SUPPLEMENTAL MATERIALS:

UNITED STATES CODE

Vol. Nine
Title 18 - Crimes and Criminal Procedure
Title 19 - Customs Duties

Stetson University College of Law:

WORKSHOP: "VIRTUAL LEGALITY" Campus Electronic Communications Law and Policy
Clearwater Beach, Florida
February 16, 1997

UNITED STATES CODE

1994 EDITION

CONTAINING THE GENERAL AND PERMANENT LAWS
OF THE UNITED STATES, IN FORCE
ON JANUARY 4, 1995

Prepared and published under authority of Title 2, U.S. Code, Section 285b,
by the Office of the Law Revision Counsel of the House of Representatives

VOLUME NINE

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

AND

TITLE 19—CUSTOMS DUTIES

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1995

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains 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 the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

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

(3) intentionally, without authorization to access any 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 adversely affects the use of the Government's operation of such computer;

(4) knowingly and with intent to defraud, accesses a Federal interest 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;

(5)(A) through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if—

(i) the person causing the transmission intends that such transmission will—

(I) damage, or cause damage to, a computer, computer system, network, information, data, or program; or

(II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program; and

(ii) the transmission of the harmful component of the program, information, code, or command—

(I) occurred without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

(II)(aa) causes loss or damage to one or more other persons of value aggregating $1,000 or more during any 1-year period; or

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

(B) through means of a computer used in interstate commerce or communication, knowingly causes the transmission of a program, information, code, or command to a computer or computer system—

(i) with reckless disregard of a substantial and unjustifiable risk that the transmission will—

(I) damage, or cause damage to, a computer, computer system, network, information, data or program; or

(II) withhold or deny or cause the withholding or denial of the use of a computer, computer services, system, network, information, data or program; and

(ii) if the transmission of the harmful component of the program, information, code, or command—

(I) occurred without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

(II)(aa) causes loss or damage to one or more other persons of a value aggregating $1,000 or more during any 1-year period; or

(bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; [1]

(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;

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

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(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 such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and [2]

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

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

(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) or (a)(5)(A) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

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

(4) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B).

(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 "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 "Federal interest 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 the use of the financial institution's operation or the Government's operation of such computer; or

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

(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 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;

[1] So in original. Probably should be followed by "or".

[2] So in original. The word "and" probably should not appear.

(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) [3] of the Federal Reserve Act.[4]

(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; and

(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.

(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) Any person who suffers damage or loss by reason of a violation of the [5] section, other than a violation of subsection (a)(5)(B), may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb) 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 section 1030(a)(5) of title 18, United States Code.

(Added Pub. L. 98-473, title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190; amended Pub. L. 99-474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub. L. 100-690, title VII, § 7065, Nov. 18, 1988, 102 Stat. 4404; Pub. L. 101-73, title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub. L. 101-647, title XII, § 1205(e), title XXV, § 2597(j), title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub. L. 103-322, title XXIX, § 290001(b)-(f), Sept. 13, 1994, 108 Stat. 2097-2099.)

REFERENCES IN TEXT

Section 11 of the Atomic Energy Act of 1954, referred to in subsec. (a)(1), is classified to section 2014 of Title 42, The Public Health and Welfare.

The Fair Credit Reporting Act, referred to in subsec. (a)(2), is title VI of Pub. L. 90-321, as added by Pub. L. 91-508, title VI, § 601, Oct. 26, 1970, 84 Stat. 1127, as amended, which is classified generally to subchapter III (§ 1681 et seq.) of chapter 41 of Title 15, Commerce and Trade. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of Title 15 and Tables.

The Farm Credit Act of 1971, referred to in subsec. (e)(4)(E), is Pub. L. 92-181, Dec. 10, 1971, 85 Stat. 583, as amended, which is classified generally to chapter 23 (§ 2001 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 2001 of Title 12 and Tables.

Section 15 of the Securities Exchange Act of 1934, referred to in subsec. (e)(4)(F), is classified to section 78o of Title 15, Commerce and Trade.

Section 1(b) of the International Banking Act of 1978, referred to in subsec. (e)(4)(H), is classified to section 3101 of Title 12, Banks and Banking.

Section 25 of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter I (§ 601 et seq.) of chapter 6 of Title 12. Section 25(a) of the Federal Reserve Act, which is classified to subchapter II (§ 611 et seq.) of chapter 6 of Title 12, was renumbered section 25A of that act by Pub. L. 102-242, title I, § 142(e)(2), Dec. 19, 1991, 105 Stat. 2281.

