105TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
105–425

WIRELESS PRIVACY ENHANCEMENT ACT OF 1998

MARCH 3, 1998.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BLILEY, from the Committee on Commerce, submitted the following

REPORT

[To accompany H.R. 2369]

[Including cost estimate of the Congressional Budget Office]

The Committee on Commerce, to whom was referred the bill (H.R. 2369) to amend the Communications Act of 1934 to strengthen and clarify prohibitions on electronic eavesdropping, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

AMENDMENT

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Wireless Privacy Enhancement Act of 1998".

SEC. 2. COMMERCE IN ELECTRONIC EAVESDROPPING DEVICES.

(a) PROHIBITION ON MODIFICATION.—Section 302(b) of the Communications Act of 1934 (47 U.S.C. 302a(b)) is amended by inserting before the period at the end thereof the following: ", or modify any such device, equipment, or system in any manner that causes such device, equipment, or system to fail to comply with such regulations".

(b) PROHIBITION ON COMMERCE IN SCANNING RECEIVERS.—Section 302(d) of such Act (47 U.S.C. 302a(d)) is amended to read as follows:

"(d) EQUIPMENT AUTHORIZATION REGULATIONS.—

"(1) PRIVACY PROTECTIONS REQUIRED.—The Commission shall prescribe regulations, and review and revise such regulations as necessary in response to subsequent changes in technology or behavior, denying equipment authorization (under part 15 of title 47, Code of Federal Regulations, or any other part of that title) for any scanning receiver that is capable of—

"(A) receiving transmissions in the frequencies that are allocated to the domestic cellular radio telecommunications service or the personal communications service;

"(B) readily being altered to receive transmissions in such frequencies;

"(C) being equipped with decoders that—

"(i) convert digital domestic cellular radio telecommunications service, personal communications service, or protected specialized mobile radio service transmissions to analog voice audio; or

"(ii) convert protected paging service transmissions to alphanumeric text; or

"(D) being equipped with devices that otherwise decode encrypted radio transmissions for the purposes of unauthorized interception.

"(2) PRIVACY PROTECTIONS FOR SHARED FREQUENCIES.—The Commission shall, with respect to scanning receivers capable of receiving transmissions in frequencies that are used by commercial mobile services and that are shared by public safety users, examine methods, and may prescribe such regulations as may be necessary, to enhance the privacy of users of such frequencies.

"(3) TAMPERING PREVENTION.—In prescribing regulations pursuant to paragraph (1), the Commission shall consider defining 'capable of readily being altered' to require scanning receivers to be manufactured in a manner that effectively precludes alteration of equipment features and functions as necessary to prevent commerce in devices that may be used unlawfully to intercept or divulge radio communication.

"(4) WARNING LABELS.—In prescribing regulations under paragraph (1), the Commission shall consider requiring labels on scanning receivers warning of the prohibitions in Federal law on intentionally intercepting or divulging radio communications.

"(5) DEFINITIONS.—As used in this subsection, the term 'protected' means secured by an electronic method that is not published or disclosed except to authorized users, as further defined by Commission regulation.".

(c) IMPLEMENTING REGULATIONS.—Within 90 days after the date of enactment of this Act, the Federal Communications Commission shall prescribe amendments to its regulations for the purposes of implementing the amendments made by this section.

SEC. 3. UNAUTHORIZED INTERCEPTION OR PUBLICATION OF COMMUNICATIONS.

