

107TH CONGRESS
2^D 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. INOUE, 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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE; TABLE OF SECTIONS.**

2 (a) SHORT TITLE.—This Act may be cited as the
3 “Consumer Broadband and Digital Television Promotion
4 Act”.

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

- Sec. 1. Short title; table of sections.
- Sec. 2. Findings.
- Sec. 3. Adoption of security system standards and encoding rules.
- Sec. 4. Preservation of the integrity of security.
- Sec. 5. Prohibition on shipment in interstate commerce of nonconforming digital media devices.
- Sec. 6. Prohibition on removal or alteration of security technology; violation of encoding rules.
- Sec. 7. Enforcement.
- Sec. 8. Federal Advisory Committee Act exemption.
- Sec. 9. Definitions.
- Sec. 10. Effective date.

7 **SEC. 2. FINDINGS.**

8 The Congress finds the following:

9 (1) The lack of high quality digital content con-
10 tinues to hinder consumer adoption of broadband
11 Internet service and digital television products.

12 (2) Owners of digital programming and content
13 are increasingly reluctant to transmit their products
14 unless digital media devices incorporate technologies
15 that recognize and respond to content security meas-
16 ures designed to prevent theft.

17 (3) Because digital content can be copied quick-
18 ly, easily, and without degradation, digital program-
19 mers and content owners face an exponentially in-
20 creasing piracy threat in a digital age.

1 (4) Current agreements reached in the market-
2 place to include security technologies in certain dig-
3 ital media devices fail to provide a secure digital en-
4 vironment because those agreements do not prevent
5 the continued use and manufacture of digital media
6 devices that fail to incorporate such security tech-
7 nologies.

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

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

15 (7) Competing business interests have frus-
16 trated agreement on the deployment of existing tech-
17 nology in digital media devices to protect digital con-
18 tent on the Internet or on digital broadcast tele-
19 vision.

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

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

5 (10) Today, cable and satellite have a competi-
6 tive advantage over digital television because the
7 closed nature of cable and satellite systems permit
8 encryption, which provides some protection for dig-
9 ital content.

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

14 (12) A solution to this problem is techno-
15 logically feasible but will require government action,
16 including a mandate to ensure its swift and ubiq-
17 uitous adoption.

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

20 (14) When protected digital content is con-
21 verted to analog for consumers, it is no longer pro-
22 tected and is subject to conversion into unprotected
23 digital form that can in turn be copied or redistrib-
24 uted illegally.

1 (15) A solution to this problem is techno-
2 logically feasible but will require government action,
3 including a mandate to ensure its swift and ubiq-
4 uitous adoption.

5 (16) Unprotected digital content on the Inter-
6 net is subject to significant piracy, through illegal
7 file sharing, downloading, and redistribution over the
8 Internet.

9 (17) Millions of Americans are currently
10 downloading television programs, movies, and music
11 on the Internet and by using “file-sharing” tech-
12 nology. Much of this activity is illegal, but dem-
13 onstrates consumers’ desire to access digital content.

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

16 (19) A solution to this problem is techno-
17 logically feasible but will require government action,
18 including a mandate to ensure its swift and ubiq-
19 uitous adoption.

20 (20) Providing a secure, protected environment
21 for digital content should be accompanied by a pres-
22 ervation of legitimate consumer expectations regard-
23 ing use of digital content in the home.

24 (21) Secure technological protections should en-
25 able content owners to disseminate digital content

1 over the Internet without frustrating consumers' le-
2 gitimate expectations to use that content in a legal
3 manner.

4 (22) Technologies used to protect digital con-
5 tent should facilitate legitimate home use of digital
6 content.

7 (23) Technologies used to protect digital con-
8 tent should facilitate individuals' ability to engage in
9 legitimate use of digital content for educational or
10 research purposes.