The date of the enactment of this subsection, referred to in subsec. (h), is the date of enactment of Pub. L. 103-322, which was approved Sept. 13, 1994.

AMENDMENTS

1994—Subsec. (a)(3). Pub. L. 103-322, § 290001(f), inserted "adversely" before "affects the use of the Government's".

Subsec. (a)(5). Pub. L. 103-322, § 290001(b), amended par. (5) generally. Prior to amendment, par. (5) read as follows: "intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

"(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

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

Subsec. (c)(3)(A). Pub. L. 103-322, § 290001(c)(2), inserted "(A)" after "(a)(5)".

Subsec. (c)(4). Pub. L. 103-322, § 290001(c)(1), (3), (4), added par. (4).

Subsec. (g). Pub. L. 103-322, § 290001(d), added subsec. (g).

Subsec. (h). Pub. L. 103-322, § 290001(e), added subsec. (h).

1990—Subsec. (a)(1). Pub. L. 101-647, § 3533, substituted "paragraph y" for "paragraph r".

Subsec. (e)(3). Pub. L. 101-647, § 1205(e), inserted "commonwealth," before "possession or territory of the United States".

Subsec. (e)(4)(G). Pub. L. 101-647, § 2597(j)(2), which directed substitution of a semicolon for a period at end of subpar. (G), could not be executed because it ended with a semicolon.

Subsec. (e)(4)(H), (I). Pub. L. 101-647, § 2597(j), added subpars. (H) and (I).

1989—Subsec. (e)(4)(A). Pub. L. 101-73, § 962(a)(5)(A), substituted "an institution," for "a bank".

Subsec. (e)(4)(C) to (H). Pub. L. 101-73, § 962(a)(5)(B), (C), redesignated subpars. (D) to (H) as (C) to (G), respectively, and struck out former subpar. (C) which read as follows: "an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;".

1988—Subsec. (a)(2). Pub. L. 100-690 inserted a comma after "financial institution" and struck out the comma that followed a comma after "title 15".

[3] See References in Text note below.

[4] So in original. The period probably should be a semicolon.

[5] So in original. Probably should be "this".

1986—Subsec. (a). Pub. L. 99-474, § 2(b)(2), struck out last sentence which read as follows: "It is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer."

Subsec. (a)(1). Pub. L. 99-474, § 2(c), substituted "or exceeds authorized access" for ", or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend".

Subsec. (a)(2). Pub. L. 99-474, § 2(a), (c), substituted "intentionally" for "knowingly", substituted "or exceeds authorized access" for ", or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend", struck out "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)," after "financial institution,", inserted "or of a card issuer as defined in section 1602(n) of title 15," and struck out "or" appearing at end.

Subsec. (a)(3). Pub. L. 99-474, § 2(b)(1), amended par. (3) generally. Prior to amendment, par. (3) read as follows: "knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;".

Subsec. (a)(4) to (6). Pub. L. 99-474, § 2(d), added pars. (4) to (6).

Subsec. (b). Pub. L. 99-474, § 2(e), struck out par. (1) designation and par. (2) which provided a penalty for persons conspiring to commit an offense under subsec. (a).

Subsec. (c). Pub. L. 99-474, § 2(f)(9), substituted "(b)" for "(b)(1)" in introductory text.

Subsec. (c)(1)(A). Pub. L. 99-474, § 2(f)(1), substituted "under this title" for "of not more than the greater of $10,000 or twice the value obtained by the offense".

Subsec. (c)(1)(B). Pub. L. 99-474, § 2(f)(2), substituted "under this title" for "of not more than the greater of $100,000 or twice the value obtained by the offense".

Subsec. (c)(2)(A). Pub. L. 99-474, § 2(f)(3), (4), substituted "under this title" for "of not more than the greater of $5,000 or twice the value obtained or loss created by the offense" and inserted reference to subsec. (a)(6).

Subsec. (c)(2)(B). Pub. L. 99-474, § 2(f)(3), (5)-(7), substituted "under this title" for "of not more than the greater of $10,000 or twice the value obtained or loss created by the offense", "not more than" for "not than", inserted reference to subsec. (a)(6), and substituted "; and" for the period at end of subpar. (B).

Subsec. (c)(3). Pub. L. 99-474, § 2(f)(8), added par. (3).

