and trace order; and

(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

(c) Time period and extensions.--

(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) Nondisclosure of existence of pen register or a trap and trace device.--An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that--

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached or applied, or who has been ordered by the court who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

Section 3124. Assistance in installation and use of a pen register or a trap and trace device

April 24, 2000

(a) Pen registers.--Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

(b) Trap and trace device.--Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123(b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

(c) Compensation.--A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

(d) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this chapter or request pursuant to section 3125 of this title.

(e) Defense.--A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(f) Communications assistance enforcement orders.--Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

Section 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; or

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

(D) an immediate threat to public health or safety; or

(E) an ongoing attack on the integrity or availability of a protected computer punishable pursuant to 18 U.S.C. §1030(c)(2)(C).

Emergency
exception
to trap and
trace for
ongoing
attacks

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.

(b) 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) 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) 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.

Section 3126. Reports concerning pen registers and trap and trace devices

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice.

Section 3127. Definitions for chapter

As used in this chapter--

- (1) the terms "wire communication", "electronic communication", and "electronic communication service" have the meanings set forth for such terms in section 2510 of this title;
- (2) the term "court of competent jurisdiction" means--
 - ~~(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or~~
 - (A) any district court of the United States (including a magistrate judge of such a court) or United States Court of Appeals having jurisdiction over the offense being investigated; or
 - (B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;
- (3) the term "pen register" means a device or process which records or decodes electronic or other impulses which identify the numbers dialed or otherwise dialing, routing, addressing, and signaling information transmitted ~~on the telephone line to which such device is attached~~ by an instrument or facility from which a wire or electronic communication is transmitted, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;
- (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information relevant to identifying the source of a wire or electronic communication ~~of an instrument or device from which a wire or electronic communication was transmitted~~;
- (5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and
- (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.

[Redline-strikeout version: JUVENILE DELINQUENCY]

TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART IV--CORRECTION OF YOUTHFUL OFFENDERS
CHAPTER 403--JUVENILE DELINQUENCY

§ 5032. Delinquency proceedings in district courts; transfer for criminal prosecution

A juvenile alleged to have committed an act of juvenile delinquency, other than a violation of law committed within the special maritime and territorial jurisdiction of the United States for which the maximum authorized term of imprisonment does not exceed six months, shall not be proceeded against in any court of the United States unless the Attorney General, after investigation, certifies to the appropriate district court of the United States that (1) the juvenile court or other appropriate court of a State does not have jurisdiction or refuses to assume jurisdiction over said juvenile with respect to such alleged act of juvenile delinquency, (2) the State does not have available programs and services adequate for the needs of juveniles, or (3) the offense charged is a crime of violence that is a felony or an offense described in section 401 of the Controlled Substances Act (21 U.S.C. 841), or section 1002(a), 1003, 1005, 1009, or 1010(b)(1), (2), or (3) of the Controlled Substances Import and Export Act (21 U.S.C. 952(a), 953, 955, 959, 960(b)(1), (2), (3)), section 922(x) or section 924(b), (g), or (h) of this title, or is a violation of section 1030(a)(1), section 1030(a)(2)(B), 1030(a)(3), or a felony violation of 1030(a)(5) where such violation of 1030(a)(5) is eligible for punishment under 1030(c)(5)(C)(ii) through (v) of this title, and that there is a substantial Federal interest in the case or the offense to warrant the exercise of Federal jurisdiction.

Special provisions for juveniles

If the Attorney General does not so certify, such juvenile shall be surrendered to the appropriate legal authorities of such State. For purposes of this section, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

If an alleged juvenile delinquent is not surrendered to the authorities of a State pursuant to this section, any proceedings against him shall be in an appropriate district court of the United States. For such purposes, the court may be convened at any time and place within the district, in chambers or otherwise. The Attorney General shall proceed by information or as authorized under section 3401(g) of this title, and no criminal prosecution shall be instituted for the alleged act of juvenile delinquency except as provided below.

A juvenile who is alleged to have committed an act of juvenile delinquency and who is not surrendered to State authorities shall be proceeded against under this chapter unless he has

requested in writing upon advice of counsel to be proceeded against as an adult, except that, with respect to a juvenile fifteen years and older alleged to have committed an act after his fifteenth birthday which if committed by an adult would be a felony that is a crime of violence or an offense described in section 401 of the Controlled Substances Act (21 U.S.C. 841), or section 1002(a), 1005, or 1009 of the Controlled Substances Import and Export Act (21 U.S.C. 952(a), 955, 959), or section 922(x) of this title, or in section 924(b), (g), or (h) of this title, criminal prosecution on the basis of the alleged act may be begun by motion to transfer of the Attorney General in the appropriate district court of the United States, if such court finds, after hearing, such transfer would be in the interest of justice. In the application of the preceding sentence, if the crime of violence is an offense under section 113(a), 113(b), 113(c), 1111, 1113, or, if the juvenile possessed a firearm during the offense, section 2111, 2113, 2241(a), or 2241(c), "thirteen" shall be substituted for "fifteen" and "thirteenth" shall be substituted for "fifteenth". Notwithstanding sections 1152 and 1153, no person subject to the criminal jurisdiction of an Indian tribal government shall be subject to the preceding sentence for any offense the Federal jurisdiction for which is predicated solely on Indian country (as defined in section 1151), and which has occurred within the boundaries of such Indian country, unless the governing body of the tribe has elected that the preceding sentence have effect over land and persons subject to its criminal jurisdiction. However a juvenile who is alleged to have committed an act after his sixteenth birthday which if committed by an adult would be a felony offense that has as an element thereof the use, attempted use, or threatened use of physical force against the person of another, or that, by its very nature, involves a substantial risk that physical force against the person of another may be used in committing the offense, or would be an offense described in section 32, 81, 844(d), (e), (f), (h), (I) or 2275 of this title, subsection (b)(1) (A), (B), or (C), (d), or (e) of section 401 of the Controlled Substances Act, or section 1002(a), 1003, 1009, or 1010(b) (1), (2), or (3) of the Controlled Substances Import and Export Act (21 U.S.C. 952(a), 953, 959, 960(b) (1), (2), (3)), and who has previously been found guilty of an act which if committed by an adult would have been one of the offenses set forth in this paragraph or an offense in violation of a State felony statute that would have been such an offense if a circumstance giving rise to Federal jurisdiction had existed, shall be transferred to the appropriate district court of the United States for criminal prosecution.

Evidence of the following factors shall be considered, and findings with regard to each factor shall be made in the record, in assessing whether a transfer would be in the interest of justice: the age and social background of the juvenile; the nature of the alleged offense; the extent and nature of the juvenile's prior delinquency record; the juvenile's present intellectual development and psychological maturity; the nature of past treatment efforts and the juvenile's response to such efforts; the availability of programs designed to treat the juvenile's behavioral problems. In considering the nature of the offense, as required by this paragraph, the court shall consider the extent to which the juvenile played a leadership role in an organization, or otherwise influenced other persons to take part in criminal activities, involving the use or distribution of

April 24, 2000

controlled substances or firearms. Such a factor, if found to exist, shall weigh in favor of a transfer to adult status, but the absence of this factor shall not preclude such a transfer.

Reasonable notice of the transfer hearing shall be given to the juvenile, his parents, guardian, or custodian and to his counsel. The juvenile shall be assisted by counsel during the transfer hearing, and at every other critical stage of the proceedings.

Once a juvenile has entered a plea of guilty or the proceeding has reached the stage that evidence has begun to be taken with respect to a crime or an alleged act of juvenile delinquency subsequent criminal prosecution or juvenile proceedings based upon such alleged act of delinquency shall be barred.

Statements made by a juvenile prior to or during a transfer hearing under this section shall not be admissible at subsequent criminal prosecutions.

Whenever a juvenile transferred to district court under this section is not convicted of the crime upon which the transfer was based or another crime which would have warranted transfer had the juvenile been initially charged with that crime, further proceedings concerning the juvenile shall be conducted pursuant to the provisions of this chapter.

A juvenile shall not be transferred to adult prosecution nor shall a hearing be held under section 5037 (disposition after a finding of juvenile delinquency) until any prior juvenile court records of such juvenile have been received by the court, or the clerk of the juvenile court has certified in writing that the juvenile has no prior record, or that the juvenile's record is unavailable and why it is unavailable.

Whenever a juvenile is adjudged delinquent pursuant to the provisions of this chapter, the specific acts which the juvenile has been found to have committed shall be described as part of the official record of the proceedings and part of the juvenile's official record.

[redline strikeout version of amendments to the Privacy Protection Act]

UNITED STATES CODE ANNOTATED
TITLE 42. THE PUBLIC HEALTH AND WELFARE
CHAPTER 21A--PRIVACY PROTECTION
SUBCHAPTER I--FIRST AMENDMENT PRIVACY PROTECTION
PART A--UNLAWFUL ACTS

Section 2000aa. Searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offenses

(a) Work product materials

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if--

(1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of Title 18, or section 2274, 2275 or 2277 of this title, or section 783 of Title 50, or if the offense involves the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, the sexual exploitation of children, or the sale or purchase of children under section 2251, 2251A, 2252, or 2252A of Title 18); or

(2) there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being; or

(3) the seizure or examination of work product materials is incidental to the execution of

an otherwise lawful search or seizure.

(b) Other documents

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize documentary materials, other than work product materials, possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if--

(1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of Title 18, or section 2274, 2275, or 2277 of this title, or section 783 of Title 50, or if the offense involves the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, the sexual exploitation of children, or the sale or purchase of children under section 2251, 2251A, 2252, or 2252A of Title 18);

(2) there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being;

(3) there is reason to believe that the giving of notice pursuant to a subpoena duces tecum would result in the destruction, alteration, or concealment of such materials; or

(4) such materials have not been produced in response to a court order directing compliance with a subpoena duces tecum, and--

(A) all appellate remedies have been exhausted; or

(B) there is reason to believe that the delay in an investigation or trial occasioned by further proceedings relating to the subpoena would threaten the interests of justice; or

(5) the seizure or examination of documentary materials is incidental to the execution of

an otherwise lawful search or seizure.

(c) Objections to court ordered subpoenas; affidavits

In the event a search warrant is sought pursuant to paragraph (4)(B) of subsection (b) of this section, the person possessing the materials shall be afforded adequate opportunity to submit an affidavit setting forth the basis for any contention that the materials sought are not subject to seizure.

[redline strike out version of Cable Communications Policy Act]

UNITED STATES CODE ANNOTATED
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5--WIRE OR RADIO COMMUNICATION
SUBCHAPTER V-A--CABLE COMMUNICATIONS
PART IV--MISCELLANEOUS PROVISIONS

Section 551. Protection of subscriber privacy

(a) Notice to subscriber regarding personally identifiable information; definitions

(1) At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of--

- (A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;
- (B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;
- (C) the period during which such information will be maintained by the cable operator;
- (D) the times and place at which the subscriber may have access to such information in accordance with subsection (d) of this section; and
- (E) the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) of this section to enforce such limitations.

In the case of subscribers who have entered into such an agreement before the effective date of this section, such notice shall be provided within 180 days of such date and at least once a year thereafter.

(2) For purposes of this section, other than subsection (h) of this section--

- (A) the term "personally identifiable information" does not include any record of aggregate data which does not identify particular persons;
- (B) the term "other service" includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service; and
- (C) the term "cable operator" includes, in addition to persons within the definition

of cable operator in section 522 of this title, any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications service.

(b) Collection of personally identifiable information using cable system

(1) Except as provided in paragraph (2), a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.

(2) A cable operator may use the cable system to collect such information in order to--
(A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or
(B) detect unauthorized reception of cable communications.

(c) Disclosure of personally identifiable information

(1) Except as provided in paragraph (2), a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.

(2) A cable operator may disclose such information if the disclosure is--

(A) necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber;

(B) subject to subsection (h) of this section, made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed; or

(C) a disclosure of the names and addresses of subscribers to any cable service or other service, if--

(i) the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and

(ii) the disclosure does not reveal, directly or indirectly, the--

(I) extent of any viewing or other use by the subscriber of a cable

service or other service provided by the cable operator, or
(II) the nature of any transaction made by the subscriber over the
cable system of the cable operator; or

(D) required under chapters 119, 121, or 206 of title 18, United States Code. Such disclosure shall not include records revealing customer cable television viewing activity.

Cable
Act

(d) Subscriber access to information

A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator. A cable subscriber shall be provided reasonable opportunity to correct any error in such information.

(e) Destruction of information

A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) of this section or pursuant to a court order.

(f) Civil action in United States district court; damages; attorney's fees and costs; nonexclusive nature of remedy

(1) Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court.

(2) The court may award--

(A) actual damages but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher;

(B) punitive damages; and

(C) reasonable attorneys' fees and other litigation costs reasonably incurred.

(3) The remedy provided by this section shall be in addition to any other lawful remedy available to a cable subscriber.

(g) Regulation by States or franchising authorities

Nothing in this subchapter shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy.

(h) Disclosure of information to governmental entity pursuant to court order

Except as provided in subsection (c)(2)(D), a governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order--

- (1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
- (2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

[REDLINE STRIKEOUT VERSION OF BAKER ACT]

UNITED STATES CODE ANNOTATED
TITLE 20. EDUCATION
CHAPTER 31--GENERAL PROVISIONS CONCERNING EDUCATION
SUBCHAPTER III--GENERAL REQUIREMENTS AND CONDITIONS CONCERNING
OPERATION AND ADMINISTRATION OF EDUCATION PROGRAMS:
GENERAL AUTHORITY OF SECRETARY
PART 4--RECORDS; PRIVACY; LIMITATION ON WITHHOLDING FEDERAL FUNDS

Section 1232g. Family educational and privacy rights

(a) Conditions for availability of funds to educational agencies or institutions; inspection and review of education records; specific information to be made available; procedure for access to education records; reasonableness of time for such access; hearings; written explanations by parents; definitions

- (1) (A) No funds shall be made available under any applicable program to any educational agency or institution which has a policy of denying, or which effectively prevents, the parents of students who are or have been in attendance at a school of such agency or at such institution, as the case may be, the right to inspect and review the education records of their children. If any material or document in the education record of a student includes information on more than one student, the parents of one of such students shall have the right to inspect and review only such part of such material or document as relates to such student or to be informed of the specific information contained in such part of such material. Each educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time, but in no case more than forty-five days after the request has been made.

(B) No funds under any applicable program shall be made available to any State educational agency (whether or not that agency is an educational agency or institution under this section) that has a policy of denying, or effectively prevents, the parents of students the right to inspect and review the education records maintained by the State educational agency on their children who are or have been in attendance at any school of an educational agency or institution that is subject to the provisions of this section.

(C) The first sentence of subparagraph (A) shall not operate to make available to students in institutions of postsecondary education the following materials:

- (i) financial records of the parents of the student or any information contained therein;
- (ii) confidential letters and statements of recommendation, which were placed in the education records prior to January 1, 1975, if such letters or statements are not used for purposes other than those for which they were specifically intended;
- (iii) if the student has signed a waiver of the student's right of access under this subsection in accordance with subparagraph (D), confidential recommendations--

- (I) respecting admission to any educational agency or institution,
- (II) respecting an application for employment, and
- (III) respecting the receipt of an honor or honorary recognition.

(D) A student or a person applying for admission may waive his right of access to confidential statements described in clause (iii) of subparagraph (C), except that such waiver shall apply to recommendations only if (i) the student is, upon request, notified of the names of all persons making confidential recommendations and (ii) such recommendations are used solely for the purpose for which they were specifically intended. Such waivers may not be required as a condition for admission to, receipt of financial aid from, or receipt of any other services or benefits from such agency or institution.

(2) No funds shall be made available under any applicable program to any educational agency or institution unless the parents of students who are or have been in attendance at a school of such agency or at such institution are provided an opportunity for a hearing by such agency or institution, in accordance with regulations of the Secretary, to challenge the content of such student's education records, in order to insure that the records are not inaccurate, misleading, or otherwise in violation of the privacy rights of students, and to provide an opportunity for the correction or deletion of any such inaccurate, misleading or otherwise inappropriate data contained therein and to insert into such records a written explanation of the parents respecting the content of such records.

(3) For the purposes of this section the term "educational agency or institution" means any public or private agency or institution which is the recipient of funds under any applicable program.

