107TH CONGRESS
2D SESSION

S. 2048

To regulate interstate commerce in certain devices by providing for private sector development of technological protection measures to be implemented and enforced by Federal regulations to protect digital content and promote broadband as well as the transition to digital television, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 21, 2002

Mr. HOLLINGS (for himself, Mr. STEVENS, Mr. INOUYE, Mr. BREAUX, Mr. NELSON of Florida, and Mrs. FEINSTEIN) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To regulate interstate commerce in certain devices by providing for private sector development of technological protection measures to be implemented and enforced by Federal regulations to protect digital content and promote broadband as well as the transition to digital television, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF SECTIONS.

(a) SHORT TITLE.—This Act may be cited as the ''Consumer Broadband and Digital Television Promotion Act''.

(b) TABLE OF SECTIONS.—The table of sections for this Act is as follows:

SEC. 2. FINDINGS.

The Congress finds the following:

(1) The lack of high quality digital content continues to hinder consumer adoption of broadband Internet service and digital television products.

(2) Owners of digital programming and content are increasingly reluctant to transmit their products unless digital media devices incorporate technologies that recognize and respond to content security measures designed to prevent theft.

(3) Because digital content can be copied quickly, easily, and without degradation, digital programmers and content owners face an exponentially increasing piracy threat in a digital age.

(4) Current agreements reached in the marketplace to include security technologies in certain digital media devices fail to provide a secure digital environment because those agreements do not prevent the continued use and manufacture of digital media devices that fail to incorporate such security technologies.

(5) Other existing digital rights management schemes represent proprietary, partial solutions that limit, rather than promote, consumers' access to the greatest variety of digital content possible.

(6) Technological solutions can be developed to protect digital content on digital broadcast television and over the Internet.

(7) Competing business interests have frustrated agreement on the deployment of existing technology in digital media devices to protect digital content on the Internet or on digital broadcast television.

(8) The secure protection of digital content is a necessary precondition to the dissemination, and on-line availability, of high quality digital content, which will benefit consumers and lead to the rapid growth of broadband networks.

(9) The secure protection of digital content is a necessary precondition to facilitating and hastening the transition to high-definition television, which will benefit consumers.

(10) Today, cable and satellite have a competitive advantage over digital television because the closed nature of cable and satellite systems permit encryption, which provides some protection for digital content.

(11) Over-the-air broadcasts of digital television are not encrypted for public policy reasons and thus lack those protections afforded to programming delivered via cable or satellite.

(12) A solution to this problem is technologically feasible but will require government action, including a mandate to ensure its swift and ubiquitous adoption.

(13) Consumers receive content such as video or programming in analog form.

(14) When protected digital content is converted to analog for consumers, it is no longer protected and is subject to conversion into unprotected digital form that can in turn be copied or redistributed illegally.

(15) A solution to this problem is technologically feasible but will require government action, including a mandate to ensure its swift and ubiquitous adoption.

(16) Unprotected digital content on the Internet is subject to significant piracy, through illegal file sharing, downloading, and redistribution over the Internet.

(17) Millions of Americans are currently downloading television programs, movies, and music on the Internet and by using ''file-sharing'' technology. Much of this activity is illegal, but demonstrates consumers' desire to access digital content.

(18) This piracy poses a substantial economic threat to America's content industries.

(19) A solution to this problem is technologically feasible but will require government action, including a mandate to ensure its swift and ubiquitous adoption.

(20) Providing a secure, protected environment for digital content should be accompanied by a preservation of legitimate consumer expectations regarding use of digital content in the home.

(21) Secure technological protections should enable content owners to disseminate digital content

over the Internet without frustrating consumers' legitimate expectations to use that content in a legal manner.

(22) Technologies used to protect digital content should facilitate legitimate home use of digital content.

(23) Technologies used to protect digital content should facilitate individuals' ability to engage in legitimate use of digital content for educational or research purposes.

SEC. 3. ADOPTION OF SECURITY SYSTEM STANDARDS AND ENCODING RULES.

(a) PRIVATE SECTOR EFFORTS.—

(1) IN GENERAL.—The Federal Communications Commission, in consultation with the Register of Copyrights, shall make a determination, not more than 12 months after the date of enactment of this Act, as to whether—

(A) representatives of digital media device manufacturers, consumer groups, and copyright owners have reached agreement on security system standards for use in digital media devices and encoding rules; and

(B) the standards and encoding rules conform to the requirements of subsections (d) and (e).