Subsec. (e). Pub. L. 99-474, § 2(g), substituted a dash for the comma after "As used in this section", realigned remaining portion of subsection, inserted "(1)" before "the term", substituted a semicolon for the period at the end, and added pars. (2) to (7).

Subsec. (f). Pub. L. 99-474, § 2(h), added subsec. (f).

REPORTS TO CONGRESS

Section 2103 of Pub. L. 98-473 directed Attorney General to report to Congress annually, during first three years following Oct. 12, 1984, concerning prosecutions under this section.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 981, 982, 2256, 3239 of this title; title 31 section 9703.

ELECTRONIC PRIVACY INFORMATION CENTER

NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1996

H.R.3723

One Hundred Fourth Congress

of the

United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Wednesday,

the third day of January, one thousand nine hundred and ninety-six

An Act

To amend title 18, United States Code, to protect proprietary

economic information, and for other purposes.

[Italic->] Be it enacted by the Senate and House of

Representatives of the United States of America in Congress

assembled, [<-Italic]

TITLE II--NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1996.

```
SEC. 201. COMPUTER CRIME.
  Section 1030 of title 18, United States Code, is amended--
      (1) in subsection (a)--
           (A) in paragraph (1)--
               (i) by striking `knowingly accesses' and inserting
             `having knowingly accessed';
               (ii) by striking `exceeds' and inserting `exceeding';
               (iii) by striking `obtains information' and inserting
             `having obtained information';
```

`having obtained information';
(iv) by striking `the intent or';
(v) by striking `is to be used' and inserting `could be used'; and
(vi) by inserting before the semicolon at the end the following: `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';
(B) in paragraph (2)--
(i) by striking `obtains information' and inserting `obtains--
`(A) information'; and
(ii) by adding at the end the following new subparagraphs:
`(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;';
(C) in paragraph (3)--
(i) by inserting `nonpublic' before `computer of a department or agency';
(ii) by striking `adversely'; and
(iii) by striking `the use of the Government's operation of such computer' and inserting `that use by or for the Government of the United States';
(D) in paragraph (4)--
(i) by striking `Federal interest' and inserting `protected'; and
(ii) by inserting before the semicolon the following: `and the value of such use is not more than $5,000 in any 1-year period';
(E) by striking paragraph (5) and inserting the following:
`(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;'; and
(F) by inserting after paragraph (6) the following new paragraph:
`(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;';
(2) in subsection (c)--
(A) in paragraph (1), by striking `such subsection' each place that term appears and inserting `this section';
(B) in paragraph (2)--
(i) in subparagraph (A)--
(I) by inserting `, (a)(5)(C),' after `(a)(3)'; and
(II) by striking `such subsection' and inserting `this section';
(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting immediately after subparagraph (A) the following:

`(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--

`(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

(iv) in subparagraph (C) (as redesignated)--

(I) by striking `such subsection' and inserting `this section'; and

(II) by adding `and' at the end;

(C) in paragraph (3)--

(i) in subparagraph (A)--

(I) by striking `(a)(4) or (a)(5)(A)' and inserting `(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)'; and

(II) by striking `such subsection' and inserting `this section'; and

(ii) in subparagraph (B)--

(I) by striking `(a)(4) or (a)(5)' and inserting `(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)'; and

(II) by striking `such subsection' and inserting `this section'; and

(D) by striking paragraph (4);

(3) in subsection (d), by inserting `subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of' before `this section.';

(4) in subsection (e)--

(A) in paragraph (2)--

(i) by striking `Federal interest' and inserting `protected';

(ii) in subparagraph (A), by striking `the use of the financial institution's operation or the Government's operation of such computer' and inserting `that use by or for the financial institution or the Government'; and

(iii) by striking subparagraph (B) and inserting the following:

`(B) which is used in interstate or foreign commerce or communication;';

(B) in paragraph (6), by striking `and' at the end;

(C) in paragraph (7), by striking the period at the end and inserting `; and'; and

(D) by adding at the end the following new paragraphs:

`(8) the term `damage' means any impairment to the integrity or availability of data, a program, a system, or information, that--

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

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

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

`(D) threatens public health or safety; and

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

(5) in subsection (g)--

(A) by striking `, other than a violation of subsection (a)(5)(B),'; and

(B) by striking `of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)' and inserting `involving damage as defined in subsection (e)(8)(A)'.

