

[DISCUSSION DRAFT]

MARCH 20, 2015

114TH CONGRESS
1ST SESSION**H. R.** _____

To require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mrs. BLACKBURN (for herself, Mr. WELCH, Mr. BURGESS, and Mr. LOEBSACK) introduced the following bill; which was referred to the Committee on _____

A BILL

To require certain entities who collect and maintain personal information of individuals to secure such information and to provide notice to such individuals in the case of a breach of security involving such information, 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; PURPOSES.**

2 (a) SHORT TITLE.—This Act may be cited as the
3 “Data Security and Breach Notification Act of 2015”.

4 (b) PURPOSES.—The purposes of this Act are to—

5 (1) protect consumers from identity theft, eco-
6 nomic loss or economic harm, and financial fraud by
7 establishing strong and uniform national data secu-
8 rity and breach notification standards for electronic
9 data in interstate commerce while minimizing State
10 law burdens that may substantially affect interstate
11 commerce; and

12 (2) expressly preempt any related State laws
13 **[and common law]** to ensure uniformity of this
14 Act’s standards and the consistency of their applica-
15 tion across jurisdictions.

16 **SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.**

17 A covered entity shall implement and maintain rea-
18 sonable security measures and practices to protect and se-
19 cure personal information in electronic form against unau-
20 thorized access as appropriate for the size and complexity
21 of such covered entity and the nature and scope of its ac-
22 tivities.

23 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**
24 **BREACH.**

25 (a) IN GENERAL.—

1 (1) IN GENERAL.—Except as otherwise pro-
2 vided by this section, a covered entity that uses, ac-
3 cesses, transmits, stores, disposes of, or collects per-
4 sonal information shall, following the discovery of a
5 breach of security, conduct in good faith a reason-
6 able and prompt investigation of the breach of secu-
7 rity to determine whether there is a reasonable risk
8 that the breach of security has resulted in, or will
9 result in, identity theft, economic loss or economic
10 harm, or financial fraud to the individuals whose
11 personal information was subject to the breach of se-
12 curity.

13 (2) NOTICE.—Unless there is no reasonable
14 risk that the breach of security has resulted in, or
15 will result in, identity theft, economic loss or eco-
16 nomic harm, or financial fraud to the individuals
17 whose personal information was subject to the
18 breach of security, the covered entity shall notify any
19 resident of the United States that has been affected
20 by, or is reasonably believed to have been affected
21 by, the breach of security within the time specified
22 in subsection (c).

23 (3) LAW ENFORCEMENT.—A covered entity
24 shall as expeditiously as possible notify the Commis-
25 sion and the Secret Service or the Federal Bureau

1 of Investigation of the fact that a breach of security
2 has occurred if the number of individuals whose per-
3 sonal information was, or there is a reasonable basis
4 to conclude was, accessed or acquired by an unau-
5 thORIZED person exceeds 10,000.

6 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

7 (1) THIRD-PARTY ENTITIES.—

8 (A) IN GENERAL.—In the event of a
9 breach of security involving personal informa-
10 tion that is stored, processed, or maintained by
11 a third-party entity for a covered entity, such
12 third-party entity shall promptly notify such
13 covered entity of the personal information that
14 was breached. If a covered entity is acting sole-
15 ly as a third-party entity for purposes of this
16 paragraph, the third-party entity has no other
17 notification obligations under this section.

18 (B) COVERED ENTITIES WHO RECEIVE NO-
19 TICE FROM THIRD-PARTY ENTITIES.—Upon re-
20 ceiving notification from a third-party entity
21 under subparagraph (A), a covered entity shall
22 provide notification as required under sub-
23 section (a), unless it is agreed in writing that
24 the third-party entity will provide such notifica-

1 tion on behalf of the covered entity subject to
2 the requirements of subsection (d)(3).

3 (C) EXCEPTION FOR SERVICE PRO-
4 VIDERS.—A service provider shall not be consid-
5 ered a third-party entity for purposes of this
6 paragraph.

7 (2) NON-PROFIT ORGANIZATIONS.—In the event
8 of a breach of security involving personal informa-
9 tion that would trigger notification under subsection
10 (a), a non-profit organization may complete such no-
11 tification according to the procedures set forth in
12 subsection (d)(2).