(4) (A) For the purposes of this section, the term "education records" means, except as may be provided otherwise in subparagraph (B), those records, files,

April 24, 2000

documents, and other materials which--

- (i) contain information directly related to a student; and
- (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.

(B) The term "education records" does not include--

- (i) records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute;
- (ii) records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement;
- (iii) in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or
- (iv) records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.

- (5) (A) For the purposes of this section the term "directory information" relating to a student includes the following: the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.

(B) Any educational agency or institution making public directory information shall give public notice of the categories of information which it has designated as such information with respect to each student attending the institution or agency and shall allow a reasonable period of time after such notice has been given for a

April 24, 2000

parent to inform the institution or agency that any or all of the information designated should not be released without the parent's prior consent.

(6) For the purposes of this section, the term "student" includes any person with respect to whom an educational agency or institution maintains education records or personally identifiable information, but does not include a person who has not been in attendance at such agency or institution.

(b) Release of education records; parental consent requirement; exceptions; compliance with judicial orders and subpoenas; audit and evaluation of federally-supported education programs; recordkeeping

(1) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information, as defined in paragraph (5) of subsection (a) of this section) of students without the written consent of their parents to any individual, agency, or organization, other than to the following--

(A) other school officials, including teachers within the educational institution or local educational agency, who have been determined by such agency or institution to have legitimate educational interests, including the educational interests of the child for whom consent would otherwise be required;

(B) officials of other schools or school systems in which the student seeks or intends to enroll, upon condition that the student's parents be notified of the transfer, receive a copy of the record if desired, and have an opportunity for a hearing to challenge the content of the record;

(C) (i) authorized representatives of (I) the Comptroller General of the United States, (II) the Secretary, or (III) State educational authorities, under the conditions set forth in paragraph (3), or (ii) authorized representatives of the Attorney General for law enforcement purposes under the same conditions as apply to the Secretary under paragraph (3);

(D) in connection with a student's application for, or receipt of, financial aid;

(E) State and local officials or authorities to whom such information is specifically allowed to be reported or disclosed pursuant to State statute adopted--

(i) before November 19, 1974, if the allowed reporting or disclosure

concerns the juvenile justice system and such system's ability to effectively serve the student whose records are released, or

(ii) after November 19, 1974, if--

(I) the allowed reporting or disclosure concerns the juvenile justice system and such system's ability to effectively serve, prior to adjudication, the student whose records are released; and

(II) the officials and authorities to whom such information is disclosed certify in writing to the educational agency or institution that the information will not be disclosed to any other party except as provided under State law without the prior written consent of the parent of the student.

(F) organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction, if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations and such information will be destroyed when no longer needed for the purpose for which it is conducted;

(G) accrediting organizations in order to carry out their accrediting functions;

(H) parents of a dependent student of such parents, as defined in section 152 of Title 26;

(I) subject to regulations of the Secretary, in connection with an emergency, appropriate persons if the knowledge of such information is necessary to protect the health or safety of the student or other persons; and

(J) (i) the entity or persons designated in a Federal grand jury subpoena, in which case the court shall order, for good cause shown, the educational agency or institution (and any officer, director, employee, agent, or attorney for such agency or institution) on which the subpoena is served, to not disclose to any person the existence or contents of the subpoena or any information furnished to the grand jury in response to the subpoena; and
(ii) the entity or persons designated in any other subpoena or court order issued for a law enforcement purpose, in which case the court or other issuing agency may order, for good cause shown, the educational agency or institution (and any officer, director, employee, agent, or attorney for

such agency or institution) on which the subpoena or court order is served, to not disclose to any person the existence or contents of the subpoena or court order or any information furnished in response to the subpoena or court order.

Nothing in clause (E) of this paragraph shall prevent a State from further limiting the number or type of State or local officials who will continue to have access thereunder.

(2) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records other than directory information, or as is permitted under paragraph (1) of this subsection, unless--

(A) there is written consent from the student's parents specifying records to be released, the reasons for such release, and to whom, and with a copy of the records to be released to the student's parents and the student if desired by the parents, or

(B) except as provided in paragraph (1)(J), such information is furnished in compliance with judicial order, or pursuant to any lawfully issued subpoena, upon condition that parents and the students are notified of all such orders or subpoenas in advance of the compliance therewith by the educational institution or agency.

(3) Nothing contained in this section shall preclude authorized representatives of (A) the Comptroller General of the United States, (B) the Secretary, or (C) State educational authorities from having access to student or other records which may be necessary in connection with the audit and evaluation of Federally-supported education programs, or in connection with the enforcement of the Federal legal requirements which relate to such programs: Provided, That except when collection of personally identifiable information is specifically authorized by Federal law, any data collected by such officials shall be protected in a manner which will not permit the personal identification of students and their parents by other than those officials, and such personally identifiable data shall be destroyed when no longer needed for such audit, evaluation, and enforcement of Federal legal requirements.

(4) (A) Each educational agency or institution shall maintain a record, kept with the education records of each student, which will indicate all individuals (other than those specified in paragraph (1)(A) of this subsection), agencies, or organizations which have requested or obtained access to a student's education records

maintained by such educational agency or institution, and which will indicate specifically the legitimate interest that each such person, agency, or organization has in obtaining this information. Such record of access shall be available only to parents, to the school official and his assistants who are responsible for the custody of such records, and to persons or organizations authorized in, and under the conditions of, clauses (A) and (C) of paragraph (1) as a means of auditing the operation of the system.

(B) With respect to this subsection, personal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student. If a third party outside the educational agency or institution permits access to information in violation of paragraph (2)(A), or fails to destroy information in violation of paragraph (1)(F), the educational agency or institution shall be prohibited from permitting access to information from education records to that third party for a period of not less than five years.

(5) Nothing in this section shall be construed to prohibit State and local educational officials from having access to student or other records which may be necessary in connection with the audit and evaluation of any federally or State supported education program or in connection with the enforcement of the Federal legal requirements which relate to any such program, subject to the conditions specified in the proviso in paragraph (3).

(6) (A) Nothing in this section shall be construed to prohibit an institution of postsecondary education from disclosing, to an alleged victim of any crime of violence (as that term is defined in section 16 of Title 18), or a nonforcible sex offense, the final results of any disciplinary proceeding conducted by such institution against the alleged perpetrator of such crime or offense with respect to such crime or offense.

(B) Nothing in this section shall be construed to prohibit an institution of postsecondary education from disclosing the final results of any disciplinary proceeding conducted by such institution against a student who is an alleged perpetrator of any crime of violence (as that term is defined in section 16 of Title 18), or a nonforcible sex offense, if the institution determines as a result of that disciplinary proceeding that the student committed a violation of the institution's rules or policies with respect to such crime or offense.

(C) For the purpose of this paragraph, the final results of any disciplinary

proceeding--

- (i) shall include only the name of the student, the violation committed, and any sanction imposed by the institution on that student; and
- (ii) may include the name of any other student, such as a victim or witness, only with the written consent of that other student.

[Redline/Strikeout Version of 18 U.S.C. 1029]

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 47--FRAUD AND FALSE STATEMENTS

Section 1029. Fraud and related activity in connection with access devices

(a) Whoever--

- (1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
- (2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating \$1,000 or more during that period;
- (3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;
- (4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;
- (5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than \$1,000;
- (6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of--
 - (A) offering an access device; or
 - (B) selling information regarding or an application to obtain an access device;
- (7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;
- (8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody

of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b) (1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

(c) Penalties.--

(1) Generally.--The punishment for an offense under subsection (a) of this section is.--

(A) in the case of an offense that does not occur after a conviction for another offense under this section.--

(i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

(ii) if the offense is under paragraph (4), (5), (8), or (9), of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

(C) in either case, forfeiture to the United States of any personal property used or

intended to be used to commit the offense.

(2) Forfeiture procedure.--The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act, except for subsection (d) of that section.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(2) the term "counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3) the term "unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

(4) the term "produce" includes design, alter, authenticate, duplicate, or assemble;

(5) the term "traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;

(6) the term "device-making equipment" means any equipment, mechanism, process, or impression designed or primarily used for making an access device or a counterfeit access device;

(7) The term "credit card system member" means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system;

(8) the term "scanning receiver" means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument;

(9) the term "telecommunications service" has the meaning given such term in section 3 of title I of the Communications Act of 1934;

(10) the term "facilities-based carrier" means an entity that owns communications transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934; and

(11) the term "telecommunication identifying information" means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument.

...

COMPUTER HACKING AND E-COMMERCE SECURITY ACT OF 2000

PROPOSED LEGISLATIVE HISTORY

A. PURPOSE

Over the last decade, use of computers and the Internet has grown exponentially, and individuals have increasingly come to depend on this use in their daily lives. Yet as computer use has blossomed, so too have criminals increasingly exploited computers to commit crimes and to harm the safety, security, and privacy of others. Criminals use computers to send child pornography to each other using anonymous, encrypted communications; hackers break into financial computers and steal customer home address and credit card information; criminals use the Internet's inexpensive and easy communication to commit large-scale fraud on victims all over the globe; and terrorist bombers conceal their whereabouts by communicating their demands over the Internet. Deterring and punishing such wrongdoing requires a legal structure that will support detection and successful prosecution of offenders. Yet the laws defining computer offenses, and the legal tools needed to investigate criminals using the Internet, have lagged behind technological and social changes. This bill laws clarifies and updates the legal framework governing the investigation and prosecution of crime in the Information Age.

(1) PURPOSES OF AMENDMENTS TO THE COMPUTER FRAUD AND ABUSE ACT
AND THE SENTENCING COMMISSION DIRECTIVE

April 24, 2000

Following initial passage in 1984, and amendments in 1986, 1994, and 1996, the seven subsections of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030, now protect a broad range of computers that support critical infrastructures, such as the computers that run our 9-1-1 emergency services, those that hospitals use to store sensitive information and to treat patients, and those that the military uses to defend the nation. Despite the broad reach of section 1030, certain narrow "safe havens" remain which can and should be removed by coordinately narrow amendments. Most of these amendments are technical, intended to address ambiguities or deficiencies that have arisen in recent investigations and prosecutions. These clarifications are not expected to result in an appreciable increase or decrease in the number of prosecutions.

Other amendments will achieve the following: (1) enhance the effectiveness of domestic and international law enforcement efforts; (2) increase the maximum penalty for certain violations of the section that result in damage to protected computers; (3) modify a directive issued to the Sentencing Commission to assure that mandatory sentencing under the Act applies only to serious, felony violations of subsections 1030(a)(4) and (a)(5); (4) create enhanced penalties for juvenile offenders who continue to commit computer crimes as adults.

(2) PURPOSE OF AMENDMENTS TO 47 U.S.C. §223

The Internet and the widespread use of computers have created a host of new tools for communication. Existing statutes provide criminal penalties for persons who use telephones and telecommunications devices to harass or abuse others. The amendments to 47 U.S.C. §223 attempt

to update the statute to address the ways in which people use electronic communications to cause such abuse by closing several loopholes in the existing statutory scheme. These amendments: (1) clarify that the statute applies to all Internet users, regardless of the method by which they access the Internet; (2) prohibit users from using unwitting third parties to bombard their victims with messages; and (3) bar individuals from transmitting personal data about an individual – such as the route by which the victim’s children walk to school – in order to place such an individual or his family in fear of injury.

(3) **AUTHORIZATION OF FUNDING FOR THE TRAINING OF STATE AND LOCAL LAW ENFORCEMENT AND FOR REGIONAL COMPUTER FORENSICS LABORATORIES**

With the explosive growth of the use of computers and the Internet, a far greater number of criminal investigations – even of more “traditional” crimes – involve offenders using these electronic media. Indeed, the changing nature of criminal investigations requires a focused, national effort that involves law enforcement at every level of government. For example, to keep pace with these changes, nearly every law enforcement officer across the country requires at least a basic level of cybercrime training – such as how to handle electronic evidence at a crime scene so as to assure that it is not inadvertently damaged or altered. Investigators focused specifically on computer crimes, of course, require more extensive, in-depth training. In addition, in order to investigate computer crimes and gather electronic evidence effectively, state and local law enforcement agencies need access to professional, expert computer forensics laboratories. This section authorizes funds to support the National Cybercrime Training Partnership, an organization devoted to developing

cybercrime training, and to create and support regional computer forensics laboratories.

(4) PURPOSE OF DIRECTIVE TO THE SENTENCING COMMISSION TO INCREASE PENALTIES FOR CRIMES INVOLVING SUBSTANTIAL INVASION OF INDIVIDUAL PRIVACY

In a significant number of federal crimes, the offense may involve a substantial intrusion into an individual's privacy. Violations of the Computer Fraud and Abuse Act, 18 U.S.C. §1030, for example, might involve an invasion of individual privacy, such as a case in which a "hacker" obtains a person's medical or psychiatric records by breaking into a computer. Although the Sentencing Commission added commentary in 1997 allowing for enhanced penalties for certain property crimes where the conduct involved a substantial invasion of individual privacy, this section applies only to a narrow category of theft offenses. This section directs the Sentencing Commission to conduct a thorough review of all of the existing guidelines and, if appropriate, to provide an appropriate enhancement where the conduct involves a substantial invasion of a privacy interest that would not be addressed by the otherwise applicable guideline.

(5) PURPOSE OF AMENDMENTS TO THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, THE WIRETAP STATUTE, AND 18 U.S.C. §3486A

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA") in an effort to revise and expand the scope of the 1968 wiretap act. In most cases, the statute struck a workable balance among the competing interests addressed in the statute — the privacy interests of telecommunications users, the business interests of service providers, and the duty of government

investigators to protect public safety.

Notwithstanding the best efforts of those involved in crafting ECPA, however, the statute is in need of amendment. The problems in applying it today principally stem from two factors:

(1) the explosive growth of the Internet, and (2) inconsistencies and gaps in ECPA itself. With the now widespread use of computers and the Internet, the proportion of criminal activity occurring online or using telecommunications technologies has increased enormously. E-mail, voice mail, user access logs, and remotely stored files play an important — and in many cases, critical — role in investigating and prosecuting crimes ranging from extortion and murder to large-scale consumer fraud.

Second, although ECPA attempted to create a technology-neutral framework for regulating the disclosure of electronic communications and records, it was only partially successful. For example, the 1986 legislation distinguished broadly between “wire communications” (such as voice telephone calls) and “electronic communications,” which received a different level of protection. Not only does this inconsistency create practical problems in today’s network environment — where voice and non-voice data may be intertwined in a single data stream — it also fails to reflect the fact that “electronic communications” today increasingly consist of personal, private communications.

The proposed legislation therefore seeks to address these issues without substantially altering the balances struck in 1968 and 1986. Among other objectives, the amendments attempt to (1) harmonize the currently disparate treatment of wire and electronic communications; (2) increase penalties for a variety of criminal invasions of communications privacy; (3) resolve deficiencies in

the rules for government access to customer records, especially with respect to access by civil and regulatory agencies; and (4) cure omissions and inconsistencies within the statutory framework.

(6) PURPOSE OF AMENDMENTS TO PEN REGISTER AND TRAP AND TRACE STATUTE

Both technological change and legal developments have necessitated a change in the statute governing pen registers and trap and trace devices. First, advances in telecommunications technology have made the language of the statute obsolete. The definition of “pen register,” for example, refers to a “device” that is “attached” to a telephone “line.” Telephone companies, however, no longer accomplish these functions using physical hardware attached to an actual telephone line. Moreover, the statute refers specifically to telephone “numbers,” a concept made out of date by the need to trace communications over the Internet that use other means to identify users’ accounts.

Second, the deregulation of the telecommunications industry has created unprecedented hurdles in tracing long-distance telephone calls. Many companies, located in a variety of judicial districts, may handle a single call. Under the existing statute, however, a court can only order communications carriers within its district to provide tracing information to law enforcement. As a result, investigators often have to apply for many court orders in order to trace a single communication, causing needless waste of time and resources and hampering important investigations. This amendment grants authority to the courts to order all telecommunications carriers providing service in the United States, whether within the jurisdiction or not, to provide law

enforcement authorities the information needed to trace communications.