Section 705 of the Communications Act of 1934 (47 U.S.C. 605) is amended—

(1) in the heading of such section, by inserting **"INTERCEPTION OR"** after **"UNAUTHORIZED"**;

(2) in the first sentence of subsection (a), by striking "Except as authorized by chapter 119, title 18, United States Code, no person" and inserting "No person";

(3) in the second sentence of subsection (a)—

(A) by inserting "intentionally" before "intercept"; and

(B) by striking "and divulge" and inserting "or divulge";

(4) by striking the last sentence of subsection (a) and inserting the following: "Nothing in this subsection prohibits an interception or disclosure of a communication as authorized by chapter 119 of title 18, United States Code.";

(5) in subsection (e)(1)—

(A) by striking "fined not more than $2,000 or"; and

(B) by inserting "or fined under title 18, United States Code," after "6 months,"; and

(6) in subsection (e)(3), by striking "any violation" and inserting "any receipt, interception, divulgence, publication, or utilization of any communication in violation";

(7) in subsection (e)(4), by striking "any other activity prohibited by subsection (a)" and inserting "any receipt, interception, divulgence, publication, or utilization of any communication in violation of subsection (a)"; and

(8) by adding at the end of subsection (e) the following new paragraph:

"(7) Notwithstanding any other investigative or enforcement activities of any other Federal agency, the Commission shall investigate alleged violations of this section and may proceed to initiate action under section 503 of this Act to impose forfeiture penalties with respect to such violation upon conclusion of the Commission's investigation.".

PURPOSE AND SUMMARY

The purpose of H.R. 2369, the Wireless Privacy Enhancement Act of 1998, as amended, is to enhance the privacy of users of cellular and other mobile communications services. These changes are necessary to prohibit modification of currently available scanners and to prevent the development of a market for new digital scanners capable of intercepting digital communications.

The bill has four main components. First, the bill would extend current scanning receiver manufacturing restrictions to prevent the manufacture of scanners that are capable of intercepting communications in frequencies allocated to new wireless communications, namely personal communications services, and protected paging and specialized mobile radio services. Second, the bill would add a prohibition on the modification of scanners and require the Federal Communications Commission (the Commission or FCC) to strengthen its rules to prevent the modification of scanning receivers, including through adopting additional requirements to prevent the tampering of scanning receivers. Third, the bill would make it unacceptable to intentionally intercept or divulge the content of radio communications. Lastly, the bill would improve the enforcement of privacy law by increasing the penalties available for violators and requiring the Commission to move expeditiously on investigations of potential violations.

BACKGROUND AND NEED FOR LEGISLATION

Over 50 million Americans subscribe to cellular or other commercial mobile services. The majority of cellular services used today are provided with analog technology. Analog communications are susceptible to unauthorized eavesdropping from scanners since voice, an analog form of communication, need not be decoded when intercepted over a scanner. The Committee discovered through a hearing on wireless privacy in February 1997 how easily over-the-shelf scanners may be modified to enable them to intercept cellular communications. Digital cellular, the next generation of cellular services, and digital personal communications services (PCS) are less susceptible to unauthorized eavesdropping than analog cellular. PCS services are digital services that combine voice services with data (paging, messaging, caller identification) and possibly video services, over the same handset. While digital cellular and

PCS are not immune from eavesdropping, they are currently more secure than analog cellular because the equipment for intercepting digital calls is vastly more expensive and complex than existing, off-the-shelf scanners that intercept analog communications (e.g., $200 vs. $10,000–$30,000). However, one of the purposes of the bill is to prevent a market for developing for less expensive digital scanners by clearly prohibiting the authorization of such scanners by the FCC.

Several existing statutes are intended to protect cellular users' privacy. Section 705(a) of the Communications Act of 1934 prohibits the unauthorized interception and divulgence of radio communications, including cellular calls. This statute is not limited by its terms to analog radio communications and, therefore, would apply to digital cellular and PCS, as well as to other commercial mobile radio services such as paging, specialized mobile services, messaging services, etc. FCC rules also prohibit the interception of private conversations by radio scanners, whether or not the content of such radio communications is divulged (47 C.F.R. 15.9).

Section 705(e)(4) of the Communications Act makes it illegal for a person to manufacture, assemble, modify, import, export, sell, or distribute equipment knowing or having reason to know that it is intended for the unauthorized interception and divulgence of radio communications. However, the FCC has only enforced this provision for satellite cable piracy.