13 (3) COORDINATION OF NOTIFICATION WITH
14 CONSUMER REPORTING AGENCIES.—If a covered en-
15 tity is required to provide notification to more than
16 10,000 individuals under subsection (a), such cov-
17 ered entity shall also notify a consumer reporting
18 agency that compiles and maintains files on con-
19 sumers on a nationwide basis, of the timing and dis-
20 tribution of the notices. Such notice shall be given
21 to such consumer reporting agencies without unrea-
22 sonable delay and, if it will not delay notice to the
23 affected individuals, prior to the distribution of no-
24 tices to the affected individuals.

25 (c) TIMELINESS OF NOTIFICATION.—

1 (1) IN GENERAL.—Unless subject to a delay au-
2 thorized under paragraph (2), a covered entity shall
3 identify the individuals affected by a breach of secu-
4 rity and make the notification required under sub-
5 section (a) as expeditiously as possible and without
6 unreasonable delay, not later than 30 days after
7 such covered entity has taken the necessary meas-
8 ures to determine the scope of the breach of security
9 and restore the reasonable integrity, security, and
10 confidentiality of the data system. If a covered entity
11 has provided the notification to individuals required
12 under subsection (a) and after such notification dis-
13 covers additional individuals to whom notification is
14 required under such subsection with respect to the
15 same breach of security, the covered entity shall
16 make such notification to such individuals as expedi-
17 tiously as possible and without unreasonable delay.

18 (2) DELAY OF NOTIFICATION AUTHORIZED FOR
19 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-
20 POSES.—Notwithstanding paragraph (1), if a Fed-
21 eral, State, or local law enforcement agency deter-
22 mines that the notification to individuals required
23 under this section would impede a civil or criminal
24 investigation or a Federal agency determines that
25 such notification would threaten national security,

1 such notification shall be delayed upon written re-
2 quest of the law enforcement agency or Federal
3 agency which the law enforcement agency or Federal
4 agency determines is reasonably necessary and re-
5 quests in writing. A law enforcement agency or Fed-
6 eral agency may, by a subsequent written request,
7 revoke such delay or extend the period of time set
8 forth in the original request made under this para-
9 graph if further delay is necessary. If a law enforce-
10 ment agency or Federal agency requests a delay of
11 notification to individuals under this paragraph, the
12 Commission shall, upon written request of the law
13 enforcement agency or Federal agency, delay any
14 public disclosure of a notification received by the
15 Commission under this section relating to the same
16 breach of security until the delay of notification to
17 individuals is no longer in effect.

18 (d) METHOD AND CONTENT OF NOTIFICATION.—

19 (1) DIRECT NOTIFICATION.—

20 (A) METHOD OF NOTIFICATION.—A cov-
21 ered entity required to provide notification to
22 an individual under subsection (a) shall be in
23 compliance with such requirement if the covered
24 entity provides such notice by one of the fol-
25 lowing methods (if the selected method can rea-

1 sonably be expected to reach the intended indi-
2 vidual):

3 (i) Written notification by postal mail.

4 (ii) Notification by email or other
5 electronic means, if—

6 (I) the covered entity's primary
7 method of communication with the in-
8 dividual is by email or such other elec-
9 tronic means or the individual has
10 consented to receive such notification;
11 and

12 **[(II) the email or other elec-**
13 **tronic means does not contain a**
14 **hyperlink.]**

15 (B) CONTENT OF NOTIFICATION.—Regard-
16 less of the method by which notification is pro-
17 vided to an individual under subparagraph (A)
18 with respect to a breach of security, such notifi-
19 cation shall include each of the following:

20 (i) A description of the personal infor-
21 mation that was, or there is a reasonable
22 basis to conclude was, acquired or accessed
23 by an unauthorized person.

24 (ii) The date range of the breach of
25 security, or an approximate date range of

1 the breach of security if a specific date
2 range is unknown based on the information
3 available at the time of the notification.

4 (iii) A telephone number, or toll-free
5 telephone number for any covered entity
6 that does not meet the definition of a small
7 business concern or non-profit organiza-
8 tion, that the individual may use to contact
9 the covered entity to inquire about the
10 breach of security or the information the
11 covered entity maintained about that indi-
12 vidual.