(7) PURPOSE OF AMENDMENTS TO THE JUVENILE DELINQUENCY CHAPTER
CONCERNING TRANSFER OF JUVENILES FOR CRIMINAL PROSECUTION

The widespread use of computers and the Internet has created the possibility for an individual to cause drastic harm to public health and safety by damaging or shutting down computers. Certain juveniles have taken advantage of this capability, such as when a juvenile disrupted the operations of a regional airport in central Massachusetts when it lost telecommunications connections. Moreover, juveniles have violated the security of federal computers that promote our national security. Federal law enforcement authorities should have the power to investigate and prosecute such offenders. This amendment makes juveniles fifteen years of age or older who commit such violations of the Computer Fraud and Abuse Act eligible for prosecution in federal court if so certified by the Attorney General.

(8) PURPOSE OF AMENDMENTS TO THE PRIVACY PROTECTION ACT

Title 42, Section 2000aa (the “Privacy Protection Act” or “PPA”) has shielded criminal activities from legitimate law enforcement investigations, such efforts to search for and seize child pornography and to arrest those distributing it. This unintended consequence of the PPA has resulted from the exponential growth in computer use over the last decade. With the advent of the Internet and widespread computer use, almost any computer can be used to “publish” material. Thus, although Congress intended to limit government searches of places such as newspaper offices when

it passed the PPA in 1980, the PPA now potentially applies to almost any search of any computer. Moreover, because computers now commonly contain enormous data storage devices, wrongdoers can use them to store material for publication -- material that the PPA protects -- while simultaneously storing child pornography, stolen classified documents, or other contraband or evidence of crime.

This amendment clarifies the scope of the PPA, ensuring that its scope reflects Congress' original intent: the government will still be unable to search the offices of the media for work product or documentary materials. This amendment makes clear, however, that with proper judicial authorization, law enforcement officials may search for or seize information or documents that do *not* pertain to publishing (i.e. that are not work product or documentary materials), even if they happen *incidentally* to seize material intended for distribution over the Internet. Thus, the amendment prevents criminals who use computers from using the PPA as a shield to hide their criminal activity.

(9) PURPOSE OF AMENDMENTS TO THE CABLE COMMUNICATIONS POLICY ACT

The Cable Communications Policy Act, passed in 1984 to regulate various aspects of the cable television industry, did not take into account the changes in technology that have occurred over the last fifteen years. Cable television companies now often provide Internet access and telephone service in addition to television programming. This amendment clarifies that when a cable company acts as a telephone company or an Internet service provider, it must comply with the laws governing

the interception and disclosure of wire and electronic communications just like any other telephone company or Internet service provider.

(10) PURPOSE OF AMENDMENTS TO THE BAKER ACT

20 U.S.C. §1232g (the “Baker Act”) prohibits educational institutions that receive federal funding from releasing certain types of information about their students. The Baker Act accommodates the legitimate need for public safety, however, by allowing such institutions to release records in response to a grand jury subpoena. See 20 U.S.C. §1232g(b)(1)(J). Yet the Baker Act fails to take into account the fact that ECPA grants courts the authority to order holders of electronic information -- including educational institutions -- to release certain categories of information to law enforcement. See 18 U.S.C. §2703(d). In order to obtain such an order, however, the law enforcement authority must offer “specific and articulable facts” to justify its need for the records -- a much higher level of justification than that required to obtain a grand jury subpoena. The amendments to the Baker Act rectify this anomaly by allowing educational institutions to release records in response to a section 2703(d) court order.

(11) PURPOSE OF AMENDMENT TO 18 U.S.C. §1029

In recent years law enforcement authorities and the credit card industry have detected the increasing availability on the Internet of software programs that generate valid credit card numbers. These programs, when possessed and run by any person other than authorized representatives of

credit-card issuers, have only one purpose: to generate credit-card numbers that can be used for fraudulent transactions. An amendment to 18 U.S.C. §1029 adds the term “process” to the definition of “device-making equipment” to clarify that the statute applies to software programs that allow criminals to create counterfeit credit cards, just as it does to physical hardware that achieves the same purpose.

B. LEGISLATIVE HISTORY

C. COMMITTEE ACTION

D. SECTION-BY-SECTION ANALYSIS

(1) AMENDMENTS TO THE COMPUTER FRAUD AND ABUSE ACT AND TO THE SENTENCING COMMISSION DIRECTIVE

(a) Subsection 1030(c) -- Definition of computer offenses and penalties

The Department of Justice has encountered several instances in which intruders have gained unauthorized access to protected computers (whether publicly or privately owned) used in the provision of “critical infrastructure” systems and services – such as the computers that run our 9-1-1 emergency services, those that hospitals use to store sensitive information and to treat patients, and

those that the military uses to defend the nation – but where proof of damage in excess of \$5000 has not been readily available. Given the risks posed by the initial act of gaining unauthorized access to protected computers, federal jurisdiction should not be restricted to those instances in which damage of \$5,000 or more can be readily demonstrated. Therefore, amendments contained in section ____ permit federal jurisdiction to attach unambiguously at the outset of an unauthorized intrusion into such systems, rather than requiring investigators to wait for estimates of damage to confer jurisdiction. The amendments modify subsection 1030(c)(2)(A) to provide a misdemeanor penalty that applies to all violations of subsection 1030(a)(5), including those cases when loss of \$5000 or more or other aggravating circumstances cannot be proven.

Section ____ also raises the maximum penalty for felony violations of subsection 1030(a)(5). Certain offenders can cause such severe damage to protected computers that the current five year maximum does not adequately take into account the seriousness of the crime. For example, David Smith recently pled guilty to violating subsection 1030(a)(5)(A) for releasing the “Melissa” virus that caused massive damage to thousands of computers across the internet. Although Smith agreed, as part of his plea, that his conduct caused over \$80,000,000 worth of damage (the maximum dollar figure contained in the Sentencing Guidelines), experts estimate that the real amount of damage could have been as much as ten times that amount. Moreover, where an individual causes this amount of damage during such a violation, the Sentencing Guidelines call for a sentence greater than five years. Thus, amendments to section 1030(c)(2)(C) raise the maximum penalty for violations of this type to ten years.

In addition, section ____ makes a technical change in the statute to clarify the intent requirements for violations of subsection 1030(a)(5). The statute, as currently written, defines “damage” as impairment to the integrity or availability of data, a program, a system, or information that causes loss of at least \$5000; modifies or impairs medical treatment; causes physical injury; or threatens public health or safety. At the time Congress passed this statute, it intended these criteria to create jurisdictional limits on when a violation has occurred.

In order to violate subsections (a)(5)(A) and (a)(7), however, an offender must “intentionally [cause] damage without authorization” or transmit “in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer,” respectively. Congress never intended, however, that the jurisdictional limits contained in the definition of “damage” create additional elements of proof of the actor’s mental state. Importing this technical definition of damage into the intent element may have led courts to mistakenly require the government to prove, for example, in cases brought under subsection 1030(a)(5)(A), that the defendant not only intended to cause damage, but actually intended to cause over \$5,000 dollars worth of damage.

Although the amendments restructure the statute to make clear that the defendant need only intend damage and not a particular amount or type of damage, the amount or nature of the damage remains very important. The subsections concerning special classes of damage are now grafted onto the sentencing provisions that apply to violations of subsection 1030(a)(5)(A) and (B). Under this simplified scheme, all violations of subsection 1030(a)(5) involving protected computers are

punishable by imprisonment for up to one year. However — just as in the current statute — the amendments to subsection 1030(c)(2)(C) punish at the felony level violations of subsection 1030(a)(5)(A) and (B) that (1) result in aggregate loss of \$5000 or more to one or more persons (the amendment changes “individuals” to “persons” to make clearer Congress’ original intent that harm to a business or other legal entity is included);¹ (2) modify or impair medical examination, diagnosis, treatment, or care; (3) cause physical injury; or (4) threaten public health or safety.

Section ____ also clarifies that damage to multiple protected computers must be aggregated in determining whether the violation has exceeded the \$5,000 threshold for a felony offense. For example, an individual may unlawfully access five computers on a network on ten different dates — as part of a related course of conduct — but cause only \$1,000 damage to each computer during each intrusion. It would make no sense to charge such an individual with fifty misdemeanor violations, rather than a single felony count for the \$50,000 of damage that the individual caused. Only aggregation of the damage caused to the various computers properly measures the individual’s culpability for such conduct.²

Moreover, the amendments create a new category of felony violations where a hacker causes

¹ The Court in United States v. Middleton, 35 F.Supp.2d 1189, 1191-92 (N.D. Cal. 1999) correctly held that Congress intended to protect business computers as well as those owned by “natural persons,” and that the definition of damage includes damage to business entities.

² This amendment brings the statute into harmony with other statutes that permit 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 — were properly aggregated in determining whether government met \$5,000 jurisdictional requirement for felony interstate transportation of stolen goods).

damage to a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.³ Further, in order to provide greater deterrence among juvenile hackers, the amendments require that juvenile adjudications for violations of section 1030 act as prior convictions if such juveniles continue to violate section 1030 as adults. The resulting statutory scheme will offer needed flexibility in charging while at the same time enabling application of felony penalties to all serious and harmful violations.

Finally, technical amendments to section 1030(b) and (c) clarify and rationalize the section's treatment of attempted violations but do not change existing law. Just as under the current statute, a conviction for an attempt to violate section 1030 carries the same maximum penalty as a conviction for the completed offense, and it counts as a "prior conviction" for purposes of the section's recidivist sentencing provisions. This technical amendment simply makes clear how the section refers to attempted violations; it does not affect the punishments for such crimes or their treatment under the Sentencing Guidelines.

(b) Subsection 1030(e) -- New and amended definitions

³ Attacks on computers used in the national defense that occur during periods of active military engagement are particularly serious — even if they do not disrupt the war-fighting capabilities of the military — because they divert time and attention away from the military's proper objectives. At the time of sentencing, courts should consider this factor in deciding whether to make an upward departure from the sentencing range recommended by the sentencing guidelines.

(i) *Subsection 1030(e)(2) -- Definition of "protected computer"*⁴

Given the interdependency and availability of global computer networks, it is increasingly likely that hackers from within the United States may begin to concentrate their unlawful activity on systems located entirely outside of this country. Additionally, individuals in foreign countries may route communications through the United States, even as they hack from one foreign country to another. In such cases, their hope may be that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution. This amendment makes clear the intent to include computers outside of the United States within the definition of "protected computers" for purposes of section 1030, if there is any activity affecting the United States. By clarifying the fact that a domestic offense exists, the United States will be able to use speedier domestic procedures in support of international hacker investigations. Moreover, the amendment would create the option, where appropriate, of prosecuting such criminals in the United States. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation in this way will bring more of such offenders to justice.

(ii) *Subsection 1030(e)(8) -- Definition of "damage"*

Truncation of the existing definition of "damage" at subsection 1030(e)(8) is intended to achieve two goals. As discussed in section (1)(a) above, this amendment, in conjunction with the

⁴ Of course, today "computer" includes a wide array of computing devices, such as so-called "personal digital assistants" that pack remarkable computing power.

amendment of section 1030(c), clarifies the precise intent requirements the government must prove in order to establish a violation. Moreover, these amendments are intended to convert the \$5,000 valuation and other criteria previously used to define “damage” from jurisdictional requirements to definitions of the penalties for different acts.

(iii) *Subsection 1030(e)(10) -- Definition of “loss”*

This amendment is intended to clarify the types of expenses the court may take into account in establishing the \$5000 valuation of “damage,” thereby triggering the felony provisions of subsection 1030(c)(2)(C), as amended. This expansive reading of the definition of “loss” is entirely consistent with previous versions of the statute.

The 1996 amendments to the Computer Fraud and Abuse Act further sought to specify what constituted “damage” for purposes of charging subsection 1030(a)(5). The legislative history to those amendments described a situation in which an intruder, having gained unauthorized access and copied portions of a password file, then restores relevant files to their original condition. Congress observed:

Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system. Thus, although there is arguably no “damage,” the victim does suffer “loss.” If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.

Senate Report No. 357, 104th Cong., 2d sess., at 11 (1996). The legislative history to the 1986 amendments confirms that costs incurred through reliance upon altered data may be included in an

overall loss valuation. See Senate Report No. 432, 99th Cong., 2d sess., at 11-12 (1986) (loss from purchases made in reliance upon altered stock market analysis).

By adding a new subsection expressly defining the term “loss,” the amendments clarify the term’s scope and to ensure that it is broadly construed and applied to any and all portions of this section that require a showing of loss. The statutory definition comports with the definition of “loss” recently appended by the U.S. Sentencing Commission to the Federal Sentencing Guidelines (see U.S.S.G. §2B1.1 Commentary, Application note 2). The amendment is intended to reconcile procedures by which prosecutors value loss for charging purposes and by which judges value loss for sentencing purposes. Both determinations, in our view, should permit a degree of flexibility and should take into account 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 interruption of service.

(4) *Subsection 1030(a)(7) and (e)(12) – Definition of “person”*

This pair of amendments clarifies the definition of the word “person” in section 1030. Where the section refers to a “person” – such as where a “person” is the victim of a violation punishable under new subsection (c)(2)(C) – “person” plainly includes government and other legal entities. With this clarification, an amendment strikes surplusage from section 1030(a)(7).

(c) Civil and Criminal Forfeiture

Section ____ creates criminal and civil forfeiture provisions that require anyone convicted of a violation of section 1030 to forfeit to the United States property used or proceeds gained in the commission of the crime. It is the experience of the Department of Justice 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. This appears particularly to be the case with respect to hacking into government computers, even if the offense is a misdemeanor under section 1030(a)(3). These forfeiture provisions, to appear as new subsections 1030(i) and 1030(j), 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) and chapter 46 of title 18, respectively. Thus, the amendments build in all of the existing due process protections in existing law.

(d) Technical and grammatical amendments

Several amendments merely intend to restore technical and grammatical consistency to various subsections of 18 U.S.C. § 1030 following its repeated amendment in 1994 and 1996. None are intended to introduce substantive changes or otherwise affect interpretation of the Act.

In addition, a technical amendment alters section 1030(g) to take into account the new definition of “loss” and its incorporation into subparagraph (c)(2)(C)(i). This amendment is not intended to alter Congress’s previous intent to allow civil plaintiffs only economic damages for violations of section 1030(a)(5) that do not also affect medical treatment, cause physical injury,

threaten public health and safety, or affect computer systems used in furtherance of the administration of justice, the national defense, or national security. Moreover, in order to bring a civil action for a violation of subsection 1030(a)(5) that does not involve one of these special circumstances, the conduct must involve over \$5,000 in damage to a protected computer.

(e) Modification of directive to Sentencing Commission

Section 805 of the Antiterrorism and Effective Death Penalty Act of 1996, P.L. 104-132, 110 Stat. 1214 (April 24, 1996), transmitted a directive to the Sentencing Commission to ensure that all individuals convicted of a violation of sections 1030(a)(4) or (a)(5) be imprisoned for not less than six months. The amendments to section 1030, however, have created a new misdemeanor offense for violation of section 1030(a)(5)(A) where the intrusion does not cause loss valued at over \$5,000 or meet the other requirements for a felony, such as harming the safety, health, or security of others. For this misdemeanor offense, the existing 6-month mandatory appears inappropriate.

Similarly, requiring mandatory imprisonment in cases involving violations of subsection 1030(a)(5)(B) and (a)(5)(C) may not most effectively serve the ends of justice. Such violations, by their nature, occur where an individual intentionally gains unauthorized access to a protected computer system but does not intentionally damage the system. Indeed, a violation of subsection (a)(5)(C), where the hacker only negligently damages the system, constitutes a misdemeanor. It has been noted that, in some instances, prosecutors have exercised their discretion and elected not to charge some defendants whose actions otherwise would qualify them for prosecution under the

statute, knowing that the result would be mandatory imprisonment. In such circumstances, where mandatory imprisonment for 6 months might not be the most appropriate remedy, it is nonetheless best for a federal conviction to occur. A conviction, even one not resulting in mandatory imprisonment, will become a part of the defendant's criminal history and qualify the defendant for the more substantial recidivist provisions of subsection 1030(c) if the defendant does not reform after a first conviction.

Thus, the amendment makes clear that only the more serious, felony violations of subsection 1030(a)(5) qualify for the mandatory 6-month guideline sentence. These amendments are not expected to permit inappropriately light sentences, but rather to better ensure that the punishment fits the crime.

(2) AMENDMENTS TO 47 U.S.C. §223

Various technological advances and the enormous growth of computer use over the last decade have created powerful new tools for an individual to communicate with large numbers of other computer users. For example, electronic mail ("e-mail") enables an individual to send an electronic message to another individual or to a group of addressees. An individual can also utilize an automatic mailing list service (also known as a "listserv" or "mail exploder") to expand his or her audience. The service automatically forwards e-mail it receives from a subscriber to all other people who have subscribed to the service. In a similar way, "newsgroups" act as electronic bulletin boards, allowing individual users to post notices available to the general public. These, and other advances,

have stimulated new patterns of communication and discussion.