In addition to these provisions of the Communications Act and FCC regulations, the Electronic Communications Protection Act, 18 U.S.C. 2511 et seq. (1986) (ECPA), also prohibits the unauthorized interception or disclosure of cellular and other radio communications. Under ECPA, the manufacture, assembly, possession, sale or use of scanning devices which are "primarily useful" for surreptitious interception and are sent through interstate mail are prohibited. ECPA is the principal statute used to prosecute unlawful interceptions. ECPA prohibits knowingly advertising interstate for any device "primarily useful" for the surreptitious interception of electronic communications. See Section 2512(1)(c).

While interception of cellular telephone calls is illegal, it is legal under existing statutes to intercept radio communications outside of the cellular bands as long as the communication is not divulged or does not "benefit" the interceptor. For example, people may intercept public safety communications on the latest emergency occurring in their vicinity. Typically, these communications can be intercepted by an off-the-shelf scanner. Prior to passage of the Telephone Disclosure and Dispute Resolution Act (TDDRA) (P.L. 102–556, 47 U.S.C. 302(a)), which codified existing section 302, over 22 brands of scanners were capable of intercepting the cellular bands. TDDRA, in part, was designed to decrease the manufacture and availability of scanning devices capable of intercepting cellular communications. Under TDDRA, manufacturers are prohibited from manufacturing scanners that can be "readily altered" to intercept cellular communications. FCC Rule 15.121 defines "readily altered." Specifically, existing section 302(b) of the Communications Act of 1934 prohibits the manufacture, import, or sale of scanning devices that are capable of intercepting cellular calls, or of being "readily altered" for such interception. In section 302(d), Congress

required the FCC to promulgate regulations denying authorization to scanners that are capable of receiving cellular transmissions. See 47 C.F.R. §§15.121 and 15.37(f). The Committee has found that current scanning receivers may not be manufactured in a manner to effectively prohibit interception of these frequencies and the current law may not be read to apply to new technologies.

HEARINGS

The Subcommittee on Telecommunications, Trade, and Consumer Protection held a hearing on cellular privacy on February 5, 1997. The Subcommittee received testimony from: Mr. Thomas E. Wheeler, President, Cellular Telecommunications Industry Association; Mr. Bob Grove, President, Grove Enterprises; Mr. Jay Kitchen, President and CEO, Personal Communications Industry Association; Mr. Gary Shapiro, President, Consumer Electronics Manufacturers Association; Mr. Jerry Berman, Executive Director, Center for Democracy and Technology; Mr. James K. Kallstrom, Assistant Director in Charge, New York Division, Federal Bureau of Investigation, accompanied by Mr. James Y. Blankner, Inspector/Deputy Assistant Director, Information Resources Division, Federal Bureau of Investigation; Mr. William E. Kennard, then-General Counsel, Federal Communications Commission, accompanied by Mr. Richard Smith, Chief, Office of Engineering and Technology, Federal Communications Commission; and Mr. Robert S. Litt, Deputy Assistant Attorney General, Criminal Division, Department of Justice. Prior to the witnesses' testimony, a technological demonstration was conducted to highlight the ease with which scanning equipment can be "readily altered" to intercept cellular communications.

COMMITTEE CONSIDERATION

On October 29, 1997, the Subcommittee on Telecommunications, Trade, and Consumer Protection met in open markup session and approved H.R. 2369 for Full Committee consideration, amended, by a voice vote.

The Full Committee met in open markup session on February 26, 1998, and ordered H.R. 2369 reported to the House, as amended, by a voice vote.

ROLLCALL VOTES

Clause 2(l)(2)(B) of rule XI of the Rules of the House requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto. There were no recorded votes taken in connection with ordering H.R. 2369 reported. A motion by Mr. Bliley to order H.R. 2369 reported to the House, as amended, was agreed to by a voice vote, a quorum being present.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 2(l)(3)(A) of rule XI of the Rules of the House of Representatives, the Committee held an oversight hearing and made findings that are reflected in this report.