13 (iv) The toll-free contact telephone
14 numbers and addresses for a consumer re-
15 porting agency that compiles and main-
16 tains files on consumers on a nationwide
17 basis.

18 (v) The toll-free telephone number
19 and Internet website address for the Com-
20 mission whereby the individual may obtain
21 information regarding identity theft.

22 (2) SUBSTITUTE NOTIFICATION.—

23 (A) IN GENERAL.—If, after making rea-
24 sonable efforts to contact all individuals to
25 whom notice is required under subsection (a),

1 the covered entity finds that contact informa-
2 tion for 500 or more individuals is insufficient
3 or out-of-date, the covered entity shall also pro-
4 vide substitute notice to those individuals,
5 which shall be reasonably calculated to reach
6 the individuals affected by the breach of secu-
7 rity.

8 (B) FORM OF SUBSTITUTE NOTIFICA-
9 TION.—A covered entity may provide substitute
10 notification by—

11 (i) email or other electronic notifica-
12 tion to the extent that the covered entity
13 has contact information for individuals to
14 whom it is required to provide notification
15 under subsection (a) [and provided such
16 email or electronic means does not contain
17 a hyperlink]; and

18 (ii) a conspicuous notice on the cov-
19 ered entity's Internet website (if such cov-
20 ered entity maintains such a website) for
21 at least 90 days.

22 (C) CONTENT OF SUBSTITUTE NOTICE.—
23 Each form of substitute notice under clauses (i)
24 and (ii) of subparagraph (B) shall include the
25 information required under paragraph (1)(B).

1 (3) DIRECT NOTIFICATION BY A THIRD
2 PARTY.—Nothing in this Act shall be construed to
3 prevent a covered entity from contracting with a
4 third party to provide the notification required under
5 this section, provided such third party issues such
6 notification without unreasonable delay, in accord-
7 ance with the requirements of this section, and indi-
8 cates to all individuals in such notification that such
9 third party is sending such notification on behalf of
10 the covered entity.

11 (e) REQUIREMENTS OF SERVICE PROVIDERS.—

12 (1) IN GENERAL.—If a service provider becomes
13 aware of a breach of security involving data in elec-
14 tronic form containing personal information that is
15 owned or licensed by a covered entity that connects
16 to or uses a system or network provided by the serv-
17 ice provider for the purpose of transmitting, routing,
18 or providing intermediate or transient storage of
19 such data, such service provider shall notify the cov-
20 ered entity who initiated such connection, trans-
21 mission, routing, or storage of the data containing
22 personal information breached, if such covered entity
23 can be reasonably identified. If a service provider is
24 acting solely as a service provider for purposes of

1 this subsection, the service provider has no other no-
2 tification obligations under this section.

3 (2) COVERED ENTITIES WHO RECEIVE NOTICE
4 FROM SERVICE PROVIDERS.—Upon receiving notifi-
5 cation from a service provider under paragraph (1),
6 a covered entity shall provide notification as required
7 under this section.

8 **SEC. 4. ENFORCEMENT.**

9 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-
10 MISSION.—

11 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
12 TICES.—A violation of section 2 or 3 shall be treated
13 as an unfair and deceptive act or practice in viola-
14 tion of a regulation under section 18(a)(1)(B) of the
15 Federal Trade Commission Act (15 U.S.C.
16 57a(a)(1)(B)) regarding unfair or deceptive acts or
17 practices.

18 (2) POWERS OF COMMISSION.—The Commis-
19 sion shall enforce this Act in the same manner, by
20 the same means, and with the same jurisdiction,
21 powers, and duties as though all applicable terms
22 and provisions of the Federal Trade Commission Act
23 (15 U.S.C. 41 et seq.) were incorporated into and
24 made a part of this Act, and any covered entity who
25 violates this Act shall be subject to the penalties and

1 entitled to the privileges and immunities provided in
2 the Federal Trade Commission Act (15 U.S.C. 41 et
3 seq.), and as provided in clauses (ii) and (iii) of sec-
4 tion 5(4)(A).