While these new methods of communicating have many benefits, they also provide malicious computer users with new methods to harass and abuse others. The amendments to 47 U.S.C. §223 attempt to narrow loopholes in the current statutory scheme created by the advances in computer communications to prohibit such misuse of computer communication systems.

(a) *Subsections (a)(1)(C) and (a)(1)(E)*

Amendments to subsections (a)(1)(C) and (a)(1)(E) assure that section 223 applies to all users of computer network communications, rather than only a portion of such users. Section 223 already prohibits certain actions by individuals using telephones or “telecommunications devices.” Section 223(C), for example, bans anonymous telephone calls or communications intended to harass the person who receives them. Similarly, section 223(E) proscribes repeated telephone calls or communications intended to harass the recipient. Because most methods of accessing the Internet utilize a “communications device” — such as a computer modem — these subsections apply to anonymous or repeated electronic communications sent over computer networks just as they do to traditional telephone calls. See generally American Civil Liberties Union v. Reno, 929 F.Supp. 824, 829 n.5 (1996) (suggesting that modems constitute “communications devices”).

It is possible, however, to access the Internet without a telecommunications device — such as by using a university’s mainframe computer. Distinguishing between users who access the Internet in different ways is arbitrary and illogical. The amendments clarify that subsections 223(C) and 223(E) apply equally to all users of interactive computer services.

(b) *Section (a)(1)(F)*

An amendment creates a new subsection to address a new form of harassment made possible by computers. Subsection (F) prohibits an individual from shutting down a person's e-mail box or other telecommunications facility by causing third parties to send communications to him. A computer user can, for example, place an announcement on a public newsgroup espousing a controversial or extremist position in some social or political debate — advocating white-supremacist beliefs, for example. He can also "sign" the name of person he intends to harass and invite all readers of the message to respond by sending e-mail to that person's home or office e-mail address. This process can cause literally thousands of unwanted messages to bombard the victim, making that person's mailbox unusable and potentially shutting down that person's computer. This act prevents the victim from receiving legitimate communications.

Alternatively, a computer user need not pretend to be someone else in order to stimulate a flood of communications. For example, an individual recently fired from a company could send out thousands of electronic messages stating that the receiver has won a sweepstakes prize. The message could state that in order to claim the prize, the receiver must send an e-mail to the victim's mailbox — in this case the mailbox of the sender's former employer. Once again, this action could flood the mailbox and shut it down, preventing legitimate business from taking place. At a time when more and more business transactions are taking place electronically, this form of harassment can cause substantial harm.

Moreover, existing laws do not clearly prohibit this conduct. Other subsections of Section

223 create penalties for persons making anonymous harassing phone calls and those who repeatedly place calls to a particular person (see 47 U.S.C.A. §223 (a)(1)(C), (a)(1)(E)). The computer user who stimulates communications in the scenarios described above, however, does not violate either of these provisions since he does not contact the victim directly. In addition, depending on the specific facts of an investigation, traditional theories of accomplice and conspiratorial liability may not be easily applied. The abuser does not help others to violate the law because the third parties that actually attempt to communicate with the victim may have no intent to cause harm; indeed, their communications, when viewed individually, may violate no law. Similarly, the abuser does not conspire with the third parties, since they have no knowledge of the abuser's criminal intent and never enter into any form of illicit agreement.

Thus, this amendment criminalizes a computer user's conduct where, with the intent to impair the availability of a protected computer (as that term is defined by the Computer Fraud and Abuse Act, 18 U.S.C. §1030), an interactive computer service, or a telecommunications device, he causes or attempts to cause even unwitting third parties to initiate communications with the victim. The amendment does not inhibit free speech. A computer user may, for example, lawfully post messages encouraging others to contact their political representatives to express their displeasure on some topic of public debate. There, the user intends to stimulate public debate, press for some particular action, or communicate in some way without an intent to shut down their communications system. Indeed, the amendment promotes free speech by prohibiting conduct that would prevent another person from receiving communications. Thus, the proposed amendment

prohibits users from using their computers -- not to communicate -- but as a tool to abuse others.

(c) *Subsection (a)(1)(G)*

An amendment creates a new subsection designed to address another form of abuse made easier by the growth in computer use: the transmittal of personal information – whether true or not – about an individual with the intent to cause them harm or to place them in fear of harm. In one extreme case, for example, a man used such false information to abuse a woman who had spurned his romantic overtures. He posted a personal advertisements on a variety of Internet services pretending to be the woman. In each posting, he claimed – speaking as if he were the woman – that he fantasized about being raped, and he gave the woman’s home address and telephone number. Six times men knocked on her door in the middle of the night responding to the advertisement. When the woman found out why she was being targeted by would-be rapists, she placed a note on her door explaining the hoax. The man then sent e-mails to those who had responded to the Internet advertisement stating that the note on the door was simply part of the fantasy and that she “wanted to be taken by force.” See Greg Miller, *Man Pleads Guilty to Using Net to Solicit Rape*, LOS ANGELES TIMES, April 29, 1999, at C5.

In another case investigated by the United States Secret Service, the target of an investigation created a website that expressed his hatred of a public official and revealed a wide array of personal data about him, including his home address, his telephone number, and the route that his grade-school children took when walking from home to school each day. Although the website did not explicitly threaten the official, the plain intent was to cause him to fear for his life and that of his

children. This section would prohibit such use of communications media in the narrow class of cases in which the person intends to cause injury or property damage to the object of his ire, or to place him or her in fear of injury or property damage.

(e) *Technical amendment*

An additional amendment changes the title of the section to reflect the reality that repeated amendments to the section over the last decade have expanded its scope beyond mere “telephone calls.”

(3) AUTHORIZATION OF FUNDING FOR REGIONAL COMPUTER FORENSICS
LABORATORIES AND THE TRAINING OF STATE AND LOCAL LAW
ENFORCEMENT

Criminals have begun to use computers and the Internet to commit a wide variety of crimes. A far greater number of criminal investigations – even of more “traditional” crimes – involve offenders using computers or the Internet. Such crimes fall into three general categories: (1) crimes in which computers themselves are the victim, such as malicious hacking or the release of damaging viruses; (2) crimes in which the wrongdoer uses a computer to facilitate “traditional” crimes, such as by sending encrypted child pornography over the Internet; and (3) crimes in which the criminal uses the computer as a storage device, such as a drug dealer who stores his tally sheets and records on a laptop computer. The changing nature of criminal investigations and the need to develop effective computer crime prevention and response strategies requires a focused, national effort that involves law enforcement at every level of government.

In particular, the increased use of computers and the Internet by criminals has created an urgent need to enhance the training of state and local law enforcement agencies. To keep pace with these changes, nearly every law enforcement officer requires at least a basic level of cybercrime training – such as how to handle electronic evidence at a crime scene so as to assure that it is not inadvertently damaged or altered. Investigators focused specifically on computer crimes, of course, require more extensive, in-depth training. Moreover, law enforcement officers must receive continuous training in order to stay current with the rapidly changing technology.

The National Cybercrime Training Partnership (NCTP) has provided a vehicle to address this urgent need for cybercrime training. Since 1997, law enforcement officials at the federal, state, and local levels have shared forensic information and resources through NCTP and have thereby dramatically increased the success of multi-state investigations of crime involving computers. NCTP also has identified law enforcement training needs and has developed and provided training to meet those needs. Section ____ authorizes funds for this important effort.

In addition, in order to investigate computer crimes and gather electronic evidence effectively, state and local law enforcement agencies need access to professional, expert computer forensics laboratories. Such laboratories provide the critical function of preserving and analyzing electronic evidence related to a criminal investigation. Forensic laboratories require a substantial investment of resources, however, often costing more than any single agency can hope to pay. In responding to this problem, law enforcement agencies in several regions around the country have pooled their resources to establish regional computer forensics laboratories that can serve the needs

of all of the member agencies. The Department of Justice has provided funding to help establish these laboratories. Further funding is required, however, to establish similar laboratories in other parts of the country and to support the ongoing needs of the existing laboratories. Section __ authorizes funds for these purposes.

(4) DIRECTIVE TO THE SENTENCING COMMISSION TO INCREASE PENALTIES FOR
CRIMES INVOLVING SUBSTANTIAL INVASION OF INDIVIDUAL PRIVACY

In a significant number of federal crimes, the offense may involve a substantial intrusion into an individual's privacy. For example, perpetrators of certain fraud schemes may, in the course of their crime, unlawfully obtain sensitive financial and other data about an individual. Violations of the Computer Fraud and Abuse Act, 18 U.S.C. §1030, also might involve an invasion of individual privacy, such as a case in which a "hacker" obtains a person's medical or psychiatric records by breaking into a hospital computer. Hackers who break into computer networks belonging to companies and universities also commonly read the private e-mail communications of the system's users. For example, Kevin Mitnick, a hacker who recently pled guilty to invading numerous business computers, read thousands of e-mails in the course of these intrusions.

In response to concerns expressed by the U.S. Department of Justice, the Sentencing Commission's November 1997 amendments added commentary to Sec. 2.B.1 ("Theft, Embezzlement, Receipt of Stolen Property, and Property Destruction") to authorize an upward departure "[i]n cases where the loss determined under subsection (b)(1) does not fully capture the

harmfulness of the conduct,” including invasions of privacy.⁵ The Section, however, is limited to certain property offenses; it would not apply in other contexts where the offense does not fall within Sec. 2.B.1, such as certain fraud schemes. Therefore, this section directs the Sentencing Commission to conduct a thorough review of existing guidelines and, if appropriate, to provide an appropriate enhancement where the conduct involves a substantial invasion of a privacy interest that would not be addressed by the otherwise applicable guideline.

(5) AMENDMENTS TO THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, THE WIRETAP STATUTE, AND 18 U.S.C. §3486A

(a) Introduction

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) in an effort to revise and expand the scope of the 1968 wiretap act. In doing so, Congress recognized that emerging technologies — such as electronic mail and voice mail — and other factors had rendered the 1968 statute outdated and inadequate. Moreover, ECPA recognized the need not only to address the changes that had taken place in the intervening 18 years, but also to recast the statute in a technology-neutral manner. This approach, as Congress acknowledged, would better serve to

⁵ Note 15 to Sec. 2.B.1 states in its entirety:

“In cases where the loss determined under subsection (b)(1) does not fully capture the harmfulness of the conduct, an upward departure may be warranted. For example, the theft of personal information or writings (e.g., medical records, educational records, a diary) may involve a substantial violation of a privacy interest that would not be addressed by the monetary loss provisions of subsection (b)(1).”.

accommodate future telecommunications technologies within ECPA's framework.

As a general matter, ECPA's constructs have withstood the test of time. In most cases, the statute struck a workable balance among the competing interests addressed in the statute — the privacy interests of telecommunications users, the business interests of service providers, and the legitimate needs of government investigators.

Notwithstanding the best efforts of those involved in crafting ECPA, however, the statute is in need of amendment. The problems in applying it today principally stem from two factors:

(1) *The explosive growth of the Internet.* In 1986, network computing was in its infancy. Outside of research facilities, high-technology companies, and academia, electronic mail was largely unknown except to small groups of computer hobbyists. The invention of the World Wide Web, and the notion that online service providers would count their U.S. customers in the tens of millions, lay in an unimagined future. Today, of course, the Internet and online activity play an increasing role in daily life. As a corollary of this social shift, the proportion of criminal activity occurring online, or using telecommunications technologies, has also increased enormously. E-mail, voice mail, user access logs, and remotely stored files play an important — and in many cases, critical — role in investigating and prosecuting crimes ranging from extortion and murder to large-scale consumer fraud.

(2) *Inconsistencies and gaps in ECPA itself.* ECPA attained only partial success in

establishing a comprehensive, technology-neutral framework. For example, the 1986 legislation distinguished broadly between “wire communications” (such as voice telephone calls) and “electronic communications,” which received a different level of protection. Not only does this inconsistency create practical problems in today’s network environment — where voice and non-voice data may be intertwined in a single data stream — it also fails to reflect the fact that (as noted above) “electronic communications” today increasingly consist of personal, private information.

The proposed legislation seeks to address these issues without substantially altering the balances struck in 1968 and 1986. Among other objectives, the amendments attempt to

- harmonize the currently disparate treatment of wire and electronic communications;
- increase penalties for a variety of criminal invasions of communications privacy;
- resolve deficiencies in the rules for government access to customer records, especially with respect to access by civil and regulatory agencies; and
- cure omissions and inconsistencies within the statutory framework.

(b) Section-by-section analysis

(1) *Section ___ — Harmonization of “wire” and “electronic” communications*

In large part, ECPA envisioned a world in which technology-mediated voice communications (e.g., telephone calls) are conceptually distinct from non-voice communications (such as faxes, pager messages, and e-mail). To the limited extent that Congress acknowledged that data and voice might

co-exist in a single transaction,⁶ it did not anticipate the convergence of these two kinds of communications typical of today's telecommunications networks. It is no longer merely the case that a single telephone line may be used for data or voice calls; with the rise of Internet telephony, and the rapid migration of traditional telephone carriers to packet-switched networks, it has become increasingly difficult (if not impossible) for investigators to distinguish *ex ante* between voice and data in conducting court-authorized surveillance.

Indeed, the problem arises not only in real-time interceptions, but also in situations in which investigators seek court-authorized access to stored communications. With the advent of MIME — Multipurpose Internet Mail Extensions — and similar features, an e-mail may include one or more “attachments” consisting of any type of data, including voice recordings. As a result, a law enforcement officer seeking to obtain a suspect's unopened e-mail from an ISP by means of a search warrant (as required under 18 U.S.C. §2703(a)) has no way of knowing whether the inbox messages include voice attachments (*i.e.*, wire communications) which may not be compelled under section 2703.

Moreover, the assumptions of 1986 about the respective uses of voice and non-voice technologies no longer hold true. Today, non-voice media are used with increasing regularity for private communications.

Section ____ makes several changes to harmonize the treatment of wire and electronic communications. For instance, it expands 18 U.S.C. §2516(1) to apply the existing prerequisites for

⁶ See, e.g., H. Rep. 99-647 at 35.

court-authorized wire communications interception (such as high-level official approval and the investigation of an enumerated predicate offense) to most electronic communications. In addition, because the investigation of crimes that involve computers and interstate communications systems often require the interception of electronic communications, the amendments add such crimes to the list of enumerated predicate offenses in section 2516(1). Moreover, section 2516(3), which currently allows a federal prosecutor to seek such a wiretap order for electronic communications when investigating any federal felony, is narrowed in its scope: only one-way pager messages would be subject to the looser requirements of section 2516(3).

Commensurate with the above changes, an application to intercept wire or electronic communications need not be limited to a particular category (wire or electronic) of communications. For example, if prosecutors can establish probable cause to believe that a user's Internet account is being used in furtherance of a listed predicate offense, they should be authorized to intercept all pertinent communications made by means of that facility, regardless of whether the past and future communications are voice, non-voice data, or a mixture. This does not, of course, relieve an applicant from the constitutional obligation to specify with particularity the subject matter of the communications to be intercepted.

In recognition of the equal privacy interests implicated by wire and electronic communications, the bill also amends 18 U.S.C. §2515 to allow for statutory suppression of improperly intercepted electronic communications. Corresponding changes are also made to section 2518(10).

Moreover, by adding electronic communications to the scope of section 2515, the statute (in section 2518(5)) expressly permits minimization to be performed after the fact in cases where the intercepted communications are in “a code.” As the 1986 Senate Report recognized in its commentary on this amendment,

the technology used to either transmit or intercept an electronic message such as electronic mail or a computer data transmission ordinarily will not make it possible to shut down the interception and taping or recording equipment simultaneously in order to minimize in the same manner as with a wire interception. It is impossible to “listen” to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation.

S. Rep. 99-541 at 31. With the enormous increase in data transmission speeds since 1986, this concern is even more pronounced today. Investigators are physically incapable of performing real-time minimization even on relatively slow Internet dial-up connections (now commonly established at 56,000 bits per second), let alone on high-speed connections available via ISDN, DSL, and cable modems. Accordingly, the statute will continue to permit *post hoc* minimization where the nature of the technology renders real-time minimization impossible.

