

6866

2015-2016 Regular Sessions

I N A S S E M B L Y

April 8, 2015

Introduced by M. of A. DINOWITZ -- (at request of the Department of Law)
-- read once and referred to the Committee on Consumer Affairs and
Protection

AN ACT to amend the general business law and the state technology law,
in relation to the data security act

THE PEOPLE OF THE STATE OF NEW YORK, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

1 Section 1. This act shall be known and may be cited as the "data secu-
2 rity act".
3 S 2. The opening paragraph and paragraph (b) of subdivision 1 of
4 section 899-aa of the general business law, as added by chapter 442 of
5 the laws of 2005, are amended to read as follows:
6 As used in this section, AND SECTION EIGHT HUNDRED NINETY-NINE-BB OF
7 THIS ARTICLE, the following terms shall have the following meanings:
8 (b) "Private information" shall mean EITHER: (I) personal information
9 consisting of any information in combination with any one or more of the
10 following data elements, when either the personal information or the
11 data element is not encrypted, or encrypted with an encryption key that
12 has also been acquired:
13 (1) social security number;
14 (2) driver's license number or non-driver identification card number;
15 [or]
16 (3) account number, credit or debit card number, in combination with
17 any required security code, access code, or password that would permit
18 access to an individual's financial account; OR
19 (4) BIOMETRIC INFORMATION, MEANING DATA GENERATED BY AUTOMATIC MEAS-
20 UREMENTS OF AN INDIVIDUAL'S PHYSICAL CHARACTERISTICS, WHICH ARE USED BY
21 THE OWNER OR LICENSEE TO AUTHENTICATE THE INDIVIDUAL'S IDENTITY;
22 (II) A USER NAME OR EMAIL ADDRESS IN COMBINATION WITH A PASSWORD OR
23 SECURITY QUESTION AND ANSWER THAT WOULD PERMIT ACCESS TO AN ONLINE
24 ACCOUNT; OR

EXPLANATION--Matter in ITALICS (underscored) is new; matter in brackets
[] is old law to be omitted.

LBD08145-09-5

(III) ANY UNSECURED PROTECTED HEALTH INFORMATION AS DEFINED IN THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (45 C.F.R. PTS. 160, 162, 164), AS AMENDED FROM TIME TO TIME.

"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

S 3. Subdivisions 4 and 5 of section 899-aa of the general business law, as added by chapter 442 of the laws of 2005, are amended to read as follows:

4. (A) The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

(B) THE PRODUCTION OF FORENSIC REPORTS TO LOCAL AND STATE LAW ENFORCEMENT AGENCIES FOR THE PURPOSES OF INVESTIGATING AND IDENTIFYING THOSE RESPONSIBLE FOR A BREACH OF THE SECURITY OF THE SYSTEM SHALL NOT CONSTITUTE A WAIVER OF ANY APPLICABLE PRIVILEGE OR PROTECTION PROVIDED BY LAW, INCLUDING TRADE SECRET PROTECTION, AND FORENSIC REPORTS SO PRODUCED SHALL NOT BE SUBJECT TO DISCLOSURE UNDER ARTICLE SIX OF THE PUBLIC OFFICERS LAW.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction[.];

(c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or

(d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such business has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and

(3) notification to major statewide media.

(E) IN THE CASE OF A BREACH OF THE SECURITY OF THE SYSTEM INVOLVING A USER NAME, AND PASSWORD OR SECURITY QUESTION AND ANSWER WHICH WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT, AS PROVIDED IN SUBPARAGRAPH (II) OF PARAGRAPH (B) OF SUBDIVISION ONE OF THIS SECTION, AND NO OTHER PRIVATE INFORMATION DEFINED IN SUCH PARAGRAPH (B), THE PERSON OR BUSINESS MAY COMPLY WITH THIS SECTION BY PROVIDING NOTIFICATION IN ELECTRONIC OR OTHER FORM THAT DIRECTS THE PERSON WHOSE PRIVATE INFORMATION HAS BEEN BREACHED PROMPTLY TO CHANGE HIS OR HER PASSWORD AND SECURITY QUESTION OR ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS APPROPRIATE TO PROTECT THE ONLINE ACCOUNT WITH THE PERSON OR BUSINESS AND ALL OTHER ONLINE ACCOUNTS

FOR WHICH THE PERSON WHOSE PRIVATE INFORMATION HAS BEEN BREACHED USES THE SAME INFORMATION.