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

Pursuant to clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives, no oversight findings have been submitted to the Committee by the Committee on Government Reform and Oversight.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 2(l)(3)(B) of rule XI of the Rules of the House of Representatives, the Committee finds that H.R. 2369, the Wireless Privacy Enhancement Act of 1998, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 2(l)(3)(C) of rule XI of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, March 2, 1998.

Hon. TOM BLILEY,
Chairman, Committee on Commerce,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2369, the Wireless Privacy Enhancement Act of 1998.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Kim Cawley (for federal costs), Alyssa Trzeszkowski (for revenues), and Jean Wooster (for private-sector mandates).

Sincerely,

JUNE E. O'NEILL, *Director.*

Enclosure.

H.R. 2369—Wireless Privacy Enhancement Act of 1998

CBO estimates that enacting this bill would have no significant effect on the federal budget. Because the bill would establish new criminal penalties and could affect receipts, pay-as-you-go procedures would apply. H.R. 2369 contains no intergovernmental mandates as defined in the Unfunded Mandates Reform Act of 1995 (UMRA), and would not affect the budgets of state, local, or tribal governments. H.R. 2369 would impose a new private-sector mandate, but CBO estimates the direct cost to industry of complying

with the bill would fall well below the statutory threshold for private-sector mandates.

H.R. 2369 would amend the Communications Act of 1934 to prohibit modifying any equipment used to communicate electronically in any manner that would not comply with regulations affecting electronic eavesdropping. The bill would direct the Federal Communications Commission (FCC) to prepare regulations to deny the authorization to use FCC equipment for certain scanning receivers that may be capable of unauthorized interception of communication transmissions. Based on information from the FCC, we estimate that these regulations would cost less than $500,000 to promulgate, assuming appropriation of the necessary amounts. Furthermore, under current law the FCC is authorized to collect fees from the telecommunications industry sufficient to offset the cost of its regulatory program. Therefore, CBO estimates the net budgetary effect of this provision would be negligible over time.

The bill also would amend the Communications Act of 1934 to impose criminal penalties for intercepting, publishing, or divulging a communication that is not authorized. CBO estimates that this provision would have a negligible effect on revenues. The bill would direct the FCC to investigate alleged violations of this portion of the act and to enforce this provision through forfeiture penalties. Under current law, any enforcement costs that the agency incurs are offset by fees charged to the industries that the FCC regulates. As a result, we estimate this provision would not result in any significant net cost to the federal government.

H.R. 2369 would impose a new private-sector mandate, as defined by UMRA, on manufacturers, importers, sellers, and those who modify scanning receivers. The bill would expand the FCC's criteria for authorizing equipment. Based on information provided by the leading manufacturer of scanning receivers and the FCC, CBO estimates that the direct cost of complying with H.R. 2369 would fall well below the statutory threshold for private-sector mandates ($100 million in 1996, adjusted annually for inflation).

The CBO staff contacts for this estimate are: Kim Cawley for federal costs, Alyssa Trzeszkowski for revenues, and Jean Wooster for private sector mandates. This estimate was approved by Paul N. Van de Water, Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 2(l)(4) of rule XI of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause

3, which grants Congress the power to regulate commerce with foreign nations, among the several States, and with the Indian tribes.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

SECTION 1. SHORT TITLE

Section 1 designates the short title of the bill as the "Wireless Privacy Enhancement Act of 1998."

SECTION 2. COMMERCE IN ELECTRONIC EAVESDROPPING DEVICES

Section 2(a) extends the prohibition in section 302(b) of the Communications Act of 1934 to "modifying" scanning devices. While the Committee believes that "modifying" is already covered by the prohibition against "manufacturing" noncomplying scanners, it has decided to make the manufacturing prohibition explicit to prevent any misreading of the statute. By this subsection, the Committee does not intend to prohibit amateurs from modifying linear amplifiers after purchase, as permitted by Commission rules, to allow the devices to operate in the amateur 12-meter and 10-meter bands. Nor does the Committee intend for Section 2(a) to prohibit amateurs from building or modifying one amplifier per year to enable this capability, as also permitted by Commission rules. Likewise, the Committee does not intend for Section 2 to be interpreted in a manner that would permit the Commission to take actions against an amateur operator who is operating within the terms of his or her license.