In addition to harmonizing the treatment of wire and electronic communications with respect to real-time interception, section ____ also brings into alignment the rules relating to government access to stored communications. Section 2703 is amended to clarify that the existing rules for access to stored e-mail should also apply to voicemail.

(2) Section ____ — “Electronic storage” clarified

In construing the phrase “electronic storage,” a number of courts have been misled by the facial breadth of these words and disregarded the language of the statutory definition at 18 U.S.C. §2510(16). See, e.g., United States v. Smith, 155 F.3d 1051 (9th Cir. 1998); Lopez v. First Union Nat’l Bank, 129 F.3d 1186 (11th Cir. 1997). Even in 1986, Congress made clear that “electronic storage” does *not* encompass all storage of information on a magnetic or similar medium; on the contrary, it refers (at the receiving end) to incoming messages (such as e-mail and voicemail) which the intended recipient has not yet retrieved from a provider. It does not refer to incoming messages left on the provider’s system after they have been accessed by the recipient. See H. Rep. No. 647, 99th Cong., 2d Sess. 64-65 (1986).

Likewise, the phrase should not be misread as applying to communications no longer with the provider, but rather in the possession of the recipient. Cf. United States v. Reyes, 922 F. Supp. 818, 837 (S.D.N.Y. 1996) (erroneously concluding that ECPA was implicated when agents accessed messages stored in a suspect’s pager). ECPA was intended to regulate the relationships among individual users, the providers possessing those users’ records, and third parties such as the government. Given the uncertain application of the Fourth Amendment to customer records held by providers, Congress sought to impose Fourth Amendment-like statutory requirements. See, e.g., H. Rep. 99-647 at 25-26 (discussing pre-ECPA disparity between postal mail and e-mail). Where a communication is held by one of the communicating parties, by contrast, there is no custodian-of-records complexity. Congress did not intend that ECPA apply to this situation because the holder

enjoys direct Fourth Amendment protections.

Accordingly, section ___ seeks to dispel confusion by replacing the term “electronic storage” with the term “interim storage” throughout the statute, and by inserting the phrase “by an electronic communication service” in section 2510(17)(A). The scope of the term remains unchanged.

(3) Section ___ — *Law enforcement assistance to providers of electronic communication services to monitor computer trespassers*

When a computer hacker breaks into a computer belonging to someone else, he threatens the privacy, integrity, and security of the data stored on that computer. Such computer trespassers have no reasonable expectation that the commands sent to that computer will remain private. The wiretap statute, however, only partially recognizes this common-sense fact. Under the current provisions of section 2511(2)(a), victims of computer hacking may monitor electronic communications by trespassers on their computer systems to protect their rights and property. As written, however, section 2511(2)(a) may not allow such a victim to request the assistance of law enforcement in conducting the monitoring of trespassers, even though a trespasser has absolutely no expectation that his communications with the computer that he has broken into will remain private.

This outcome is plainly incorrect. The current subsection forbids victims from taking natural and reasonable steps in their own defense that would be entirely legal in the physical world. For example, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary

happen to fall within the definition of a “wire or electronic communication” according to the wiretap statute.

The crux of this problem arises out of the statute’s treatment of trespassers on the victim’s computer system. Congress intended to create extensive protections for ordinary, legitimate communications. It never intended that these same protections would apply to communications sent by a computer trespasser whose purpose is to break into computers and endanger the privacy and property of others. Just as a physical-world burglar cannot complain if the police monitor his unauthorized use of a victim’s home, so the cyber-world trespasser has no reasonable expectation that his actions inside the victim’s computer system will remain private. Yet the wiretap statute makes no distinction between the commands and communications sent by authorized users and those of trespassers.

When Congress enacted the wiretap statute in 1968, it tailored government surveillance of oral and wire communications to the constitutional mandates announced by the Supreme Court in Katz v. United States, 389 U.S. 347 (1967) and Berger v. New York, 388 U.S. 41 (1967). In the case of oral communications, it incorporated the Fourth Amendment reasonable expectation of privacy test articulated in Katz directly into the definition of “oral communication.” See 18 U.S.C. §2510(2). Apparently because Berger suggested that any use of a telephone system would support a reasonable expectation of privacy, however, Congress did not include in the statute the requirement that the actor have a reasonable expectation of privacy. When Congress added protections against the interception of “electronic communications” in 1986, it followed this example by omitting reference

to a reasonable expectation of privacy. See 18 U.S.C. § 2510(1) (definition of wire communication), 18 U.S.C. § 2510(12) (definition of electronic communication).

At that time, this approach was adequate because individuals almost always possessed a reasonable expectation of privacy in their wire and electronic communications. Although a divergence between the scope of constitutional and statutory protections existed in theory, it did not appear likely to arise in fact. See S.Rep. No. 1097, 90th Cong., 2d Sess., 96 (1968), U.S.Code Cong. & Admin. News 1968, p. 2185 (noting that Title III's provision of a statutory suppression remedy to "any party" to an intercepted wire communication was not intended "generally to press the scope of the suppression role beyond present search and seizure law.").

Increasing reliance on computer networks has exposed the flaw with this approach in the last decade, however. As presently written, the wiretap statute does not distinguish between the interception of authorized telephone and e-mail communications on one hand, and the interception of unauthorized commands sent by computer trespassers who have violated others' privacy or who have begun to destroy or manipulate data on the other. The wiretap statute treats both sets of communications as wire and/or electronic communications, and 18 U.S.C. §2511 prohibits the interception of either absent a court order or an explicit exception. However, the two cases raise different privacy concerns: authorized users enjoy a reasonable expectation of privacy in their wire and electronic communications, whereas electronic trespassers do not. See Rakas v. Illinois, 439 U.S. 128, 143 n. 12 (1978).

As a result, the statute has created the absurd result that these illicit communications enjoy

the strong statutory protections. Reasonable efforts to monitor trespassers – who have no expectation that their activities are private – can themselves result in felony violations of section 2511, as well as suppression of the intercepted communications under section 2515. See United States v. Seidlitz, 589 F.2d 152, 159 (4th Cir. 1978) (noting “a certain speciousness” in a computer hacker’s challenge to a victim’s surveillance of the hacker’s attacks, because “[u]nlike the typical telephone user who employs the telephone merely as a convenience to converse with other persons over distances, [the hacker] used the telephone to tamper with and manipulate a machine which was owned by others, located on their premises, and obviously not intended for his use”).

Moreover, by failing to differentiate between the reasonable expectation of privacy of authorized users and the lack of such expectation by computer intruders, the statute has hampered important investigations. In one case, for example, the Justice Department had to deny victim requests to monitor intrusions in a major cyberterrorism investigation that implicated the national security of the United States. See generally Gregory Vistica, *"We're in the Middle of a Cyberwar": Russian Hackers May Have Pulled Off What Could Be the Most Damaging Breach Ever of U.S. Computer Security*, NEWSWEEK, Sept. 20, 1999, at 52; *Dangerous Doings in Cyberspace*, LOS ANGELES TIMES, Nov. 3, 1999, at B 10. Moreover, although section 2511(2)(a) currently authorizes computer system owners to monitor unauthorized users in self-defense, such owners often lack the expertise, equipment, or financial resources required to monitor these attacks properly.

To correct this problem the amendments to the wiretap statute allow victims of computer attacks to authorize law enforcement officers to monitor trespassers on their computer systems in

a narrow class of cases. Before monitoring can occur, four requirements must be met. First, an amendment to section 2510(20) provides a definition of “computer trespasser” that includes only the unauthorized users of a protected computer. Moreover, section 2511(2)(a)(iii)(D) requires that investigators only intercept the communications of trespassers. If the configuration of the computer system and the technology employed to intercept the communications do not allow interception of only the trespassers’ electronic communications, then the authority under this subsection will not be employed. Thus, the amendment does create any additional authority to intercept the communications of authorized users.

Second, section 2511(2)(a)(iii)(B) requires that the person who intercepts the communication must be lawfully engaged in an ongoing investigation. This requirement makes clear that the investigation must have a lawful purpose, and that the authority to intercept ceases at the conclusion of the investigation. Third, section 2511(2)(a)(iii)(C) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation.

Finally, section 2511(2)(a)(iii)(A) requires that before monitoring may occur, the owner or operator of the protected computer must expressly authorize the interception of the trespasser’s communications. Such authorization should be explicit and specific, rather than the implied consent that is generally sufficient under section 2511(2)(c).

(4) Section ____ — *Enhanced penalties*

Section ____ bolsters the civil and criminal penalties for certain violations of the wiretap statute and ECPA. Most significantly, it eliminates existing section 2511(4)(b), which established a scheme of lesser penalties for certain first-time violations (*e.g.*, those relating to cellular telephones). Regardless of the considerations that originally inspired these reduced penalties in 1986, it is no longer defensible to punish the interception of a cellular telephone conversation with a mere fine (see 18 U.S.C. §2511(4)(b)(i)). The requirement that violations be committed intentionally (see 18 U.S.C. §2511(1)(a)-(d)) ensures that mere inadvertent overhearing of a brief portion of a communication is not criminalized. Cf. S. Rep. 99-541 at 23 (“inadvertent interceptions are not crimes under [ECPA]”).

In addition, the bill raises the maximum criminal penalties for violations of stored communications privacy. First offenses are punishable by up to 1 year in prison (5 years if the offense is committed for a tortious or illegal purpose, commercial gain or advantage, or malicious destruction). Subsequent offenses are punishable by up to 5 years’ imprisonment (10 years if the subsequent offense involves one of the aggravating factors).

Section ____ also resolves a division in the courts over whether 18 U.S.C. §2520 sets a minimum civil penalty of \$10,000 for most eavesdropping violations, or whether the statute permits an award of zero damages. Compare Rodgers v. Wood, 910 F.2d 444 (7th Cir. 1990) (statute mandates minimum award of \$10,000) with Nalley v. Nalley, 53 F.3d 649 (4th Cir. 1995) (finding that court may award zero damages). Given the fact that ECPA clearly subjects violators of chapter 121 (regarding obtaining private stored communications) to a minimum award of \$1,000 (see 18

U.S.C. §2707(c)), it is irrational to permit an award of zero damages for the greater invasion occasioned by real-time interception of private communications. Accordingly, the amendments to section 2520 provide for an award of not less than \$10,000 in civil cases where wrongdoing is proven.

(5) *Section ____ — Prohibited interception devices*

Section 2512 of Title 18 establishes various criminal prohibitions for conduct involving devices capable of illegally intercepting private communications. Specifically, it is unlawful to

(a) mail or carry in interstate or foreign commerce;

(b) manufacture, assemble, possess, or sell; or

(c) advertise via mail or other means transported in interstate or foreign commerce

any device whose design "renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications," provided that the defendant knows (or has reason to know) of such capability. 18 U.S.C. §2512(1)(a), (1)(b), & (1)(c)(i).

It is unclear to what extent the section applies to legal radio scanners which have been modified to intercept wireless telephone calls. The frequency bands allocated for wireless calls typically represent only a small fraction of the overall frequency ranges accessible with a modified scanner. These scanners can also be put to a variety of legitimate uses, such as monitoring the radio traffic of emergency services or sporting events (e.g., stock car races). As a result, the government may not be able to establish that such devices are "primarily useful" for illegal interceptions.

The solution, however, is not to eliminate the "primarily useful" requirement. It is worthwhile to revisit the legislative history of section 2512's enactment. According to the Senate Report accompanying the Omnibus Crime Control and Safe Streets Act of 1968,

[t]he statutory phrase is intended to establish a relatively narrow category of devices whose principal use is likely to be for wiretapping or eavesdropping. A device will not escape the prohibition merely because it may have innocent uses. The crucial test is whether the design of the device renders it *primarily* useful for *surreptitious* listening. . . .

The prohibition will thus be applicable to, among others, such objectionable devices as the martini olive transmitter, the spike mike, the infinity transmitter, and the microphone disguised as a wristwatch, picture frame, cuff link, tie clip, fountain pen, stapler, or cigarette pack. . . .

At the same time, the prohibitions of section 2512 will cause no substantial interference with the production, distribution, or use of legitimate electronics equipment, whether by the electronics industry or others. Size alone is not the criterion under the section. A device does not fall under the prohibitions merely because it is small, or because it may be adapted to wiretapping or eavesdropping.

S. Rep. No. 1097, 90th Cong., 2d Sess., reprinted at 1968 U.S. Code Cong. & Admin. News 2112, 2183 (emphasis in original).

The foregoing makes clear that Congress chose the "primarily useful" standard precisely because of its narrowness. If the standard were changed to encompass any device "useful" for surreptitious interception, the statute would effectively criminalize such items as conventional tape recorders or the parabolic microphones used by broadcast networks in covering sporting events. Congress wisely elected to prohibit a narrower class of devices, and it is improvident to eliminate

the term "primarily" from the statute.

Nevertheless, section 2512 can be effectively revised to address the growing problem of wireless telephone call interception, and in a manner that does not impair the distinctions Congress had in mind in 1968. When Congress drew the proscriptive line at devices "primarily useful" for intercepting communications, it did so because there was no more precise, technical way to distinguish between a legal microphone and "the martini olive transmitter." Scanners capable of intercepting the frequencies dedicated to wireless communications, by contrast, can be defined with relative precision.

Thus, section ____ amends Chapter 119 to cover those scanners whose manufacture or importation is prohibited by (and subject to civil fines and forfeiture under) FCC regulations. This amendment expands the criminal penalties of section 2512 to cover newly imported or manufactured scanners whose cellular interception capability represents only a fraction of their overall frequency range. The new language makes such scanners *per se* "primarily useful" for illegal eavesdropping, regardless of whether they have other lawful uses.

Consistent with the FCC regulations, however, the amendment would not criminalize such scanners if the scanners were manufactured or imported prior to April 26, 1994. By making this distinction, the proposed amendment would inhibit the future availability of illegal scanners without criminalizing the currently lawful possession of a pre-1994 scanner that can receive cellular frequencies.

The amendment addresses a second potential shortcoming in section 2512. Subsection (1)(c) criminalizes the advertisement of interception devices via "newspaper, magazine, handbill, or other

publication . . . sent through the mail or transported in interstate or foreign commerce." To date, there have been no cases addressing the issue of whether this language applies to advertisements on the Internet; indeed, there do not appear to be any decisions discussing the statute's applicability even to traditional electronic media such as radio or television. Rather, court decisions have discussed section 2512(1)(c) only in cases involving physical media such as catalogs or brochures. Further, the history of the original legislation creating section 2512 -- title III of the Omnibus Crime Control and Safe Streets Acts of 1968 -- sheds no light on the scope of this language.

It is unclear whether the courts would apply this provision to Internet advertising. This uncertainty stems from certain federal appeals court decisions holding that similar language in other federal criminal statutes does not reach intangible materials. For example, the Tenth Circuit has held that sections 1462 and 1465 of Title 18 -- proscribing the interstate "carriage" or "transport[]," respectively, of obscene matter -- do not reach conduct involving intangible articles such as prerecorded "phone sex" messages delivered over telephone lines. See United States v. Carlin Commun., Inc., 815 F.2d 1367, 1371 (10th Cir. 1987).

Other courts, however, have interpreted these same statutes as applying to intangible materials. Thus, the Sixth Circuit has applied section 1465 to the transmission of obscene computer image files over long-distance telephone lines. See United States v. Thomas, 74 F.3d 701, 706-07 (6th Cir. 1996), cert. denied, 117 U.S. 74 (1996).⁷

⁷The 1996 Communications Decency Act amended sections 1462 and 1465, expressly prohibiting the interstate carriage or transportation of obscene matter via "interactive computer service." See Pub. L. 104-104, Title V, §507, 110 Stat. 137.

As a result of these divided interpretations of comparable language in other federal statutes, it is not clear whether courts will apply subsection 2512(1)(c) in its present form to Internet advertisements for interception devices. A court could, for example, interpret "newspaper, magazine, handbill, or other publication" to mean only tangible publications. Yet electronic advertisements for devices that violate section 2512 cause the same problems and harms as advertisements in print media. Accordingly, the amendment to subsection 2512(1)(c) makes both forms of advertising equally illegal.