(F) IN THE CASE OF A BREACH OF THE SECURITY OF THE SYSTEM INVOLVING THE LOGIN CREDENTIALS OF AN EMAIL ACCOUNT FURNISHED BY THE PERSON OR BUSINESS AS PROVIDED IN SUBPARAGRAPH (II) OF PARAGRAPH (B) OF SUBDIVISION ONE OF THIS SECTION, THE PERSON OR BUSINESS SHALL NOT COMPLY WITH THIS SECTION BY PROVIDING THE SECURITY BREACH NOTIFICATION TO THAT EMAIL ADDRESS, BUT SHALL, INSTEAD, COMPLY WITH THIS SECTION BY PROVIDING NOTICE BY ANOTHER METHOD DESCRIBED IN THIS SUBDIVISION OR BY CLEAR AND CONSPICUOUS NOTICE DELIVERED TO THE RESIDENT ONLINE WHEN THE RESIDENT IS CONNECTED TO THE ONLINE ACCOUNT FROM AN INTERNET PROTOCOL ADDRESS OR ONLINE LOCATION FROM WHICH THE PERSON OR BUSINESS KNOWS THE RESIDENT CUSTOMARILY ACCESSES THE ACCOUNT.

S 4. Paragraph (a) of subdivision 6 of section 899-aa of the general business law, as amended by chapter 491 of the laws of 2005, is amended to read as follows:

(a) whenever the attorney general shall believe from evidence satisfactory to him OR HER that there is a violation of this [article] SECTION he OR SHE may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this [article] SECTION, if notification was not provided to such person pursuant to this [article] SECTION, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this [article] SECTION knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, provided that the latter amount shall not exceed one [hundred fifty thousand] MILLION dollars.

S 5. Paragraph (a) of subdivision 1 of section 208 of the state technology law, as added by chapter 442 of the laws of 2005, is amended to read as follows:

(a) "Private information" shall mean EITHER: (I) personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number; or

(3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account;

(II) A USER NAME OR EMAIL ADDRESS IN COMBINATION WITH A PASSWORD OR SECURITY QUESTION AND ANSWER THAT WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT; OR

(III) ANY UNSECURED PROTECTED HEALTH INFORMATION AS DEFINED IN THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (45 C.F.R. PTS. 160, 162, 164), AS AMENDED FROM TIME TO TIME.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

S 6. The general business law is amended by adding a new section 899-bb to read as follows:

1 S 899-BB. DATA SECURITY REQUIREMENTS. 1. REASONABLE SAFEGUARDS. (A)
2 ANY PERSON OR BUSINESS THAT CONDUCTS BUSINESS IN NEW YORK STATE, AND
3 OWNS OR LICENSES COMPUTERIZED DATA WHICH INCLUDES PRIVATE INFORMATION OF
4 A RESIDENT OF NEW YORK SHALL DEVELOP, IMPLEMENT AND MAINTAIN REASONABLE
5 SAFEGUARDS TO PROTECT THE SECURITY, CONFIDENTIALITY AND INTEGRITY OF THE
6 PRIVATE INFORMATION, INCLUDING DISPOSAL OF DATA.

7 (B) THE FOLLOWING SHALL BE DEEMED TO BE IN COMPLIANCE WITH PARAGRAPH
8 (A) OF THIS SUBDIVISION:

9 (I) A PERSON OR BUSINESS THAT COMPLIES WITH A STATE OR FEDERAL LAW
10 PROVIDING GREATER PROTECTION TO PRIVATE INFORMATION THAN THAT PROVIDED
11 BY THIS SECTION;

12 (II) A PERSON OR BUSINESS THAT IS SUBJECT TO AND COMPLIES WITH REGU-
13 LATIONS PROMULGATED PURSUANT TO TITLE V OF THE GRAMM-LEACH-BLILEY ACT OF
14 1999 (15 U.S.C. 6801 TO 6809);

15 (III) A PERSON OR BUSINESS THAT COMPLIES WITH CURRENT INTERNATIONAL
16 STANDARDS ORGANIZATION STANDARDS FOR INFORMATION SECURITY;

17 (IV) A PERSON OR BUSINESS THAT IS SUBJECT TO AND COMPLIES WITH REGU-
18 LATIONS IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY
19 ACT OF 1996 (45 C.F.R. PARTS 160 AND 164) AND THE HEALTH INFORMATION
20 TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT, AS AMENDED FROM TIME TO
21 TIME;

22 (V) A PERSON OR BUSINESS THAT COMPLIES WITH CURRENT NATIONAL INSTITUTE
23 OF STANDARDS AND TECHNOLOGY STANDARDS AS REFERENCED IN SUBDIVISION THREE
24 OF THIS SECTION; OR