(2) REPORT TO THE COMMERCE AND JUDICIARY COMMITTEES.—Within 6 months after the date of enactment of this Act, the Commission shall report to the Senate Committee on Commerce, Science and Transportation, the Senate Committee on the Judiciary, the House of Representatives Committee on Commerce, and the House of Representatives Committee on the Judiciary as to whether—

(A) substantial progress has been made toward the development of security system standards and encoding rules that will conform to the requirements of subsections (d) and (e);

(B) private sector negotiations are continuing in good faith;

(C) there is a reasonable expectation that final agreement will be reached within 1 year after the date of enactment of this Act; and

(D) if it is unlikely that such a final agreement will be reached by the end of that year, the deadline should be extended.

(b) AFFIRMATIVE DETERMINATION.—If the Commission makes a determination under subsection (a)(1) that

an agreement on security system standards and encoding rules that conform to the requirements of subsections (d) and (e) has been reached, then the Commission shall—

(1) initiate a rulemaking, within 30 days after the date on which the determination is made, to adopt those standards and encoding rules; and

(2) publish a final rule pursuant to that rulemaking, not later than 180 days after initiating the rulemaking, that will take effect 1 year after its publication.

(c) NEGATIVE DETERMINATION.—If the Commission makes a determination under subsection (a)(1) that an agreement on security system standards and encoding rules that conform to the requirements of subsections (d) and (e) has not been reached, then the Commission—

(1) in consultation with representatives described in subsection (a)(1)(A) and the Register of Copyrights, shall initiate a rulemaking, within 30 days after the date on which the determination is made, to adopt security system standards and encoding rules that conform to the requirements of subsections (d) and (e); and

(2) shall publish a final rule pursuant to that rulemaking, not later than 1 year after initiating the

rulemaking, that will take effect 1 year after its publication.

(d) SECURITY SYSTEM STANDARDS.—In achieving the goals of setting open security system standards that will provide effective security for copyrighted works, the security system standards shall ensure, to the extent practicable, that—

(1) the standard security technologies are—

(A) reliable;

(B) renewable;

(C) resistant to attack;

(D) readily implemented;

(E) modular;

(F) applicable to multiple technology platforms;

(G) extensible;

(H) upgradable;

(I) not cost prohibitive; and

(2) any software portion of such standards is based on open source code.

(e) ENCODING RULES.—

(1) LIMITATIONS ON THE EXCLUSIVE RIGHTS OF COPYRIGHT OWNERS.—In achieving the goal of promoting as many lawful uses of copyrighted works as possible, while preventing as much infringement

as possible, the encoding rules shall take into account the limitations on the exclusive rights of copyright owners, including the fair use doctrine.

(2) PERSONAL USE COPIES.—No person may apply a security measure that uses a standard security technology to prevent a lawful recipient from making a personal copy for lawful use in the home of programming at the time it is lawfully performed, on an over-the-air broadcast, premium or non-premium cable channel, or premium or non-premium satellite channel, by a television broadcast station (as defined in section 122(j)(5)(A) of title 17, United States Code), a cable system (as defined in section 111(f) of such title), or a satellite carrier (as defined in section 119(d)(6) of such title).

(f) MEANS OF IMPLEMENTING STANDARDS.—The security system standards adopted under subsection (b), (c), or (g) shall provide for secure technical means of implementing directions of copyright owners for copyrighted works.

(g) COMMISSION MAY REVISE STANDARDS AND RULES THROUGH RULEMAKING.—

(1) IN GENERAL.—The Commission may conduct subsequent rulemakings to modify any security system standards or encoding rules established

under subsection (b) or (c) or to adopt new security system standards that conform to the requirements of subsections (d) and (e).

(2) CONSULTATION REQUIRED.—The Commission shall conduct any such subsequent rulemaking in consultation with representatives of digital media device manufacturers, consumer groups, and copyright owners described in subsection (a)(1)(A) and with the Register of Copyrights.

(3) IMPLEMENTATION.—Any final rule published in such a subsequent rulemaking shall—

(A) apply prospectively only; and

(B) take into consideration the effect of adoption of the modified or new security system standards and encoding rules on consumers' ability to utilize digital media devices manufactured before the modified or new standards take effect.