(6) *Section ____— Clarification of inapplicability of 18 U.S.C. §2515 to certain disclosures*

This section makes a carefully limited clarifying amendment to 18 U.S.C. §2515, the statutory exclusionary rule for violations of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, so as clearly to exempt two situations: (1) those in which private individuals illegally intercept or record a communication, but the recording later comes into the possession of a party in a criminal trial, who then wishes to introduce it; and (2) those in which a government actor violates chapter 119 (e.g., by engaging in an illegal wiretap) and the government thereafter seeks to use the communication to prosecute that violator.

At present, appellate decisions are in apparent conflict over whether section 2515 precludes the use of communications in the first category described above. Under one possible interpretation of section 2515, if a private individual consensually records a conversation in aid of an illegal activity, or illegally records a conversation between other parties without their consent, the contents

of such recordings are not admissible in a criminal trial or hearing even if the government had no role in having the evidence recorded and only acquired it, through lawful means, at a later date. This situation occurs because, under 18 U.S.C. §2511(2)(d), a consenting party, not acting under color of law, may record only if the recording is for a non-criminal or non-tortious purpose. Thus, if the payer of a bribe secretly records the transaction in which he or she pays the bribe to an official, and the government later obtains the recording and seeks to use it against the official to prove the bribe, section 2515 arguably precludes such use. One appellate court has so held. United States v. Vest, 813 F.2d 477 (1st Cir. 1987).

By contrast, another appellate court has held that section 2515 does not bar the government from using recordings made by an illegal gambling business (of bets placed by telephone) to prevent disagreements with bettors over the amounts of their bets. United States v. Underhill, 813 F.2d 105 (6th Cir.), cert. denied, 484 U.S. 821, 846 (1987). While the court in Vest acknowledged that no deterrent purpose would be served by suppression because the government played no role in the illegal recording, it relied on the fact that further disclosure in court of the contents would magnify the original privacy violation. The court in Underhill, on the other hand, relied on clear legislative history indicating that Congress, despite the facial breadth of section 2515, did not intend to permit lawbreakers to immunize themselves from prosecution by the very criminal purposes that made the recordings illegal.

The same disagreement among circuit courts exists regarding the admissibility of recordings made by private actors intercepting communications without the consent of any of the parties. In one case, a court barred the use before a grand jury of such illegally intercepted communications. See

In re Grand Jury, 111 F.3d 1066 (3d Cir. 1997). By contrast, where a wife secretly installed a recording device to intercept her husband's conversations with other persons, the Sixth Circuit concluded that section 2515 did not bar the use of the contents of those communications in a prosecution of the husband, given the government's lack of involvement in the original interception. See United States v. Murdock, 63 F.3d 1391 (6th Cir. 1995).

Whether or not Vest and In re Grand Jury were correctly decided under the existing statutory provision, an exemption should be created under section 2515 for that narrow class of cases in which the government lawfully obtains illegal recordings made by private parties and seeks to use them as evidence in a criminal trial or hearing. The truth-seeking function of a criminal proceeding is of paramount importance. In the absence of any deterrent purpose to be served by exclusion, this truth-seeking function should prevail over the concern that disclosure in the criminal proceeding would somehow exacerbate the original illegal recording.

Conversely, if evidence contained in an illegally intercepted recording tends to exculpate a defendant, that defendant should be entitled to introduce the evidence so long as he did not participate in the interception in any way. The instant amendment thus reflects the belief that a private violation of the statute should not trigger the severe result of exclusion of otherwise probative evidence in a criminal case (just as the Fourth Amendment, of course, does not apply to non-governmental searches and seizures⁸). Accordingly, this section would amend section 2515 to

⁸ The history of section 2515's original enactment makes clear that Congress intended that it embody existing Fourth Amendment standards. See S. Rep. No. 1097, 90th Cong. 2d Sess., reprinted in 1968 U.S.C.C.A.N. 2112, 2185 (no intention "to press the scope of the suppression role beyond present search and seizure law").

expressly exempt such disclosures from its purview.

In addition, the amendment would also permit the use of illegal intercepts made by governmental actors for the limited purpose of prosecuting those actors. In one recent case, United States v. Grice, 37 F. Supp. 2d 428 (D.S.C. 1998), an employee of a county sheriff's department illegally intercepted conversations between two prisoners and their attorneys. When the United States sought to use the recording to prosecute that violation, the district court ruled the evidence inadmissible. The amendment would permit such use, but only for the limited purpose of prosecuting the violator of chapter 119; the recordings could not be used against the victims of the violation even if those recordings contained evidence of separate criminal activity by such victims. A conforming amendment is also made to section 2518(10)(a).

(7) Section ____ — *Voluntary disclosure of customer records*

Section ____ addresses a number of deficiencies in sections 2702 and 2703 of Title 18. Currently, section 2702 regulates the ability of public service providers to voluntarily disclose the contents of stored customer communications (including stored files) to others. Section 2703, on the other hand, establishes rules by which the government may compel a provider to produce either the contents of stored customer communications or non-content\ records (such as system activity logs and identifying information). Section 2703 (in subsection (c)) also addresses the issue of providers' voluntary (i.e., non-compelled) disclosure of non-content customer records.

The first change made by section ____ is structural. The amendments relocate the permissive

disclosure rules of section 2703 to section 2702. Thus, section 2702 will now regulate all permissive disclosures (of content and non-content records alike) by public providers. Section 2703 will only cover compulsory disclosures by providers (both public and nonpublic).

Second, section 2702 is amended to permit, but not require, a service provider to disclose either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. Under current law, if an ISP's customer receives an e-mail death threat from another customer of the same ISP, and the victim provides a copy of the communication to the ISP, the ISP is limited in what actions it may take. On one hand, the ISP may disclose the contents of the forwarded communication to law enforcement (or to any other third party as it sees fit). See 18 U.S.C. §2702(b)(3). On the other hand, current law does not expressly authorize the ISP to voluntarily provide law enforcement with the identity, home address, and other subscriber information of the user making the threat. See 18 U.S.C. §2703(c)(1)(B),(C) (permitting disclosure to government entities only in response to legal process). In those cases where the risk of death or injury is imminent, the law should not require providers to sit idly by. This voluntary disclosure, however, in no way creates an affirmative obligation to review customer communications in search of such imminent dangers.

Section ____ also cures a drafting omission in the 1986 legislation. Under existing law, a provider (even one providing services to the public) may disclose the contents of a customer's communications — to law enforcement or anyone else — in order to protect its rights or property. See 18 U.S.C. §2702(b)(5). However, the current statute does not expressly permit a provider to

voluntarily disclose *non-content* records (such as a subscriber's login records) to law enforcement for purposes of self-protection. See 18 U.S.C. §2703(c)(1)(B). Yet the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records. Cf. United States v. Auler, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (phone company's authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device) (citing United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975)).

Moreover, as a practical matter providers must have the right to disclose the facts surrounding attacks on their systems. When a telephone carrier is defrauded by a subscriber, or when an ISP's authorized user launches a network intrusion against his own ISP, the provider must have the legal ability to report the complete details of the crime to law enforcement. To clarify that service providers do have the statutory authority to make such disclosures, the bill inserts appropriate language into new subsection 2702(c)(3).

In interpreting section 2702 (and section 2703), it is critical to understand who constitutes a "subscriber or customer" of an "electronic communication service" or "remote computing service." Obviously, an ISP's accountholders, who typically pay a monthly or annual fee, qualify.

Such a fee-for-service arrangement is neither necessary nor sufficient by itself. The users of some free services — for example, free Web-based e-mail providers — should properly be understood to enjoy the protections of ECPA. However, consider the users of a for-pay Web site that provides access to a proprietary database of information: unlike an ISP or Web-based e-mail

service, the database provider is not acting as an electronic communication service or remote computing service (i.e., it neither provides the intermediate means of communicating with third parties, nor furnishes storage or processing of a user's own data). Thus, although the database service may be said to have subscribers or customers, the nature of the service itself takes those users' records outside the scope of ECPA.

Naturally, records reflecting the activity of a computer network intruder normally do not qualify for protection as subscriber records. In the special case where an intruder misuses the account of an ISP's legitimate subscriber, records concerning activity in the account should be treated as subscriber records; note, however, that they may be disclosed with the legitimate subscriber's consent, or pursuant to the ISP's protection of its rights and property.

(8) *Section ____ — Government access to customer communications and records*

Existing section 2703 establishes the mechanisms by which governmental entities may compel a provider to produce certain subscriber records. The proposed amendments make a number of changes to eliminate surplusage, provide for access by non-law enforcement agencies (e.g., regulatory agencies such as the FTC and SEC), and clarify the meaning of certain terms.

Section 2703(b) concerns governmental access to the contents of electronic communications held (1) by an electronic communications system for more than 180 days or (2) by a remote computing service. Currently, under section 2703(b) a governmental entity can obtain the contents of such electronic communications (e.g., opened e-mail) without prior notification to the subscriber

by means of a Federal or state search warrant. Using an administrative, grand jury, or trial subpoena (or a court order under § 2703(d)) requires prior notice to the subscriber, although notice can be delayed under certain circumstances. The statute does not discuss the applicability of pre-trial subpoenas (*i.e.*, a subpoena duces tecum), commonly employed in civil discovery.

The proposed amendment makes two changes. First, it bars the delay of notice where a party uses a trial subpoena. Second, it permits a party to use an authorized subpoena duces tecum, again with advance notice to the subscriber required (and nondelayable). This amendment permits governmental agencies with civil investigative authority to obtain the contents of wire and electronic communications related to their investigative jurisdiction, and also permits the government, when it is a party in litigation, to obtain the contents of wire and electronic communications in the same manner as any private litigant.

Section ___ also amends sections 2703(c) and (d), sections that regulate governmental access to non-content records pertaining to a subscriber of an electronic communications service or a remote computing service. Under current law, a governmental agency may generally obtain such records through subscriber consent, a criminal search warrant, or an order under 2703(d); in addition, records falling within an enumerated list may be compelled with a subpoena under subsection 2703(c)(1)(C).

In order to obtain an order under section 2703(d), currently the government must offer specific and articulable facts showing reasonable grounds to believe that the transactional records or other information sought are relevant and material to an ongoing *criminal* investigation. Thus, civil investigative authorities have no means under current law to obtain transactional records (other

than the limited information covered by 2703(c)(1)(C)). The proposed amendment revises section 2703(d) to permit agencies having civil investigative authority to obtain transactional records through the use of a court order (with no notice to the customer required). In the alternative, a governmental entity may obtain all of a customer's transactional records by using a subpoena (such as a grand jury, trial, or administrative subpoena, or a subpoena duces tecum) with prior notice to the subscriber.

Thus, a governmental entity will have to make a choice when it seeks to obtain not only a customer's basic subscriber information but all non-content, transactional records. To compel all such records, and to do so without giving notice to the customer, the government must use a search warrant or a court order under section 2703(d). If, on the other hand, the government is willing to provide prior notice to the customer, it may use a subpoena.

The proposed amendment retains the mechanism — embodied in current subsection 2703(c)(1)(C) — through which the government may, without giving notice, compel a limited class of information. To be redesignated as § 2703(c)(2), this provision permits the use of a subpoena to compel subscriber identifying information, telephone records, and the like. The amendment broadens the scope of authorized subpoenas, including explicitly adding subpoenas duces tecum to the list of legal process that may be used to compel such records.

The amendment also redresses certain anomalies in the existing subsection 2703(c)(1)(C), which does not mention certain records (such as credit card number or other form of payment) also relevant to determining a customer's true identity. In many cases, users register with Internet service

providers using false names, making the method of payment an essential means of determining true identity.

In addition, section ____ cures another imbalance in the existing subsection 2703(c)(1)(C), which permits disclosure of certain transaction-related information (“local and long-distance telephone toll billing records”⁹). The amendment expands the categories of information available by adding “records of session times and durations,” as well as “any temporarily assigned network address.” In the Internet context, such records would include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session (such as when the user connects via telephone dial-up) or the remote IP address from which a customer connects to the provider (as where the user, already connected to one Internet host, connects via the Internet to the provider who is the recipient of the subpoena).

This amendment does not permit a governmental entity to compel other transaction-related records, such as the e-mail addresses of the persons with whom the customer has corresponded in the past (see H. Rep. No. 103-827 at 31), or the IP addresses of the web sites that the person visited during a given session. To obtain such records, the government must use a section 2703(d) court order (as is the case today), or a subpoena with prior notice (not delayable) under the language of

⁹ The bill amends the phrase “local and long distance telephone toll billing records” to refer instead to “local and long distance telephone connection records.” This change makes explicit the existing rule that records of local calls are included, even where such calls do not incur additional per-call charges. See In re Grand Jury, 894 F. Supp. 355, 359 (W.D. Mo. 1995) (subpoena may be used to compel “all records of calls from or attributed to a particular number, regardless of whether, in fact, a separate charge is assessed for each call”).

new section 2703(c)(1)(C).

Further, section 2703(d) contains an anomaly: although it explicitly permits state investigators to obtain court orders to obtain records from electronic communication services, it grants only federal courts jurisdiction to issue such orders. The amendment to section 2703(d), together with an expanded definition of “court of competent jurisdiction” contained in section 2711(3), clarifies that both federal and state courts have the power to issue orders pursuant to section 2703(d).

Finally, new section 2703(c)(3) addresses a growing problem in online law enforcement. In many cases, investigators may observe evidence of a crime (such as admissions by a participant in an online chat room) but lack evidence that the crime is one over which they have jurisdiction. For example, federal investigators have observed chat room participants admitting to incestuous sexual relations with their minor children, a crime normally subject to state (but not federal) prosecution. In such cases, the investigator cannot open an investigation, and cannot readily determine which jurisdiction has proper authority over the offense. In order to facilitate such referrals, new section 2703(c)(3) permits a governmental entity to require the provider to disclose, on the basis of a written request, the geographical location (city, state, country) associated with the user. Such a request may not call for the user’s street address, real name, or other information.

(9) *Section ____ — Delay of notice provisions; extensions*

Where notice to subscriber is required under § 2703(b), such notice may be delayed under

section 2705(a). Under present law, the delay may be authorized administratively (*i.e.*, without the intervention of a judicial officer) under § 2705(a)(1)(B). While this delay may be extended in accordance with § 2705(a)(4), that section is ambiguous on the question of whether the extension may also be approved administratively or only on the authority of a court (“only in accordance with subsection (b)”). The amendment makes clear that only a court order may authorize extensions of delay beyond the initial 90-day period.

(10) *Section ____ — Requests to preserve historical customer records*

In 1996, Congress added subsection (f) to 18 U.S.C. §2703, providing a mechanism whereby investigators may require a service provider to preserve historical customer records pending the issuance of legal process. Because such records (whether in the form of communications contents or transactional records) are often ephemeral, this amendment met a critical law enforcement need.

However, on rare occasions, a provider may refuse to comply with this request. Section 2707 already creates a civil remedy to redress violations of ECPA. Since some doubt may exist over our intent to allow the government to bring suit under section 2707, the amendment to section 2703(f) clarifies that the government entity requesting records’ preservation may maintain a cause of action under section 2707 against the noncomplying provider.

(12) *Section ____ — Miscellaneous corrections*

Section ____ strikes duplicative language found at 18 U.S.C. §2516(1)(p). It also corrects

certain statutory cross-references in 18 U.S.C. §2510. In addition, it amends 18 U.S.C. §2511(2)(g)(i) so that wire communications that the sender intentionally makes readily accessible to the general public — like such electronic communications under the present statute — may be intercepted without violating Chapter 119. The amendment clarifies that this subsection does not relate to radio communications; rather, those communications are addressed separately in existing §2511(2)(g)(ii). Finally, 18 U.S.C. §2518(7) contains a technical amendment to clarify an incorrect reference to subsection 2518(8)(d).

(13) *Section ____ – Technical Amendment to 18 U.S.C. 3486A*

Section 2703(c) of Title 18 grants government agencies the authority to issue administrative subpoenas for certain basic subscriber information. Section 3486A of Title 18 implements this provision by defining the circumstances under which a government entity may obtain such information during an investigation of child abuse or child exploitation. Section ____ makes a technical amendment to this provision to make it conform to changes in section 2703(c).