25 (VI) A PERSON OR BUSINESS THAT IMPLEMENTS AN INFORMATION SECURITY
26 PROGRAM THAT INCLUDES THE FOLLOWING:

27 (A) ADMINISTRATIVE SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE
28 PERSON OR BUSINESS:

29 (I) DESIGNATES ONE OR MORE EMPLOYEES TO COORDINATE THE SECURITY
30 PROGRAM;

31 (II) IDENTIFIES REASONABLY FORESEEABLE INTERNAL AND EXTERNAL RISKS;

32 (III) ASSESSES THE SUFFICIENCY OF SAFEGUARDS IN PLACE TO CONTROL THE
33 IDENTIFIED RISKS;

34 (IV) TRAINS AND MANAGES EMPLOYEES IN THE SECURITY PROGRAM PRACTICES
35 AND PROCEDURES;

36 (V) SELECTS SERVICE PROVIDERS CAPABLE OF MAINTAINING APPROPRIATE SAFE-
37 GUARDS, AND REQUIRES THOSE SAFEGUARDS BY CONTRACT;

38 (VI) ADJUSTS THE SECURITY PROGRAM IN LIGHT OF BUSINESS CHANGES OR NEW
39 CIRCUMSTANCES; AND

40 (B) TECHNICAL SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE PERSON OR
41 BUSINESS:

42 (I) ASSESSES RISKS IN NETWORK AND SOFTWARE DESIGN;

43 (II) ASSESSES RISKS IN INFORMATION PROCESSING, TRANSMISSION AND STOR-
44 AGE;

45 (III) DETECTS, PREVENTS AND RESPONDS TO ATTACKS OR SYSTEM FAILURES;

46 (IV) REGULARLY TESTS AND MONITORS THE EFFECTIVENESS OF KEY CONTROLS,
47 SYSTEMS AND PROCEDURES; AND

48 (C) PHYSICAL SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE PERSON OR
49 BUSINESS:

50 (I) ASSESSES RISKS OF INFORMATION STORAGE AND DISPOSAL;

51 (II) DETECTS, PREVENTS AND RESPONDS TO INTRUSIONS;

52 (III) PROTECTS AGAINST UNAUTHORIZED ACCESS TO OR USE OF PRIVATE INFOR-
53 MATION DURING OR AFTER THE COLLECTION, TRANSPORTATION AND DESTRUCTION OR
54 DISPOSAL OF THE INFORMATION; AND

1 (IV) DISPOSES OF PRIVATE INFORMATION AFTER IT IS NO LONGER NEEDED FOR
2 BUSINESS PURPOSES BY ERASING ELECTRONIC MEDIA SO THAT THE INFORMATION
3 CANNOT BE READ OR RECONSTRUCTED.

4 2. REBUTTABLE PRESUMPTION. A PERSON OR BUSINESS THAT OBTAINS AN INDE-
5 PENDENT, THIRD-PARTY AUDIT AND CERTIFICATION ANNUALLY UNDER THE DATA
6 SECURITY STANDARD LISTED IN PARAGRAPH (B) OF SUBDIVISION ONE OF THIS
7 SECTION SHALL RECEIVE A REBUTTABLE PRESUMPTION THAT IT MAINTAINED
8 REASONABLE SAFEGUARDS TO PROTECT THE SECURITY, CONFIDENTIALITY AND
9 INTEGRITY OF THE PRIVATE INFORMATION.

10 3. CERTIFICATION AUTHORITY AND REGULATION. THE DEPARTMENT OF FINAN-
11 CIAL SERVICES SHALL PROMULGATE REGULATIONS REGARDING INDEPENDENT,
12 THIRD-PARTY LICENSED INSURERS RESPONSIBLE FOR CERTIFYING ENTITIES THAT
13 MEET THE REASONABLE DATA SECURITY REQUIREMENTS SET FORTH IN SUBPARAGRAPH
14 (VI) OF PARAGRAPH (B) OF SUBDIVISION ONE OF THIS SECTION.

15 4. SAFE HARBOR. ANY PERSON OR BUSINESS THAT COMPLIES WITH THE MOST UP
16 TO DATE VERSION OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
17 SPECIAL PUBLICATION 800-53 SHALL BE IMMUNE FROM LIABILITY IN A CIVIL
18 ACTION, INCLUDING BUT NOT LIMITED TO AN ACTION BROUGHT BY THE ATTORNEY
19 GENERAL, RESULTING FROM UNAUTHORIZED ACCESS TO PRIVATE INFORMATION BY A
20 THIRD-PARTY ABSENT EVIDENCE OF WILLFUL MISCONDUCT, BAD FAITH OR GROSS
21 NEGLIGENCE. COMPLIANCE MUST BE CERTIFIED ANNUALLY BY AN INDEPENDENT,
22 THIRD-PARTY LICENSED INSURER, AUTHORIZED BY THE NATIONAL INSTITUTE OF
23 STANDARDS AND TECHNOLOGY.