(h) MODIFICATION OF TECHNOLOGY BY PRIVATE SECTOR.—

(1) IN GENERAL.—After security system standards have been established under subsection (b), (c), or (g) of this section, representatives of digital media device manufacturers, consumer groups, and copyright owners described in subsection (a)(1)(A)

may modify the standard security technology that adheres to the security system standards rules established under this section if those representatives determine that a change in the technology is necessary because—

(A) the technology in use has been compromised; or

(B) technological improvements warrant upgrading the technology in use.

(2) IMPLEMENTATION NOTIFICATION.—The representatives described in paragraph (1) shall notify the Commission of any such modification before it is implemented or, if immediate implementation is determined by the representatives to be necessary, as soon thereafter as possible.

(3) COMPLIANCE WITH SUBSECTION (d) REQUIREMENTS.—The Commission shall ensure that any modification of standard security technology under this subsection conforms to the requirements of subsection (d).

SEC. 4. PRESERVATION OF THE INTEGRITY OF SECURITY.

An interactive computer service shall store and transmit with integrity any security measure associated with standard security technologies that is used in connection with copyrighted material such service transmits or stores.

SEC. 5. PROHIBITION ON SHIPMENT IN INTERSTATE COMMERCE OF NONCONFORMING DIGITAL MEDIA DEVICES.

(a) IN GENERAL.—A manufacturer, importer, or seller of digital media devices may not—

(1) sell, or offer for sale, in interstate commerce, or

(2) cause to be transported in, or in a manner affecting, interstate commerce,

a digital media device unless the device includes and utilizes standard security technologies that adhere to the security system standards adopted under section 3.

(b) EXCEPTION.—Subsection (a) does not apply to the sale, offer for sale, or transportation of a digital media device that was legally manufactured or imported, and sold to the consumer, prior to the effective date of regulations adopted under section 3 and not subsequently modified in violation of section 6(a).

SEC. 6. PROHIBITION ON REMOVAL OR ALTERATION OF SECURITY TECHNOLOGY; VIOLATION OF ENCODING RULES.

(a) REMOVAL OR ALTERATION OF SECURITY TECHNOLOGY.—No person may—

(1) knowingly remove or alter any standard security technology in a digital media device lawfully transported in interstate commerce; or

(2) knowingly transmit or make available to the public any copyrighted material where the security measure associated with a standard security technology has been removed or altered, without the authority of the copyright owner.

(b) COMPLIANCE WITH ENCODING RULES.—No person may knowingly apply to a copyrighted work, that has been distributed to the public, a security measure that uses a standard security technology in violation of the encoding rules adopted under section 3.

SEC. 7. ENFORCEMENT.

(a) IN GENERAL.—The provisions of section 1203 and 1204 of title 17, United States Code, shall apply to any violation of this Act as if—

(1) a violation of section 5 or 6(a)(1) of this Act were a violation of section 1201 of title 17, United States Code; and

(2) a violation of section 4 or section 6(a)(2) of this Act were a violation of section 1202 of that title.

(b) STATUTORY DAMAGES.—A court may award damages for each violation of section 6(b) of not less than $200 and not more than $2,500, as the court considers just.

SEC. 8. FEDERAL ADVISORY COMMITTEE ACT EXEMPTION.

The Federal Advisory Committee Act (5 U.S.C. App.) does not apply to any committee, board, commission, council, conference, panel, task force, or other similar group of representatives of digital media devices and representatives of copyright owners convened for the purpose of developing the security system standards and encoding rules described in section 3.

SEC. 9. DEFINITIONS.

In this Act:

(1) STANDARD SECURITY TECHNOLOGY.—The term ''standard security technology'' means a security technology that adheres to the security system standards adopted under section 3.

(2) INTERACTIVE COMPUTER SERVICE.—The term ''interactive computer service'' has the meaning given that term in section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f)).

(3) DIGITAL MEDIA DEVICE.—The term ''digital media device'' means any hardware or software that—

(A) reproduces copyrighted works in digital form;

(B) converts copyrighted works in digital form into a form whereby the images and sounds are visible or audible; or

(C) retrieves or accesses copyrighted works in digital form and transfers or makes available for transfer such works to hardware or software described in subparagraph (B).

(4) COMMISSION.—The term ''Commission'' means the Federal Communications Commission.

SEC. 10. EFFECTIVE DATE.

This Act shall take effect on the date of enactment of this Act, except that sections 4, 5, and 6 shall take effect on the day on which the final rule published under section 3(b) or (c) takes effect.

○