Nor does the Committee intend for Section 2(a) to be interpreted in a manner that would discourage manufacturers or dealers of amateur equipment from providing amateur licensees with information about permissible modifications of transceivers to enable them to transmit and receive on Military Affiliate Radio Service and the Civil Air Patrol, to the extent such transmission and reception is permissible under 18 U.S.C. 2511(g) or other statutes. The Committee expects that the new regulations required under Section 2 will preserve the ability of amateurs to modify transceivers for the legitimate purposes discussed above.

Section 2(b) makes amendments to section 302(d) of the Communications Act of 1934. Section 2(b) amends section 302(d)(1) to expand its scope to cover new communications technologies such as personal communications services (PCS) and protected specialized mobile radio and paging services. It also requires the Commission to deny equipment authorization to scanners that are capable of being equipped with certain decoders. By this language, the Committee does not intend to hamper the inclusion of consumer-friendly features on radio scanners such as external audio jacks. The Committee intends manufacturers to design scanners with ports that the manufacturer does not anticipate can be used: (1) to equip

the scanner with a decoder that can convert digital cellular, personal communications services, or protected specialized mobile radio services to analog voice audio; (2) to convert protected paging services to alphanumeric text; or (3) to otherwise decrypt radio transmissions for the purposes of unauthorized interception. Thus, after the enactment of the Wireless Privacy Enhancement Act, manufacturers will be under an obligation to design scanners with consumer-friendly features that the manufacturer does not anticipate can be used to equip such scanners with prohibited decoders.

The Committee notes that nothing in this bill is intended to impede the development and deployment of scanning receivers designed as an integral part of a licensed wireless communications station or wireless communications system, or designed as communications test equipment not available to the general public.

Section 2(b) amends and replaces section 302(d)(2) of the Communications Act of 1934 with a new provision providing the Commission with the authority to prescribe rules to enhance the privacy of users of frequencies shared by commercial services and the public safety community. Section 2(b) also adds a new section 302(d)(3) that requires that the Commission consider requiring that scanning receivers be manufactured in a manner that prevents any tampering or alteration by the user that would permit the device to be used unlawfully for interception or divulgence of radio communications. By this provision, the Committee intends that the order adopting the regulations reflect on the record a discussion of possible means for manufacturers to prevent tampering or alteration of scanners for such illegal use. New section 302(d)(4) requires the Commission to consider requiring scanning manufacturers to include warning labels on scanners notifying users of prohibited uses. The Committee, likewise, intends that the order adopting the regulations reflect on the record a discussion of the benefits of warning labels. New section 302(d)(5) adds a definition of "protected" to the statute to be used in conjunction with the amendments made by this bill to section 302(d)(1).

Section 2(b) recognizes that some frequencies available for commercial mobile services are shared with public safety and other private wireless users. Again, nothing in this legislation is intended to impede the development and deployment of scanning receivers designed as an integral part of a licensed wireless communications station or wireless communications system, or designed as communications test equipment not available to the general public.

Section 2(c) requires the Commission to revise its rules, within 90 days, to implement the changes made by section 2. For purposes of Section 2(b) and the implementing regulations required by section 2(c), the Committee expects that the Commission will provide an effective date to the regulations that will provide an adequate transition period for scanner manufacturers to comply, so that scanner manufacturers or distributors are able to sell their current inventory. The Committee, therefore, expects the Commission to reflect on the record of the rulemaking required by Section 2, as is its practice, a discussion of the manufacturers' normal product development and production cycles in determining effective dates for the relevant requirements within the regulations, while bearing in mind the overall purpose of the bill to increase the privacy of wire-

less users. The Committee expects the Commission to promulgate regulations under Section 2(d)(2) which ensure that any privacy enhancement measures resulting from such regulations do not interfere with or impede the otherwise normal and proper use of radio scanners for reception of public safety and other allowed frequencies under law.