24 5. ENFORCEMENT. (A) WHENEVER THE ATTORNEY GENERAL SHALL BELIEVE FROM
25 EVIDENCE SATISFACTORY TO HIM OR HER THAT THERE IS A VIOLATION OF THIS
26 SECTION HE OR SHE MAY BRING AN ACTION IN THE NAME AND ON BEHALF OF THE
27 PEOPLE OF THE STATE OF NEW YORK, IN A COURT OF JUSTICE HAVING JURISDIC-
28 TION TO ISSUE AN INJUNCTION, TO ENJOIN AND RESTRAIN THE CONTINUATION OF
29 SUCH VIOLATION. IN SUCH ACTION, PRELIMINARY RELIEF MAY BE GRANTED UNDER
30 ARTICLE SIXTY-THREE OF THE CIVIL PRACTICE LAW AND RULES. IN SUCH ACTION,
31 THE COURT MAY AWARD DAMAGES FOR ACTUAL COSTS OR LOSSES INCURRED BY A
32 PERSON AS A RESULT OF THE FAILURE BY A PERSON OR BUSINESS TO COMPLY WITH
33 THE DATA SECURITY REQUIREMENTS SET FORTH IN THIS SECTION, INCLUDING
34 CONSEQUENTIAL FINANCIAL LOSSES, AS WELL AS A CIVIL PENALTY OF UP TO TWO
35 HUNDRED FIFTY DOLLARS, WHICH PENALTY MAY BE INCREASED BY A FACTOR LESS
36 THAN OR EQUAL TO THE NUMBER OF PERSONS WHOSE PRIVATE INFORMATION WAS
37 COMPROMISED; PROVIDED HOWEVER, THAT THE AGGREGATE AMOUNT OF ANY CIVIL
38 PENALTIES SO IMPOSED SHALL NOT EXCEED TEN MILLION DOLLARS. WHENEVER THE
39 COURT SHALL DETERMINE THAT A PERSON OR BUSINESS VIOLATED THIS SECTION
40 KNOWINGLY OR RECKLESSLY, THE COURT MAY, IN LIEU OF IMPOSING A CIVIL
41 PENALTY AS SET FORTH ABOVE, INSTEAD IMPOSE A CIVIL PENALTY OF UP TO ONE
42 THOUSAND DOLLARS, WHICH PENALTY MAY BE INCREASED BY A FACTOR LESS THAN
43 OR EQUAL TO THE NUMBER OF PERSONS WHOSE PRIVATE INFORMATION WAS COMPRO-
44 MISED; PROVIDED HOWEVER, THAT THE AGGREGATE AMOUNT OF ANY CIVIL PENAL-
45 TIES SO IMPOSED SHALL NOT EXCEED THE GREATER OF FIFTY MILLION DOLLARS OR
46 THREE TIMES THE AGGREGATE AMOUNT OF ANY ACTUAL COSTS AND LOSSES AS
47 DETERMINED BY THE COURT. A COURT MAY AWARD A CIVIL PENALTY PURSUANT TO
48 THIS PARAGRAPH WITHOUT A SHOWING OF FINANCIAL LOSS.

49 (B) THE REMEDIES PROVIDED BY THIS SECTION SHALL BE IN ADDITION TO ANY
50 OTHER LAWFUL REMEDY AVAILABLE.

51 (C) NO ACTION MAY BE BROUGHT UNDER THE PROVISIONS OF THIS SECTION
52 UNLESS SUCH ACTION IS COMMENCED WITHIN THREE YEARS IMMEDIATELY AFTER THE
53 DATE OF THE ACT OR OMISSION COMPLAINED OF OR THE DATE OF DISCOVERY OF
54 SUCH ACT OR OMISSION.

55 S 7. Section 208 of the state technology law is amended by adding a
56 new subdivision 9 to read as follows:

1 9. DATA SECURITY REQUIREMENTS. (A) ANY STATE ENTITY THAT OWNS, MAIN-
2 TAINS, OR OTHERWISE POSSESSES PRIVATE INFORMATION SHALL DEVELOP, IMPL-
3 EMENT AND MAINTAIN REASONABLE SAFEGUARDS TO PROTECT THE SECURITY, CONF-
4 DENTIALITY AND INTEGRITY OF THE PRIVATE INFORMATION, INCLUDING DISPOSAL
5 OF DATA.