(6) AMENDMENTS TO THE STATUTE GOVERNING PEN REGISTERS AND TRAP AND TRACE DEVICES

(a) *The Need for Updating*

The existing legal procedures for pen register and trap-and-trace authority are antiquated and need to be updated. Changes in technology and the communications industry have made orders for the installation of pen registers or trap and trace devices ineffective in many recent criminal

investigations. For example, in 1996, a hacker (who later turned out to be launching his attacks from a foreign country) extensively penetrated DOD computers. This hacker was dialing into a computer at Harvard University and used this computer as an intermediate staging point in an effort to conceal his location and identity. Investigators obtained a trap and trace order instructing the phone company, Nynex, to trace these calls, but Nynex could only report that the communications were coming to it from a long-distance carrier, MCI. Investigators then applied for a court order to obtain the connection information from MCI, but since the hacker was no longer actually using the connection, MCI could not identify its source. Only if the investigators could have served MCI with a trap and trace order while the hacker was actively on-line could they have successfully traced back and located him.

In addition, investigators encountered similar difficulties in attempting to track Kevin Mitnick, a criminal who continued to hack into computers attached to the Internet despite the fact that he was on supervised release for a prior computer crime conviction. The FBI attempted to trace these electronic communications while they were in progress. In order to evade arrest, however, Mitnick moved around the country and used cloned cellular phones and other evasive techniques. His hacking attacks would often pass through one of two cellular carriers, a local phone company, and then two Internet service providers. In this situation, where investigators and service providers had to act quickly to trace Mitnick in the act of hacking, only many repeated attempts – accompanied by an order to each service provider – finally produced success. Fortunately, Mitnick was such a persistent hacker that he gave law enforcement many chances to complete the trace. Most cases will

not provide that opportunity, however.

Substantial changes in the communications industry since the original 1986 legislation have made the current statute outdated. These changes can be divided into two categories: technological and legal.

(i) *Technological changes*

The existing statute speaks of a pen register or trap and trace “device” being “attached” to a telephone “line.” However, the rapid computerization of the telephone system has changed the tracing process. No longer are such functions normally accomplished by physical hardware components attached to telephone lines. Instead, these functions are typically performed by computerized collection and retention of call routing information passing through a communications system.

Another technological change is the development and deployment of wireless telephone technology. The statute's definition of a “pen register” as a “device” that is “attached” to a particular “telephone line” is particularly obsolete when applied to the wireless portion of a cellular phone call, which has no line to which anything can be attached. While courts have authorized pen register orders for wireless phones based on the notion of obtaining access to a “virtual line,” updating the law to keep pace with current technology is a better course.

Moreover, the statute is ill-equipped to facilitate the tracing of communications that take place over the Internet, which has developed explosively over the last ten years. For example, the pen register definition refers to telephone “numbers” rather than on the broader concept of a user's

communications account. Although pen register and trap orders have been obtained for activity on computer networks, Internet service providers have challenged the application of the statute to electronic communications, frustrating legitimate investigations. Amendments to the statute are needed to clarify the statute's proper application to tracing communications in an electronic environment. These amendments do not, however, affect what data electronic communication service providers must be capable of providing to law enforcement in response to a court order; other statutes address the assistance capabilities of providers.

(ii) *Legal developments*

Because of deregulation of the telecommunications industry, one communication may be carried by multiple providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it at a switch to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to an incumbent local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not pass source information with each call, identifying that source may require compelling information from a host of providers located throughout the country.

Under present law, a court may only authorize the installation of a pen register or trap device "within the jurisdiction of the court." As a result, when one provider indicates that the source of a communication is a carrier in another district, a second order may be necessary. Indeed, in one case the Justice Department needed four separate orders to trace a hacker's communications. This duplicative process of obtaining a separate order for each link in the communications chain can be

quite time-consuming, and it serves no useful purpose since the original court has already authorized the trace. Moreover, a second or third order addressed to a particular carrier that carried part of a prior communication may prove useless during the next attack: in computer intrusion cases, for example, the target may use an entirely different path (*i.e.*, utilize a different set of intermediate providers) for his or her subsequent activity.

(b) *Scope of the Update*

As noted above, the amendments seek to improve the statute in two crucial respects. First, they clarify that the statute applies not only to landline telephone devices, but also to the full range of communications facilities that carry "wire" or "electronic" communications, including wireless telephones and computer user accounts.

The legislation also provides that for federal investigations, a single court order shall apply to all carriers providing service in the United States who are carrying the communications identified in the order. For such circumstances, the legislation also removes the prohibition on disclosure of tracing information that would otherwise apply to communications providers.

(c) *Section-by-Section Analysis*

(i) *Issuance of trace orders*

Section ____ divides existing 18 U.S.C. §3123(a) into two separate provisions. New subsection (a)(1), applicable only to federal investigations, provides for the applicability of the order to any provider of communication services in the United States whose assistance is appropriate to effectuate the order. If information that is the subject of an order under the statute is available from

more than one provider, the order may be served on any provider that has access to the information.

For example, a federal prosecutor may need to obtain an order to trace calls made to a telephone within the prosecutor's local district. The order will apply not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, the law enforcement officer may have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication's path and the next carrier in the chain. The officer would then serve the same court order on the next carrier, as well as convey the relevant connection information learned from the first carrier; the second carrier would provide the connection information in its possession for the communication. The officer would repeat this process until he serves the order on the originating carrier who is able to identify the source of the communication.

Consistent with the change above, section ____ also amends Section 3123(b)(1)(C) so that the geographic limits of a trap and trace order need not be specified in federal investigations. However, because the new law contemplates nationwide effect for orders obtained by federal authorities, section ____ amends 18 U.S.C. §3127(2)(A) to impose a "nexus" requirement that the issuing court have jurisdiction over the particular crime being investigated.

(ii) *Technological neutrality*

Section ____ updates the language of the statute to clarify that it applies to a broad variety of communications technologies. References to the target "line," for example, are revised

April 24, 2000

to encompass a "line or other facility." Such a facility might include, for example, a cellular telephone number; a cellular telephone identified by its electronic serial number (ESN); an Internet user account or e-mail address; or an Internet Protocol (IP) address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, section 3123(b)(1)(C) allows applicants for pen register or trap and trace orders to submit a description of the communications to be traced that uses a combination of these descriptors, as well as other facts and evidence in the particular investigation.

Moreover, the amendments clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information -- all "dialing, routing, addressing, and signaling information" -- utilized in the processing and transmitting of wire and electronic communications.¹⁰ This concept, that the information properly obtained by using a pen register or trap and trace device is non-content transactional data, applies across the board to all communications media, and to actual connections as well as attempted connections (such as busy signals and similar signals in the telephone context and packets that merely request a telnet connection in the Internet context).

Further, because the pen register or trap and trace "device" is often incapable of being physically "attached" to the target facility, section ____ makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of

¹⁰ Thus, for example, non-content information contained in the "options field" of a network packet header constitutes "signaling" information and is properly obtained by an authorized pen register or trap and trace device.

physical mechanisms, the amendment allows the pen register or trap and trace device to be "attached or applied" to the target facility. Likewise, the definitions of "pen register" and "trap and trace device" in section 3127 are revised to include an intangible "process" (such as a software routine) which collects the same information as a physical device.

(iii) *Emergency Authority*

Amendments to section 3125 add long-overdue exceptions for immediate threats to national security (corresponding to the emergency wiretap provision at 18 U.S.C. § 2518(7)(a)(ii)), immediate threats to public health or safety, and investigations under the National Information Infrastructure Protection Act, 18 U.S.C. § 1030. In the last of these three circumstances, rapid investigative response is made essential both by the nature of the medium—in which attackers may move seamlessly and almost instantaneously through a series of "stepping stone" victim sites, launching attacks from each — and by the often ephemeral character of network routing evidence. Of course, amending the statute to allow government entities to install and use pen register and trap and trace devices without prior authorization involving an emergency threatening national security in no way limits the government's ability to exercise its non-statutory powers in such emergency situations.

(7) AMENDMENTS TO THE JUVENILE DELINQUENCY CHAPTER CONCERNING
TRANSFER OF JUVENILES FOR CRIMINAL PROSECUTION

This bill modifies section 5032 of title 18 to allow the federal government to investigate and prosecute juveniles who commit certain serious computer offenses. In recent years, computers and

the Internet have enabled juvenile offenders to commit crimes and create risks to the public like never before. For example, juvenile hackers have penetrated numerous sensitive computers, including computers run by the Defense Department, even when military operations were being planned or were in progress. In addition, in March of 1998, a juvenile hacker interfered with a computer that provided telecommunications services to an entire community in central Massachusetts, including its regional airport. This action interrupted communications between the airport and approaching aircraft, disrupting its ability to operate safely at night. Moreover, federal law enforcement officials plainly should have the power to investigate and prosecute intrusions into federal computers. Yet prior to these amendments, federal jurisdiction would not necessarily attach in any of these cases. When an individual attacks a federal computer, or when a hacker uses interstate communications or the Internet to compromise the health, safety, or security of the public, it clearly raises substantial federal interests and warrants federal jurisdiction.

(8) AMENDMENTS TO THE PRIVACY PROTECTION ACT

The Privacy Protection Act of 1980 ("PPA"), 42 U.S.C. § 2000aa, et seq., makes it unlawful for local, state, or federal law enforcement authorities to "search for or seize any *work product materials*" or any "*documentary materials* ... possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. § 2000aa(a), (b). The statute defines "work product materials" as materials prepared or possessed in anticipation of communicating such materials to the public,

except if the materials constitute contraband or the fruits or instrumentalities of crime. Id. § 2000aa-7(b). "Documentary materials," on the other hand, consist of materials upon which information is recorded, once again with the exception of contraband and the fruits or instrumentalities of crime. Id. § 2000aa-7(a). Thus, other than for the exceptions, the PPA effectively imposes a "no-search" rule on work product materials and a "subpoena-first" rule on documentary materials held by third parties who plan to use them to communicate to the public. Although the statute appears reasonable on its face, its application in the current electronic environment has inadvertently shielded criminal activities from legitimate law enforcement investigations, such efforts to arrest and prosecute those who distribute child pornography over the Internet.

(a) Intent of the PPA

Congress passed the PPA in response to the Supreme Court's decision in Zurcher v. Stanford Daily, 436 U.S. 537 (1978). In Zurcher, the Supreme Court upheld a police search, pursuant to a valid search warrant, of the offices of The Stanford Daily newspaper for photographs taken at the scene of a crime. The Court rejected the newspaper's claim that search warrants could not be used to recover evidence from those engaging in First Amendment-protected activities. Id. at 565-567. The Court also held that law enforcement officers could use search warrants to recover evidence from innocent third parties. Id. at 555 ("state's interest in enforcing the criminal law and recovering evidence is the same whether the third party is culpable or not"). The Court concluded, therefore, that "the critical element in a reasonable search is not that the owner of the property is suspected of

a crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *Id.* at 556.

In response to the Court's ruling, Congress passed the PPA. Congress intended to restrict searches for mere evidence of crime held by *innocent third parties* who were engaged in First Amendment-protected activities — evidence that law enforcement officials might otherwise obtain through less intrusive means, such as by issuing a subpoena. The purpose of restricting law enforcement in this fashion, of course, was to protect the confidentiality of non-evidentiary files also held by this special group of innocent third parties — both the drafts of articles not yet published and the research and other supporting information (e.g., notes and interviews) which they never intended to publish. Thus, the PPA protects an author or publisher (like The Stanford Daily) — who is not a suspect in the investigation — from law enforcement attempts to search through his or her work product or documentary materials in order to find and seize evidence. To preserve the confidentiality of these designated materials, the PPA instructs investigators not to search for the evidence at all, but to compel the innocent third parties to find and produce it themselves. This goal of Congress remains unchanged, and our amendments do not alter this protection for innocent third parties.

Congress never intended, however, to protect criminals from court-authorized searches, and the legislative history to the PPA is replete with statements to this effect. For example, the Senate Judiciary Committee Report stated that the purpose of the PPA is to "limit searches for materials held by persons involved in First Amendment activities *who are themselves not suspected of* participation in the criminal activity for which the materials are sought." S. Rep. No. 96-874, 96th Cong., 2d Sess. 11 (1980), reprinted in 1980 U.S.C.C.A.N. 3950, 3957 (emphasis added). Moreover,

the Committee Report stated that the intention in enacting the PPA was "not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation." *Id.* Indeed, the language of the statute itself allows searches and seizures of any person who "has committed or is committing the criminal offense to which the materials relate." 42 U.S.C.A. § 2000aa(a)(1), (b)(1). Plainly, Congress had no desire to inhibit law enforcement investigators that need to search the premises of a suspected wrongdoer.

(b) The problem of commingling of protected documents and evidence

Because Congress enacted this statute before the widespread proliferation of computers, it could not fully consider the problem raised by the commingling of protected information and contraband. Although commingling can, of course, occur with paper records — for example, if a reporter engaging in tax fraud placed a copy of the fraudulent tax return in a filing cabinet with his or her work-related notes — such commingling never presented a significant problem for two reasons. First, the statute applied only to members of the traditional media, a limited group not usually associated with committing crimes. Second, when searching for paper records, investigators can generally examine records on site and then seize only those records that are the subject of their warrant. Thus, investigators can avoid violating the PPA by not "searching for" or "seizing" any protected material since they do not need to carry away anything but the object of their search.¹¹

¹¹ Of course, investigators may briefly isolate or possess protected material during the execution of the warrant, but such possession occurs during the execution of every search warrant and does not constitute a seizure.

With the widespread use of computers and the Internet, however, both of these limiting factors have disappeared. First, every computer user has become a potential publisher. For example, a single computer can provide (1) an electronic "bulletin board" for the posting of news items by individuals using the Internet; (2) user accounts where private individuals can store drafts of news items that they intend to post on the "bulletin board"; and (3) a website from which anyone with access to the Internet could view or download child pornography. Although the second category of data arguably constitutes "work product" under the PPA,¹² law enforcement officials plainly have the duty to search for and seize the third category of data.

Second, potential liability under the PPA may arise for law enforcement officials in such a scenario because it has become both unreasonable and impractical, and in some instances technically impossible to search for and seize the contraband without simultaneously seizing protected material. In the new electronic environment, where computer systems with gigabytes of storage have become ubiquitous, law enforcement agents generally cannot extract legally seizable evidence from commingled protected material without actually seizing, at least temporarily, those protected materials, or, perhaps more intrusively, without moving into and occupying the search premises for extended durations. Because of the volume of data to be searched or because of technical concerns (e.g. encryption), law enforcement agents must very often remove the seized computer or an exact

¹² No court has yet held that an electronic message, posted for viewing by the general public by way of a Bulletin Board System or the Internet, constitutes a "similar form of public communication" to newspapers, books, and broadcasts under the PPA. Although the instant amendments to the PPA do not opine on this subject, a court might make this ruling if presented with the right facts.

copy of all the data to a laboratory for analysis.

Moreover, liability may attach in such cases because the prohibition on searching for or seizing materials is stated in the disjunctive: violations may lie *either* for searching for *or* seizing such materials. Thus even a temporary seizure or examination may result in liability, despite the fact that such a PPA violation lies far outside the scope of the issues raised by the Zurcher decision. Zurcher involved a search of a newspaper office, and the warrant was drawn to intentionally seize photographs that had been made in contemplation of publication. The PPA, designed to address the Zurcher decision, accordingly should deter law enforcement from intentionally *searching for* evidentiary materials in the possession of innocent third parties engaged in information dissemination. But making unlawful the reasonable but incidental seizure of PPA-protected materials pursuant to an otherwise lawful search or seizure carries no similar deterrent effect, and it contravenes the clearly stated intent of Congress to neither shield criminals nor unduly hinder law enforcement efforts.

(c) Problems faced by law enforcement

The potential — and unpredictable — liability inadvertently created by the PPA has inhibited the investigation and prosecution of crimes committed using computers. For example, individuals have used computers to distribute child pornography, copyrighted software, and stolen credit card numbers over ordinary phone lines and the Internet. Some of these individuals have attempted to use the PPA to shield their illegal activities by intentionally storing PPA-protected materials on the same storage devices that they use for their illegal activities. Indeed, law enforcement agents have

encountered individuals using computers for illegal activities that have posted the following message on their sign-on screens:

NOTICE TO LAW ENFORCEMENT AGENTS:

The owners and users of this system are exercising First Amendment Rights. . . . Some material on this system is in preparation for public dissemination and is "work product material" protected under the First Amendment Privacy Protection Act of 1980 Each and every person who has such "work product material" stored on this system is entitled to recover at least minimum damages of \$1000 *plus all legal expenses* While the agency you work for *might* pay your legal fees and judgments against you, why take chances?