5 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
6 ERAL.—

7 (1) CIVIL ACTION.—In any case in which the
8 attorney general of a State has reason to believe
9 that an interest of the residents of that State has
10 been or is threatened or adversely affected by any
11 covered entity who violates section 2 or 3 of this
12 Act, the attorney general of the State, as *parens*
13 *patriae*, may bring a civil action on behalf of the
14 residents of the State in a district court of the
15 United States of appropriate jurisdiction to—

16 (A) enjoin further violation of such section
17 by the defendant;

18 (B) compel compliance with such section;

19 or

20 (C) obtain civil penalties in the amount de-
21 termined under paragraph (2).

22 (2) CIVIL PENALTIES.—

23 (A) CALCULATION.—

24 (i) TREATMENT OF VIOLATIONS OF
25 SECTION 2.—For purposes of paragraph

1 (1)(C) with regard to a violation of section
2 2, the amount determined under this para-
3 graph is the amount calculated by multi-
4 plying the number of days that a covered
5 entity is not in compliance with such sec-
6 tion by an amount not greater than
7 \$11,000.

8 (ii) TREATMENT OF VIOLATIONS OF
9 SECTION 3.—For purposes of paragraph
10 (1)(C) with regard to a violation of section
11 3, the amount determined under this para-
12 graph is the amount calculated by multi-
13 plying the number of violations of such
14 section by an amount not greater than
15 \$11,000. Each failure to send notification
16 as required under section 3 to a resident of
17 the State shall be treated as a separate
18 violation.

19 (B) MAXIMUM TOTAL LIABILITY.—Not-
20 withstanding the number of actions which may
21 be brought against a covered entity under this
22 subsection, the maximum civil penalty for which
23 any covered entity may be liable under this sub-
24 section shall not exceed—

1 (i) \$2,500,000 for each violation of
2 section 2; and

3 (ii) \$2,500,000 for all violations of
4 section 3 resulting from a single breach of
5 security.

6 (C) ADJUSTMENT FOR INFLATION.—Be-
7 ginning on the date that the Consumer Price
8 Index is first published by the Bureau of Labor
9 Statistics that is after one year after the date
10 of enactment of this Act, and each year there-
11 after, the amounts specified in clauses (i) and
12 (ii) of subparagraph (A) and clauses (i) and (ii)
13 of subparagraph (B) shall be increased by the
14 percentage increase in the Consumer Price
15 Index published on that date from the Con-
16 sumer Price Index published the previous year.

17 (D) PENALTY FACTORS.—In determining
18 the amount of such a civil penalty, the degree
19 of culpability, any history of prior such conduct,
20 ability to pay, effect on ability to continue to do
21 business, and such other matters as justice may
22 require shall be taken into account.

23 (3) INTERVENTION BY THE FEDERAL TRADE
24 COMMISSION.—

1 (A) NOTICE AND INTERVENTION.—In all
2 cases, the State shall provide prior written no-
3 tice of any action under paragraph (1) to the
4 Commission and provide the Commission with a
5 copy of its complaint, except in any case in
6 which such prior notice is not feasible, in which
7 case the State shall serve such notice imme-
8 diately upon instituting such action. The Com-
9 mission shall have the right—

10 (i) to intervene in the action;

11 (ii) upon so intervening, to be heard
12 on all matters arising therein; and

13 (iii) to file petitions for appeal.

14 (B) PENDING PROCEEDINGS.—If the Fed-
15 eral Trade Commission initiates a Federal civil
16 action for a violation of this Act, no State at-
17 torney general may bring an action for a viola-
18 tion of this Act that resulted from the same or
19 related acts or omissions against a defendant
20 named in the civil action initiated by the Fed-
21 eral Trade Commission.

22 (4) CONSTRUCTION.—For purposes of bringing
23 any civil action under paragraph (1), nothing in this
24 Act shall be construed to prevent an attorney gen-
25 eral of a State from exercising the powers conferred

1 on the attorney general by the laws of that State
2 to—

3 (A) conduct investigations;

4 (B) administer oaths or affirmations; or

5 (C) compel the attendance of witnesses or
6 the production of documentary and other evi-
7 dence.

8 (c) NO PRIVATE CAUSE OF ACTION.—Nothing in this
9 Act shall be construed to establish a private cause of ac-
10 tion against a person for a violation of this Act.