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

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

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or 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 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.

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

AMENDMENTS

1988—Pub. L. 100-690, title VII, § 7067, Nov. 18, 1988, 102 Stat. 4405, which directed amendment of item 2710 by inserting "for chapter" after "Definitions" was executed by making the insertion in item 2711 to reflect the probable intent of Congress and the intervening redesignation of item 2710 as 2711 by Pub. L. 100-618, see below.

Pub. L. 100-618, § 2(b), Nov. 5, 1988, 102 Stat. 3197, added item 2710 and redesignated former item 2710 as 2711.

CHAPTER REFERRED TO IN OTHER SECTIONS

This chapter is referred to in section 2511 of this title.

§ 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 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 commercial advantage, malicious destruction or damage, or private commercial gain—

(A) a fine of [1] under this title or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

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

(2) a fine of [1] under this title or imprisonment for not more than six months, or both, in any other case.

(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 communications service;

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

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

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1860; amended Pub. L. 103-322, title XXXIII, § 330016(1)(K), (U), Sept. 13, 1994, 108 Stat. 2147, 2148.)

AMENDMENTS

1994—Subsec. (b)(1)(A). Pub. L. 103-322, § 330016(1)(U), substituted "under this title" for "not more than $250,000".

Subsec. (b)(2). Pub. L. 103-322, § 330016(1)(K), substituted "under this title" for "not more than $5,000".

EFFECTIVE DATE

Section 202 of title II of Pub. L. 99-508 provided that: "This title and the amendments made by this title [enacting this chapter] shall take effect ninety days after the date of the enactment of this Act [Oct. 21, 1986] and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect."

SHORT TITLE OF 1988 AMENDMENT

Pub. L. 100-618, § 1, Nov. 5, 1988, 102 Stat. 3195, provided that: "This Act [enacting section 2710 of this title and renumbering former section 2710 as 2711 of this title] may be cited as the 'Video Privacy Protection Act of 1988'."

§ 2702. Disclosure of contents

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

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

(2) a person or entity providing 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.

(b) EXCEPTIONS.—A person or entity 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

(6) to a law enforcement agency, if such contents—

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

(B) appear to pertain to the commission of a crime.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1860; amended Pub. L. 100-690, title VII, § 7037, Nov. 18, 1988, 102 Stat. 4399.)

AMENDMENTS

1988—Subsec. (b)(2). Pub. L. 100-690 substituted "2517" for "2516".

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in section 2706 of this title.

§ 2703. Requirements for governmental access

(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity

[1] So in original. The word "of" probably should not appear.

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

(b) CONTENTS OF 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 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.

(2) Paragraph (1) is applicable with respect to any 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 provider of electronic communication service or remote computing service may 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) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;

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

(iii) has the consent of the subscriber or customer to such disclosure.

(C) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the name, address, telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under subparagraph (B).

(2) A governmental entity receiving 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) may be issued by any court that is a court of competent jurisdiction described in section 3126(2)(A) [1] 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. 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.

(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.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1861; amended Pub. L. 100-690, title VII, §§ 7038, 7039, Nov. 18, 1988, 102 Stat. 4399; Pub. L. 103-322, title XXXIII, § 330003(b), Sept. 13, 1994, 108 Stat. 2140; Pub. L. 103-414, title II, § 207(a), Oct. 25, 1994, 108 Stat. 4292.)

[1] See References in Text note below.

REFERENCES IN TEXT

The Federal Rules of Criminal Procedure, referred to in subsecs. (a), (b)(1)(A), and (c)(1)(B)(i), are set out in the Appendix to this title.

Section 3126(2)(A), referred to in subsec. (d), was renumbered section 3127(2)(A) of this title by Pub. L. 100-690, title VII, § 7092(a)(1), Nov. 18, 1988, 102 Stat. 4410.

AMENDMENTS

1994—Subsec. (c)(1)(B). Pub. L. 103-414, § 207(a)(1)(A), redesignated cls. (ii) to (iv) as (i) to (iii), respectively, and struck out former cl. (i) which read as follows: "uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury or trial subpoena;".

Subsec. (c)(1)(C). Pub. L. 103-414, § 207(a)(1)(B), added subpar. (C).

Subsec. (d). Pub. L. 103-414, § 207(a)(2), amended first sentence generally. Prior to amendment, first sentence read as follows: "A court order for disclosure under subsection (b) or (c) of this section may be issued by any court that is a court of competent jurisdiction set forth in section 3127(2)(A) of this title and shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry."