11 **SEC. 3. ADOPTION OF SECURITY SYSTEM STANDARDS AND**
12 **ENCODING RULES.**

13 (a) PRIVATE SECTOR EFFORTS.—

14 (1) IN GENERAL.—The Federal Communica-
15 tions Commission, in consultation with the Register
16 of Copyrights, shall make a determination, not more
17 than 12 months after the date of enactment of this
18 Act, as to whether—

19 (A) representatives of digital media device
20 manufacturers, consumer groups, and copyright
21 owners have reached agreement on security sys-
22 tem standards for use in digital media devices
23 and encoding rules; and

1 (B) the standards and encoding rules con-
2 form to the requirements of subsections (d) and
3 (e).

4 (2) REPORT TO THE COMMERCE AND JUDICI-
5 ARY COMMITTEES.—Within 6 months after the date
6 of enactment of this Act, the Commission shall re-
7 port to the Senate Committee on Commerce, Science
8 and Transportation, the Senate Committee on the
9 Judiciary, the House of Representatives Committee
10 on Commerce, and the House of Representatives
11 Committee on the Judiciary as to whether—

12 (A) substantial progress has been made to-
13 ward the development of security system stand-
14 ards and encoding rules that will conform to
15 the requirements of subsections (d) and (e);

16 (B) private sector negotiations are con-
17 tinuing in good faith;

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

21 (D) if it is unlikely that such a final agree-
22 ment will be reached by the end of that year,
23 the deadline should be extended.

24 (b) AFFIRMATIVE DETERMINATION.—If the Commis-
25 sion makes a determination under subsection (a)(1) that

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

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

7 (2) publish a final rule pursuant to that rule-
8 making, not later than 180 days after initiating the
9 rulemaking, that will take effect 1 year after its pub-
10 lication.

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

16 (1) in consultation with representatives de-
17 scribed in subsection (a)(1)(A) and the Register of
18 Copyrights, shall initiate a rulemaking, within 30
19 days after the date on which the determination is
20 made, to adopt security system standards and en-
21 coding rules that conform to the requirements of
22 subsections (d) and (e); and

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

1 rulemaking, that will take effect 1 year after its pub-
2 lication.

3 (d) SECURITY SYSTEM STANDARDS.—In achieving
4 the goals of setting open security system standards that
5 will provide effective security for copyrighted works, the
6 security system standards shall ensure, to the extent prac-
7 ticable, that—

8 (1) the standard security technologies are—

9 (A) reliable;

10 (B) renewable;

11 (C) resistant to attack;

12 (D) readily implemented;

13 (E) modular;

14 (F) applicable to multiple technology plat-
15 forms;

16 (G) extensible;

17 (H) upgradable;

18 (I) not cost prohibitive; and

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

21 (e) ENCODING RULES.—

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

1 as possible, the encoding rules shall take into ac-
2 count the limitations on the exclusive rights of copy-
3 right owners, including the fair use doctrine.

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

16 (f) MEANS OF IMPLEMENTING STANDARDS.—The se-
17 curity system standards adopted under subsection (b), (c),
18 or (g) shall provide for secure technical means of imple-
19 menting directions of copyright owners for copyrighted
20 works.

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

23 (1) IN GENERAL.—The Commission may con-
24 duct subsequent rulemakings to modify any security
25 system standards or encoding rules established

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

4 (2) CONSULTATION REQUIRED.—The Commis-
5 sion shall conduct any such subsequent rulemaking
6 in consultation with representatives of digital media
7 device manufacturers, consumer groups, and copy-
8 right owners described in subsection (a)(1)(A) and
9 with the Register of Copyrights.

10 (3) IMPLEMENTATION.—Any final rule pub-
11 lished in such a subsequent rulemaking shall—

12 (A) apply prospectively only; and

13 (B) take into consideration the effect of
14 adoption of the modified or new security system
15 standards and encoding rules on consumers'
16 ability to utilize digital media devices manufac-
17 tured before the modified or new standards take
18 effect.

19 (h) MODIFICATION OF TECHNOLOGY BY PRIVATE
20 SECTOR.—

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

1 may modify the standard security technology that
2 adheres to the security system standards rules estab-
3 lished under this section if those representatives de-
4 termine that a change in the technology is necessary
5 because—

6 (A) the technology in use has been com-
7 promised; or

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

10 (2) IMPLEMENTATION NOTIFICATION.—The
11 representatives described in paragraph (1) shall no-
12 tify the Commission of any such modification before
13 it is implemented or, if immediate implementation is
14 determined by the representatives to be necessary,
15 as soon thereafter as possible.