SECTION 3. UNAUTHORIZED INTERCEPTION OR PUBLICATION OF COMMUNICATIONS

Section 3(a) makes amendments to section 705 of the Communications Act of 1934. Section 3(a)(1) alters the heading provided to section 705. Section 3(a)(2) strikes "except as authorized by chapter 119, title 18, United States Code" from the first sentence of section 705(a) of the Communications Act. This is later addressed by section 3(a)(4).

Section 3(a)(3) eliminates the requirement that a violation of section 705(a) requires both interception and divulgence. The bill separates this provision into intentional interception or divulgence and, thus, the intentional interception itself is illegal.

Section 3(a)(4) preserves the authorization of certain interceptions or disclosures provided in Chapter 119 of Title 18. That chapter governs wire and electronic communications interception and interception of oral communications. Section 2511 of that chapter provides a number of exceptions to the chapter's prohibitions on interception. The majority of these exceptions relate to government interception. However, section 2511(g) provides a number of broad exceptions for the interception by private parties of radio communications, including those that are transmitted: (a) over a system that is configured for ready access by the general public; (b) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (c) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system that is readily accessible to the general public; (d) by a station operating in the amateur, citizens band (CB); and (e) by any marine or aeronautical communications system.

Because the Committee preserved the Chapter 119 exceptions in its amendment of section 705(a) of the Communications Act, the Committee does not intend for the Commission or any other enforcement agency to investigate or fine parties for the interceptions authorized by Chapter 119. Therefore, the Committee does not intend for uses of scanning receivers and receiving radios such as short-wave radios, that are consistent with the section 2511(g) exceptions to be investigated or fined under section 705(a).

Section 3(a)(5) increases the penalties for violating section 705(a) to be consistent with those under ECPA, relating to the interception or divulgence prohibition. Currently, the fine for willful violation is $2,000, 6 months in jail, or both; under ECPA, the penalties can be increased based upon repeated violations. Section 3(a)(5), therefore, provides an additional penalty option.

Paragraphs (6) and (7) make appropriate changes to section 705(e)(3) and (4) to be consistent with the changes made by section 3(a)(3) of the bill.

Paragraph (8) adds a new section 705(e)(7) to the Communications Act that would require the FCC to investigate and take action, notwithstanding any other investigations by other agencies or departments, on possible violations of the Communications Act or Commission rules on wireless communications privacy. With regards to the responsibility for enforcement under this paragraph, the Committee does not intend to preclude the Department of Justice or the Federal Bureau of Investigation from initiating and conducting separate or parallel investigations of allegations of violations of Chapter 119 of Title 18 of the United States Code.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

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

COMMUNICATIONS ACT OF 1934

* * * * * * *

TITLE III—PROVISIONS RELATING TO RADIO

PART I—GENERAL PROVISIONS

* * * * * * *

SEC. 302. DEVICES WHICH INTERFERE WITH RADIO RECEPTION.

(a) * * *

(b) No person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply with regulations promulgated pursuant to this section*, or modify any such device, equipment, or system in any manner that causes such device, equipment, or system to fail to comply with such regulations*.

* * * * * * *

[(d)(1) Within 180 days after the date of enactment of this subsection, the Commission shall prescribe and make effective regulations denying equipment authorization (under part 15 of title 47, Code of Federal Regulations, or any other part of that title) for any scanning receiver that is capable of—

[(A) receiving transmissions in the frequencies allocated to the domestic cellular radio telecommunications service,

[(B) readily being altered by the user to receive transmissions in such frequencies, or

[(C) being equipped with decoders that convert digital cellular transmissions to analog voice audio.