Pub. L. 103-322 substituted "section 3127(2)(A)" for "section 3126(2)(A)".

1988—Subsecs. (b)(1)(B)(i), (c)(1)(B)(i). Pub. L. 100-690, § 7038, inserted "or trial" after "grand jury".

Subsec. (d). Pub. L. 100-690, § 7039, inserted "may be issued by any court that is a court of competent jurisdiction set forth in section 3126(2)(A) of this title and" before "shall issue".

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 2701, 2702, 2704, 2705, 2706, 2707 of this title.

§ 2704. Backup preservation

(a) BACKUP PRESERVATION.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of—

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider—

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) CUSTOMER CHALLENGES.—(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement—

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity

are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1863.)

REFERENCES IN TEXT

The Federal Rules of Civil Procedure, referred to in subsec. (b)(2), are set out in the Appendix to Title 28, Judiciary and Judicial Procedure.

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 2701, 2706 of this title.

§ 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 a Federal or State grand jury subpoena 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).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(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.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1864.)

SECTION REFERRED TO IN OTHER SECTIONS

This section is referred to in sections 2703, 2704 of this title.

§ 2706. Cost reimbursement

(a) PAYMENT.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) AMOUNT.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) EXCEPTION.—The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1866; amended Pub. L. 100-690, title VII, § 7061, Nov. 18, 1988, 102 Stat. 4404.)

AMENDMENTS

1988—Subsec. (c). Pub. L. 100-690 inserted heading.

§ 2707. Civil action

(a) CAUSE OF ACTION.—Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or customer 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.

(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 to 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 discovered or had a reasonable opportunity to discover the violation.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1866.)

§ 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.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1867.)

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) DUTY TO PROVIDE.—A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director, may—

(1) request the name, address, length of service, and toll billing records of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that—

(A) the name, address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that—

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with—

(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act [1] or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or

(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act [1] or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.

(c) PROHIBITION OF CERTAIN DISCLOSURE.—No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1867; amended Pub. L. 103-142, Nov. 17, 1993, 107 Stat. 1491.)

AMENDMENTS

1993—Subsec. (b). Pub. L. 103-142, § 1, amended subsec. (b) generally. Prior to amendment, subsec. (b) read as follows: "REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the wire or electronic communication service provider to which the request is made that—

"(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

"(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)."

Subsec. (e). Pub. L. 103-142, § 2, inserted ", and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate," after "Senate".

[1] So in original. Probably should be "Act of 1978".

§ 2710. Wrongful disclosure of video tape rental or sale records

(a) DEFINITIONS.—For purposes of this section—

(1) the term "consumer" means any renter, purchaser, or subscriber of goods or services from a video tape service provider;

(2) the term "ordinary course of business" means only debt collection activities, order fulfillment, request processing, and the transfer of ownership;

(3) the term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider; and

(4) the term "video tape service provider" means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

(b) VIDEO TAPE RENTAL AND SALE RECORDS.—(1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer—

(A) to the consumer;

(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;

(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;

(D) to any person if the disclosure is solely of the names and addresses of consumers and if—

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and

(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for

the exclusive use of marketing goods and services directly to the consumer;

(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or

(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if—

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government 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 video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) CIVIL ACTION.—(1) Any person aggrieved by any act of a person 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 in an amount of $2,500;

(B) punitive damages;

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

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) PERSONALLY IDENTIFIABLE INFORMATION.—Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, 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 of a State.

(e) DESTRUCTION OF OLD RECORDS.—A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date 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 (b)(2) or (c)(2) or pursuant to a court order.

(f) PREEMPTION.—The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section.

(Added Pub. L. 100-618, § 2(a)(2), Nov. 5, 1988, 102 Stat. 3195.)

REFERENCES IN TEXT

The Federal Rules of Criminal Procedure, referred to in subsec. (b)(2)(C), are set out in the Appendix to this title.

PRIOR PROVISIONS

A prior section 2710 was renumbered section 2711 of this title.

§ 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.

(Added Pub. L. 99-508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1868, § 2710; renumbered § 2711, Pub. L. 100-618, § 2(a)(1), Nov. 5, 1988, 102 Stat. 3195.)

AMENDMENTS

1988—Pub. L. 100-618 renumbered section 2710 of this title as this section.