11 **SEC. 5. DEFINITIONS.**

12 In this Act:

13 (1) BREACH OF SECURITY.—The term “breach
14 of security” means a compromise of the security,
15 confidentiality, or integrity of, or loss of, data in
16 electronic form that results in, or there is a reason-
17 able basis to conclude has resulted in, unauthorized
18 access to or acquisition of personal information from
19 a covered entity.

20 (2) COMMISSION.—The term “Commission”
21 means the Federal Trade Commission.

22 (3) CONSUMER REPORTING AGENCY THAT COM-
23 PILES AND MAINTAINS FILES ON CONSUMERS ON A
24 NATIONWIDE BASIS.—The term “consumer reporting
25 agency that compiles and maintains files on con-

1 sumers on a nationwide basis” has the meaning
2 given that term in section 603(p) of the Fair Credit
3 Reporting Act (15 U.S.C. 1681a(p)).

4 (4) COVERED ENTITY.—

5 (A) IN GENERAL.—The term “covered en-
6 tity” means—

7 (i) a sole proprietorship, partnership,
8 corporation, trust, estate, cooperative, as-
9 sociation, or other entity in or affecting
10 commerce that acquires, maintains, stores,
11 sells, or otherwise uses data in electronic
12 form that includes personal information,
13 over which the Commission has authority
14 pursuant to section 5(a)(2) of the Federal
15 Trade Commission Act (15 U.S.C.
16 45(a)(2));

17 (ii) notwithstanding section 5(a)(2) of
18 the Federal Trade Commission Act (15
19 U.S.C. 45(a)(2)), common carriers subject
20 to the Communications Act of 1934 (47
21 U.S.C. 151 et seq.); and

22 (iii) notwithstanding any jurisdictional
23 limitation of the Federal Trade Commis-
24 sion Act (15 U.S.C. 41 et seq.), any non-
25 profit organization.

1 (B) EXCEPTIONS.—The term “covered en-
2 tity” does not include—

3 (i) a covered entity, as defined in sec-
4 tion 160.103 of title 45, Code of Federal
5 Regulations; or

6 (ii) a broker, dealer, investment com-
7 pany, investment adviser, or person en-
8 gaged in providing insurance that is sub-
9 ject to title V of Public Law 106–102 (15
10 U.S.C. 6801 et seq.).

11 (5) DATA IN ELECTRONIC FORM.—The term
12 “data in electronic form” means any data stored
13 electronically or digitally on any computer system or
14 other database and includes recordable tapes and
15 other mass storage devices.

16 (6) ENCRYPTION.—The term “encryption”—
17 (A) means the protection of data in elec-
18 tronic form, in storage or in transit, using an
19 encryption technology that has been generally
20 accepted by experts in the field of information
21 security at the time the breach of security oc-
22 curred that renders such data indecipherable in
23 the absence of associated cryptographic keys
24 necessary to enable decryption of such data;
25 and

1 (B) includes appropriate management and
2 safeguards of such cryptographic keys in order
3 to protect the integrity of the encryption.

4 (7) NON-PROFIT ORGANIZATION.—The term
5 “non-profit organization” means an organization
6 that is described in section 501(c)(3) of the Internal
7 Revenue Code of 1986 and exempt from tax under
8 section 501(a) of such Code.

9 (8) PERSONAL INFORMATION.—

10 (A) IN GENERAL.—The term “personal in-
11 formation” means any information or compila-
12 tion of information in electronic form that in-
13 cludes the following:

14 (i) An individual’s first and last name
15 or first initial and last name in combina-
16 tion with any one of the following data ele-
17 ments:

18 (I) A driver’s license number,
19 passport number, or alien registration
20 number or other government-issued
21 unique identification number.

22 (II) Any two of the following:

23 (aa) Home address or tele-
24 phone number.

1 (bb) Mother's maiden name,
2 if identified as such.

3 (cc) Month, day, and year of
4 birth.

5 (ii) A financial account number or
6 credit or debit card number or other iden-
7 tifier, in combination with any security
8 code, access code, or password that is re-
9 quired for an individual to obtain credit,
10 withdraw funds, or engage in a financial
11 transaction.

12 (iii) A unique account identifier (other
13 than for an account described in clause
14 (ii)), electronic identification number, bio-
15 metric data unique to an individual, user
16 name, or routing code in combination with
17 any associated security code, access code,
18 biometric data unique to an individual, or
19 password that is required for an individual
20 to obtain money, or purchase goods, serv-
21 ices, or any other thing of value.