The language "[s]ome material on this system" is extremely significant. It is seldom the case that a computer is used solely for illegal purposes such as the distribution of contraband. Were this the case, the computer and the evidence it contains could be seized without regard to the PPA, since contraband is specifically excluded from the definitions of work product and documentary materials. 42 U.S.C. § 2000aa-7(a) (defining "documentary materials"); 42 U.S.C. § 2000aa-7(b) (defining "work product materials"). In most cases, only certain portions of a website or electronic bulletin board will be set aside for illegal activities, while other portions are used for completely legal activities such as the legitimate distribution of information. As the quoted language makes clear, however, criminals are well aware that under the PPA, protected materials can be used to shield contraband from search and seizure. Congress, of course, never intended to shield contraband when it enacted the PPA.

Moreover, in addition to exposing law enforcement to unintended liability, the PPA, as it stands, creates unnecessary problems during the execution of warrants, problems that potentially

harm the health and safety of the public. In 1999, for example, Special Agents of the Federal Bureau of Investigation uncovered a system of computers used to provide child pornography to anyone with access to the Internet. These computers, however, also provided Internet accounts to third parties, many of whom did not know about the illegal activities of the computers' operators. These unrelated accounts may have contained material protected by the PPA. The investigators determined that it would be impossible to search the computers on site while at the same time allowing the computers to continue to operate. Thus, in an effort to reduce their potential liability under the PPA for seizing the third party accounts, the investigators decided to obtain a search warrant authorizing them only to *copy* the computers' stored data and allow the computers to continue to operate. This, of course, had the effect of allowing the child pornography to remain accessible to the public — and possibly even allowing the pornographers or their confederates to copy the images to an unknown computer — while computer experts reviewed the data to segregate the illegal files. Congress never intended to hamper law enforcement efforts in this way.

(d) The solution

While the PPA must be amended so that it does not shield child pornographers, copyright infringers, and other criminals, such amendments should not inhibit those activities that the PPA was designed to protect. Indeed, the importance of protecting the confidentiality of these sensitive materials remains as great today as it has ever been. Thus, the law should limit the intrusiveness of government searches but should not unnecessarily hinder law enforcement's efforts to enforce the criminal laws. The language of this bill achieves this delicate balance between important values.

The bill's new provisions, Title 42, United States Code, sections 2000aa(a)(3) and 2000aa(b)(5), make it clear that law enforcement agents may still search for or seize contraband, instrumentalities, and evidence not protected by the PPA, even if work product or documentary material may incidentally be examined or seized during a search. It is important to note, however, that where an innocent third party possesses the items sought, and if the items sought are commingled with work product or documentary materials, existing regulations already require investigators to avoid using a search warrant or subpoena where less intrusive means are appropriate. See, e.g., 28 C.F.R. 50.10 (requiring Justice Department officials to use all other means available to obtain information before issuing subpoena to member of the news media); 28 C.F.R. §59.4(a) and 28 C.F.R. §59.4(c)(1)(11) (in determining whether to use a warrant or subpoena to obtain documentary materials, an attorney for the government should consider whether there is a close relationship of friendship, loyalty, or sympathy between the possessor of the materials and a suspect). Thus, even though the PPA would not restrict such incidental seizures, the Committee believes that government agents will need to consider what method is proper for obtaining the evidence based upon the facts of the case at hand.

Although these amendments to the PPA address the problem of incidental searches or seizures, these changes do not in any way alter the statute's effect in cases like Zurcher. The law enforcement officials who searched The Stanford Daily — which was not involved in any criminal activity — sought the very documentary materials that the PPA now protects. These materials, therefore, were not “incidental” to the search, and they therefore would not meet the exception found in the new amendments. Thus, even under the new law, when law enforcement agents encounter a

situation like that in the Zurcher case, they will still have to use a subpoena as the original PPA directed.

But in other cases, where the search is “otherwise lawful” (i.e. the object of the search is something other than “work product” or “documentary” materials), these amendments to the PPA will ensure that investigators can carry out their duties, even when PPA-protected materials may be commingled with seizable ones. The amendments’ use of the term “incidental” clearly prohibits situations in which protected materials are the object of the search. The term “incidental,” which appears in other statutes (see, e.g., 18 U.S.C. §2510(17)), means something which is “occurring or likely to occur at the same time or as a consequence.”¹³ Accordingly, in order to be “incidental” within the intent of this provision, any search or seizure of protected materials would have to be a concomitant consequence of a search for materials not protected by the PPA.¹⁴

Additionally, of course, the link between the incidental items and the lawful object of the search or seizure must be reasonable on the facts of the case. This requirement that such a search be reasonable is directly analogous to the Fourth Amendment requirement of reasonableness both in the scope of a search warrant and in its execution. See O'Connor v. Ortega, 480 U.S. 709, 726 (1987); United States v. Henson, 848 F.2d 1374 (6th Cir. 1988); United States v. Tamura, 694 F.2d 591 (9th Cir. 1982). Cases that have nothing to do with the PPA have caused courts to wrestle with

¹³ The American Heritage Dictionary, Second College Edition (1989).

¹⁴ This provision does not, of course, require that the incidental seizure of protected materials be inadvertent; law enforcement officers may knowingly seize protected materials where such seizure is incidental to a lawful search.

whether, under all the facts and circumstances, seizing certain incidental materials was sufficiently reasonable to meet the Fourth Amendment standard. Thus, the amendments do not, by any means, invite law enforcement to use "an otherwise lawful" search as a pretext for an unreasonable rummaging of other documents — whether protected by the PPA or not. On the contrary, this new exception to the PPA will allow courts to apply existing and well-established Fourth Amendment jurisprudence in analyzing the analogous question of whether any incidental search or seizure of PPA-protected materials has been reasonable under the circumstances.

(9) AMENDMENTS TO THE CABLE COMMUNICATIONS POLICY ACT

The Cable Communications Policy Act currently establishes two different sets of rules regarding privacy protection and disclosure to law enforcement: one governing cable service ("Cable Act") (47 U.S.C. §551), and the other applying to the use of telephone service and Internet access, (the wiretap statute (18 U.S.C. §2510 et seq.), the Electronic Communications Policy Act ("ECPA") (18 U.S.C. §2701 et seq.), and the pen register and trap and trace statute (18 U.S.C. §3121 et seq.). Yet today, unlike in 1984 when Congress passed the Cable Communications Policy Act, many cable companies offer not only traditional cable programming services but also Internet access and telephone service. The rules governing law enforcement access to the records of communication service providers' customers, however, should not depend on whether the customer has chosen to use a cable company or a more traditional type of provider for his telephone or Internet service. Congress believes that cable companies offering such services should comply with court orders and

April 24, 2000

other legal process permitted under the wiretap statute, ECPA, and the pen register and trap and trace statute with respect to their telephone and Internet customers.

In recent years, however, cable companies have increasingly balked at complying with such process, noting the seeming inconsistency of these statutes with their duty of nondisclosure (except under stringent limits) under the Cable Communications Policy Act. See In re Application of United States, 36 F. Supp. 2d __ (D. Mass. Feb. 9, 1999) (noting apparent statutory conflict and ultimately granting application for order under 18 U.S.C. 2703(d) against cable company providing Internet service). These complications have at times delayed or frustrated investigations.

In addition, section 551 is flawed because it permits law enforcement to obtain information only when that information constitutes evidence of an offense. In some cases, however, the information sought from a service provider is not evidence of a crime, even though it helps to solve one. For example, law enforcement officials may try to arrest a fugitive who is accessing his e-mail account from a remote location, and they need to obtain information from the cable company that shows from what location he is accessing that account. Moreover, whether law enforcement can obtain a court order to obtain such information should not depend on whether the fugitive has chosen to connect to the Internet using a cable company instead of a traditional Internet service provider.

Accordingly, the amendment inserts a new subsection 551(c)(2)(D) to confirm that cable companies, like other providers, remain subject to ECPA, the wiretap statute, and the trap and trace statute with respect to the provision of telephone and Internet services, notwithstanding section 551. However, the amendment preserves the Cable Act's primacy with respect to records revealing what

ordinary cable television programming a customer chooses to purchase, such as particular premium channels or "pay per view" shows. Thus, in a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a government entity can compel disclosure under ECPA only those customer records relating to Internet service.

(10) AMENDMENTS TO THE BAKER ACT

20 U.S.C. §1232g (the "Baker Act") prohibits educational institutions that receive federal funding from releasing certain types of information about their students. The Baker Act accommodates the legitimate needs of law enforcement, however, by allowing such institutions to release records in response to a grand jury subpoena. See 20 U.S.C. §1232g(b)(1)(J). Yet the Baker Act fails to take into account the fact that ECPA grants courts the authority to order holders of electronic information -- including educational institutions -- to release such information to law enforcement. See 18 U.S.C. §2703(d). In order to obtain such an order, however, the law enforcement authority must offer "specific and articulable facts" to justify its need for the records -- a much higher level of justification than that required to obtain a grand jury subpoena. The amendments to the Baker Act rectify this anomaly by allowing educational institutions to release records in response to a section 2703(d) court order.

(11) AMENDMENTS TO 18 U.S.C. §1029

An amendment to 18 U.S.C. §1029 amends the definition of "device-making equipment" by

adding the term “process.” The current text of subsection 1029(e)(6) defines “device-making equipment” as “any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device.” The legislative history accompanying the enactment of this subsection in 1984 could be read to indicate that Congress intended this definition to refer primarily to pieces of physical equipment, such as credit-card encoders and embossers, that criminals use to make counterfeit credit cards.

In recent years, however, law enforcement authorities and the credit card industry have detected the increasing availability on the Internet of software programs that generate valid credit card numbers. These programs, when possessed and run by any person other than authorized representatives of credit-card issuers, have only one purpose: to generate credit-card numbers that can be used for fraudulent transactions over the Internet, with a telephone, or through the mail. Inclusion of the term “process” in the definition of subsection (e)(6) clarifies that subsection 1029(a)(4) applies equally to the production of, trafficking in, control or custody of, or possession of credit-card generation software – as well as any other process or computer program for generating access devices or counterfeit access devices – with the intent to defraud.

V. REGULATORY IMPACT STATEMENT

(10)

VI. COST ESTIMATE

VII. CHANGES IN EXISTING LAW

(3) Section ____ — *Law enforcement assistance to providers of electronic communication services to monitor computer trespassers*

When a computer hacker breaks into a computer belonging to someone else, he threatens the privacy, integrity, and security of the data stored on that computer. Such computer trespassers have no reasonable expectation that the commands sent to that computer will remain private. The wiretap statute, however, only partially recognizes this common-sense fact. Under the current provisions of section 2511(2)(a), victims of computer hacking may monitor electronic communications by trespassers on their computer systems to protect their rights and property. As written, however, section 2511(2)(a) may not allow such a victim to request the assistance of law enforcement in conducting the monitoring of trespassers, even though a trespasser has absolutely no expectation that his communications with the computer that he has broken into will remain private.

This outcome is plainly incorrect. The current subsection forbids victims from taking natural and reasonable steps in their own defense that would be entirely legal in the physical world. For example, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary happen to fall within the definition of a “wire or electronic communication” according to the wiretap statute.

The crux of this problem arises out of the statute’s treatment of trespassers on the victim’s computer system. Congress intended to create extensive protections for ordinary, legitimate communications. It never intended that these same protections would apply to communications sent by a computer trespasser whose purpose is to break into computers and

endanger the privacy and property of others. Just as a physical-world burglar cannot complain if the police monitor his unauthorized use of a victim's home, so the cyber-world trespasser has no reasonable expectation that his actions inside the victim's computer system will remain private. Yet the wiretap statute makes no distinction between the commands and communications sent by authorized users and those of trespassers.

When Congress enacted the wiretap statute in 1968, it tailored government surveillance of oral and wire communications to the constitutional mandates announced by the Supreme Court in Katz v. United States, 389 U.S. 347 (1967) and Berger v. New York, 388 U.S. 41 (1967). In the case of oral communications, it incorporated the Fourth Amendment reasonable expectation of privacy test articulated in Katz directly into the definition of "oral communication." See 18 U.S.C. §2510(2). Apparently because Berger suggested that any use of a telephone system would support a reasonable expectation of privacy, however, Congress did not include in the statute the requirement that the actor have a reasonable expectation of privacy. When Congress added protections against the interception of "electronic communications" in 1986, it followed this example by omitting reference to a reasonable expectation of privacy. See 18 U.S.C. § 2510(1) (definition of wire communication), 18 U.S.C. § 2510(12) (definition of electronic communication).

At that time, this approach was adequate because individuals almost always possessed a reasonable expectation of privacy in their wire and electronic communications. Although a divergence between the scope of constitutional and statutory protections existed in theory, it did not appear likely to arise in fact. See S.Rep. No. 1097, 90th Cong., 2d Sess., 96 (1968), U.S.Code Cong. & Admin. News 1968, p. 2185 (noting that Title III's provision of a statutory

suppression remedy to "any party" to an intercepted wire communication was not intended "generally to press the scope of the suppression role beyond present search and seizure law.").

Increasing reliance on computer networks has exposed the flaw with this approach in the last decade, however. As presently written, the wiretap statute does not distinguish between the interception of authorized telephone and e-mail communications on one hand, and the interception of unauthorized commands sent by computer trespassers who have violated others' privacy or who have begun to destroy or manipulate data on the other. The wiretap statute treats both sets of communications as wire and/or electronic communications, and 18 U.S.C. §2511 prohibits the interception of either absent a court order or an explicit exception. However, the two cases raise different privacy concerns: authorized users enjoy a reasonable expectation of privacy in their wire and electronic communications, whereas electronic trespassers do not. See Rakas v. Illinois, 439 U.S. 128, 143 n. 12 (1978).

As a result, the statute has created the absurd result that these illicit communications enjoy the strong statutory protections. Reasonable efforts to monitor trespassers – who have no expectation that their activities are private – can themselves result in felony violations of section 2511, as well as suppression of the intercepted communications under section 2515. See United States v. Seidlitz, 589 F.2d 152, 159 (4th Cir. 1978) (noting "a certain speciousness" in a computer hacker's challenge to a victim's surveillance of the hacker's attacks, because "[u]nlike the typical telephone user who employs the telephone merely as a convenience to converse with other persons over distances, [the hacker] used the telephone to tamper with and manipulate a machine which was owned by others, located on their premises, and obviously not intended for his use").

Moreover, by failing to differentiate between the reasonable expectation of privacy of

authorized users and the lack of such expectation by computer intruders, the statute has hampered important investigations. In one case, for example, the Justice Department had to deny victim requests to monitor intrusions in a major cyberterrorism investigation that implicated the national security of the United States. See generally Gregory Vistica, *"We're in the Middle of a Cyberwar": Russian Hackers May Have Pulled Off What Could Be the Most Damaging Breach Ever of U.S. Computer Security*, NEWSWEEK, Sept. 20, 1999, at 52; *Dangerous Doings in Cyberspace*, LOS ANGELES TIMES, Nov. 3, 1999, at B 10. Moreover, although section 2511(2)(a) currently authorizes computer system owners to monitor unauthorized users in self-defense, such owners often lack the expertise, equipment, or financial resources required to monitor these attacks properly.

To correct this problem the amendments to the wiretap statute allow victims of computer attacks to authorize law enforcement officers to monitor trespassers on their computer systems in a narrow class of cases. Before monitoring can occur, four requirements must be met. First, an amendment to section 2510(20) provides a definition of "computer trespasser" that includes only the unauthorized users of a protected computer. Moreover, section 2511(2)(a)(iii)(D) requires that investigators only intercept the communications of trespassers. If the configuration of the computer system and the technology employed to intercept the communications do not allow interception of only the trespassers' electronic communications, then the authority under this subsection will not be employed. Thus, the amendment does create any additional authority to intercept the communications of authorized users.

Second, section 2511(2)(a)(iii)(B) requires that the person who intercepts the communication must be lawfully engaged in an ongoing investigation. This requirement makes clear that the investigation must have a lawful purpose, and that the authority to intercept ceases

at the conclusion of the investigation. Third, section 2511(2)(a)(iii)(C) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation.

Finally, section 2511(2)(a)(iii)(A) requires that before monitoring may occur, the owner or operator of the protected computer must expressly authorize the interception of the trespasser's communications. Such authorization should be explicit and specific, rather than the implied consent that is generally sufficient under section 2511(2)(c).