[(2) Beginning 1 year after the effective date of the regulations adopted pursuant to paragraph (1), no receiver having the capabilities described in subparagraph (A), (B), or (C) of paragraph (1), as such capabilities are defined in such regulations, shall be manufac-

tured in the United States or imported for use in the United States.]

(d) EQUIPMENT AUTHORIZATION REGULATIONS.—

(1) PRIVACY PROTECTIONS REQUIRED.—The Commission shall prescribe regulations, and review and revise such regulations as necessary in response to subsequent changes in technology or behavior, denying equipment authorization (under part 15 of title 47, Code of Federal Regulations, or any other part of that title) for any scanning receiver that is capable of—

(A) receiving transmissions in the frequencies that are allocated to the domestic cellular radio telecommunications service or the personal communications service;

(B) readily being altered to receive transmissions in such frequencies;

(C) being equipped with decoders that—

(i) convert digital domestic cellular radio telecommunications service, personal communications service, or protected specialized mobile radio service transmissions to analog voice audio; or

(ii) convert protected paging service transmissions to alphanumeric text; or

(D) being equipped with devices that otherwise decode encrypted radio transmissions for the purposes of unauthorized interception.

(2) PRIVACY PROTECTIONS FOR SHARED FREQUENCIES.—The Commission shall, with respect to scanning receivers capable of receiving transmissions in frequencies that are used by commercial mobile services and that are shared by public safety users, examine methods, and may prescribe such regulations as may be necessary, to enhance the privacy of users of such frequencies.

(3) TAMPERING PREVENTION.—In prescribing regulations pursuant to paragraph (1), the Commission shall consider defining "capable of readily being altered" to require scanning receivers to be manufactured in a manner that effectively precludes alteration of equipment features and functions as necessary to prevent commerce in devices that may be used unlawfully to intercept or divulge radio communication.

(4) WARNING LABELS.—In prescribing regulations under paragraph (1), the Commission shall consider requiring labels on scanning receivers warning of the prohibitions in Federal law on intentionally intercepting or divulging radio communications.

(5) DEFINITIONS.—As used in this subsection, the term "protected" means secured by an electronic method that is not published or disclosed except to authorized users, as further defined by Commission regulation.

* * * * * * *

TITLE VII—MISCELLANEOUS PROVISIONS

* * * * * * *

SEC. 705. UNAUTHORIZED *INTERCEPTION OR* PUBLICATION OF COMMUNICATIONS.

(a) [Except as authorized by chapter 119, title 18, United States Code, no person] *No person* receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. No person not being authorized by the sender shall *intentionally* intercept any radio communication [and] *or* divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. [This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator.] *Nothing in this subsection prohibits an interception or disclosure of a communication as authorized by chapter 119 of title 18, United States Code.*

* * * * * * *

(e)(1) Any person who willfully violates subsection (a) shall be [fined not more than $2,000 or] imprisoned for not more than 6 months, *or fined under title 18, United States Code,* or both.

* * * * * * *

(3)(A) Any person aggrieved by [any violation] *any receipt, interception, divulgence, publication, or utilization of any communication in violation* of subsection (a) or paragraph (4) of this subsection may bring a civil action in a United States district court or in any other court of competent jurisdiction.

* * * * * * *

(4) Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized

decryption of satellite cable programming, or direct-to-home satellite services, or is intended for [any other activity prohibited by subsection (a)] *any receipt, interception, divulgence, publication, or utilization of any communication in violation of subsection (a)*, shall be fined not more than $500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both. For purposes of all penalties and remedies established for violations of this paragraph, the prohibited activity established herein as it applies to each such device shall be deemed a separate violation.

* * * * * * *

(7) Notwithstanding any other investigative or enforcement activities of any other Federal agency, the Commission shall investigate alleged violations of this section and may proceed to initiate action under section 503 of this Act to impose forfeiture penalties with respect to such violation upon conclusion of the Commission's investigation.

○