22 (iv) A non-truncated social security
23 number.

24 (v) [For any telecommunications car-
25 rier or interconnected VoIP provider, the

1 location of, number from which and to
2 which a call is placed, and the time and
3 duration of such call.】

4 (B) EXCEPTIONS.—The term “personal in-
5 formation” does not include—

6 (i) information that is encrypted or
7 rendered unusable, unreadable, or indeci-
8 pherable through data security technology
9 or methodology that is generally accepted
10 by experts in the field of information secu-
11 rity at the time the breach of security oc-
12 curred, such as redaction or access con-
13 trols; or

14 (ii) information obtained from a pub-
15 licly available source, including information
16 obtained from a news report, periodical, or
17 other widely distributed media, or from
18 Federal, State, or local government
19 records.

20 (9) SERVICE PROVIDER.—The term “service
21 provider” means a covered entity subject to the
22 Communications Act of 1934 (47 U.S.C. 151 et
23 seq.) that provides electronic data transmission,
24 routing, intermediate and transient storage, or con-
25 nection to its system or network, where such entity

1 providing such service does not select or modify the
2 content of the electronic data, is not the sender or
3 the intended recipient of the data, and does not dif-
4 ferentiate personal information from other informa-
5 tion that such entity transmits, routes, stores, or for
6 which such entity provides connections. Any such en-
7 tity shall be treated as a service provider under this
8 Act only to the extent that it is engaged in the pro-
9 vision of such transmission, routing, intermediate
10 and transient storage, or connections.

11 (10) SMALL BUSINESS CONCERN.—The term
12 “small business concern” has the meaning given
13 such term under section 3 of the Small Business Act
14 (15 U.S.C. 632).

15 (11) STATE.—The term “State” means each of
16 the several States, the District of Columbia, the
17 Commonwealth of Puerto Rico, Guam, American
18 Samoa, the Virgin Islands of the United States, the
19 Commonwealth of the Northern Mariana Islands,
20 any other territory or possession of the United
21 States, and each federally recognized Indian tribe.

22 **SEC. 6. EFFECT ON OTHER LAWS.**

23 (a) PREEMPTION OF STATE INFORMATION SECURITY
24 LAWS.—No State or political subdivision of a State shall,
25 with respect to a covered entity subject to this Act, adopt,

1 maintain, enforce, or impose or continue in effect any law,
2 rule, regulation, duty, requirement, standard, or other
3 provision having the force and effect of law relating to or
4 with respect to the security of data in electronic form or
5 notification following a breach of security.

6 **[(b) COMMON LAW.—**This section shall not exempt
7 a covered entity from liability under common law. **[The**
8 *parties to this staff draft have not yet reached agreement*
9 *on the scope of preemption and continue to discuss the*
10 *issue.]*

11 **(c) CERTAIN FTC ENFORCEMENT LIMITED TO DATA**
12 **SECURITY AND BREACH NOTIFICATION.—**

13 **(1) DATA SECURITY AND BREACH NOTIFICA-**
14 **TION.—**Insofar as sections 201, 202, 222, 338, and
15 631 of the Communications Act of 1934 (47 U.S.C.
16 201, 202, 222, 338, and 551), and any regulations
17 promulgated thereunder, apply to covered entities
18 with respect to securing information in electronic
19 form from unauthorized access, including notifica-
20 tion of unauthorized access to data in electronic
21 form containing personal information, such sections
22 and regulations promulgated thereunder shall have
23 no force or effect, unless such regulations pertain
24 solely to 9-1-1 calls.

1 (2) RULE OF CONSTRUCTION.—Nothing in this
2 subsection otherwise limits the Federal Communica-
3 tions Commission’s authority with respect to sec-
4 tions 201, 202, 222, 338, and 631 of the Commu-
5 nications Act of 1934 (47 U.S.C. 201, 202, 222,
6 338, and 551).

7 (d) PRESERVATION OF COMMISSION AUTHORITY.—
8 Nothing in this Act may be construed in any way to limit
9 or affect the Commission’s authority under any other pro-
10 vision of law.

11 **SEC. 7. EFFECTIVE DATE.**

12 This Act shall take effect 1 year after the date of
13 enactment of this Act.