16 (3) COMPLIANCE WITH SUBSECTION (d) RE-
17 QUIREMENTS.—The Commission shall ensure that
18 any modification of standard security technology
19 under this subsection conforms to the requirements
20 of subsection (d).

21 **SEC. 4. PRESERVATION OF THE INTEGRITY OF SECURITY.**

22 An interactive computer service shall store and trans-
23 mit with integrity any security measure associated with
24 standard security technologies that is used in connection
25 with copyrighted material such service transmits or stores.

1 **SEC. 5. PROHIBITION ON SHIPMENT IN INTERSTATE COM-**
2 **MERCE OF NONCONFORMING DIGITAL MEDIA**
3 **DEVICES.**

4 (a) IN GENERAL.—A manufacturer, importer, or sell-
5 er of digital media devices may not—

6 (1) sell, or offer for sale, in interstate com-
7 merce, or

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

10 a digital media device unless the device includes and uti-
11 lizes standard security technologies that adhere to the se-
12 curity system standards adopted under section 3.

13 (b) EXCEPTION.—Subsection (a) does not apply to
14 the sale, offer for sale, or transportation of a digital media
15 device that was legally manufactured or imported, and
16 sold to the consumer, prior to the effective date of regula-
17 tions adopted under section 3 and not subsequently modi-
18 fied in violation of section 6(a).

19 **SEC. 6. PROHIBITION ON REMOVAL OR ALTERATION OF SE-**
20 **CURITY TECHNOLOGY; VIOLATION OF EN-**
21 **CODING RULES.**

22 (a) REMOVAL OR ALTERATION OF SECURITY TECH-
23 NOLOGY.—No person may—

24 (1) knowingly remove or alter any standard se-
25 curity technology in a digital media device lawfully
26 transported in interstate commerce; or

1 (2) knowingly transmit or make available to the
2 public any copyrighted material where the security
3 measure associated with a standard security tech-
4 nology has been removed or altered, without the au-
5 thority of the copyright owner.

6 (b) COMPLIANCE WITH ENCODING RULES.—No per-
7 son may knowingly apply to a copyrighted work, that has
8 been distributed to the public, a security measure that
9 uses a standard security technology in violation of the en-
10 coding rules adopted under section 3.

11 **SEC. 7. ENFORCEMENT.**

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

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

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

21 (b) STATUTORY DAMAGES.—A court may award
22 damages for each violation of section 6(b) of not less than
23 \$200 and not more than \$2,500, as the court considers
24 just.

1 **SEC. 8. FEDERAL ADVISORY COMMITTEE ACT EXEMPTION.**

2 The Federal Advisory Committee Act (5 U.S.C. App.)
3 does not apply to any committee, board, commission, coun-
4 cil, conference, panel, task force, or other similar group
5 of representatives of digital media devices and representa-
6 tives of copyright owners convened for the purpose of de-
7 veloping the security system standards and encoding rules
8 described in section 3.

9 **SEC. 9. DEFINITIONS.**

10 In this Act:

11 (1) **STANDARD SECURITY TECHNOLOGY.**—The
12 term “standard security technology” means a secu-
13 rity technology that adheres to the security system
14 standards adopted under section 3.

15 (2) **INTERACTIVE COMPUTER SERVICE.**—The
16 term “interactive computer service” has the meaning
17 given that term in section 230(f) of the Communica-
18 tions Act of 1934 (47 U.S.C. 230(f)).

19 (3) **DIGITAL MEDIA DEVICE.**—The term “digital
20 media device” means any hardware or software
21 that—

22 (A) reproduces copyrighted works in digital
23 form;

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

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

5 (4) COMMISSION.—The term “Commission”
6 means the Federal Communications Commission.

7 **SEC. 10. EFFECTIVE DATE.**

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

○