6 (B) THE FOLLOWING SHALL BE DEEMED TO BE IN COMPLIANCE WITH PARAGRAPH
7 (A) OF THIS SUBDIVISION:

8 (I) A STATE ENTITY THAT COMPLIES WITH A STATE OR FEDERAL LAW PROVIDING
9 GREATER PROTECTION TO PRIVATE INFORMATION THAN THAT PROVIDED BY THIS
10 SECTION;

11 (II) A STATE ENTITY THAT IS SUBJECT TO AND COMPLIES WITH REGULATIONS
12 PROMULGATED PURSUANT TO TITLE V OF THE GRAMM-LEACH-BLILEY ACT OF 1999
13 (15 U.S.C. 6801 TO 6809);

14 (III) A STATE ENTITY THAT COMPLIES WITH THE MOST CURRENT INTERNATIONAL
15 STANDARDS ORGANIZATION STANDARDS FOR INFORMATION SECURITY;

16 (IV) A STATE ENTITY THAT IS SUBJECT TO AND COMPLIES WITH REGULATIONS
17 IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF
18 1996 (45 C.F.R. PARTS 160 AND 164) AND THE HEALTH INFORMATION TECHNOLOGY
19 FOR ECONOMIC AND CLINICAL HEALTH ACT, AS AMENDED FROM TIME TO TIME;

20 (V) A STATE ENTITY THAT COMPLIES WITH CURRENT NATIONAL INSTITUTE OF
21 STANDARDS AND TECHNOLOGY STANDARDS; OR

22 (VI) A STATE ENTITY THAT IMPLEMENTS AN INFORMATION SECURITY PROGRAM
23 THAT INCLUDES THE FOLLOWING:

24 (A) ADMINISTRATIVE SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE
25 STATE ENTITY:

26 (I) DESIGNATES ONE OR MORE EMPLOYEES TO COORDINATE THE SECURITY
27 PROGRAM;

28 (II) IDENTIFIES REASONABLY FORESEEABLE INTERNAL AND EXTERNAL RISKS;

29 (III) ASSESSES THE SUFFICIENCY OF SAFEGUARDS IN PLACE TO CONTROL THE
30 IDENTIFIED RISKS;

31 (IV) TRAINS AND MANAGES EMPLOYEES IN THE SECURITY PROGRAM PRACTICES
32 AND PROCEDURES;

33 (V) SELECTS SERVICE PROVIDERS CAPABLE OF MAINTAINING APPROPRIATE SAFE-
34 GUARDS, AND REQUIRES THOSE SAFEGUARDS BY CONTRACT; AND

35 (VI) ADJUSTS THE SECURITY PROGRAM IN LIGHT OF BUSINESS CHANGES OR NEW
36 CIRCUMSTANCES;

37 (B) TECHNICAL SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE STATE
38 ENTITY:

39 (I) ASSESSES RISKS IN NETWORK AND SOFTWARE DESIGN;

40 (II) ASSESSES RISKS IN INFORMATION PROCESSING, TRANSMISSION AND STOR-
41 AGE;

42 (III) DETECTS, PREVENTS AND RESPONDS TO ATTACKS OR SYSTEM FAILURES;
43 AND

44 (IV) REGULARLY TESTS AND MONITORS THE EFFECTIVENESS OF KEY CONTROLS,
45 SYSTEMS AND PROCEDURES; AND

46 (C) PHYSICAL SAFEGUARDS SUCH AS THE FOLLOWING, IN WHICH THE STATE
47 ENTITY:

48 (I) ASSESSES RISKS OF INFORMATION STORAGE AND DISPOSAL;

49 (II) DETECTS, PREVENTS AND RESPONDS TO INTRUSIONS;

50 (III) PROTECTS AGAINST UNAUTHORIZED ACCESS TO OR USE OF PRIVATE INFOR-
51 MATION DURING OR AFTER THE COLLECTION, TRANSPORTATION AND DESTRUCTION OR
52 DISPOSAL OF THE INFORMATION; AND

53 (IV) DISPOSES OF PRIVATE INFORMATION AFTER IT IS NO LONGER NEEDED FOR
54 BUSINESS PURPOSES OR AS REQUIRED BY LOCAL, STATE OR FEDERAL LAW BY ERAS-
55 ING ELECTRONIC MEDIA SO THAT THE INFORMATION CANNOT BE READ OR RECON-
56 STRUCTED.

1 S 8. This act shall take effect January 1, 2016.