

Amendment No. 858

Assembly Amendment to Senate Bill No. 267 First Reprint (BDR 52-110)

Proposed by: Assemblywoman Kirkpatrick

Amends: Summary: No Title: Yes Preamble: No Joint Sponsorship: No Digest: Yes

ASSEMBLY ACTION			Initial and Date	SENATE ACTION			Initial and Date
Adopted	☐	Lost	☐ _____	Adopted	☐	Lost	☐ _____
Concurred In	☐	Not	☐ _____	Concurred In	☐	Not	☐ _____
Receded	☐	Not	☐ _____	Receded	☐	Not	☐ _____

EXPLANATION: Matter in (1) *blue bold italics* is new language in the original bill; (2) *green bold italic underlining* is new language proposed in this amendment; (3) ~~red strikethrough~~ is deleted language in the original bill; (4) ~~purple double strikethrough~~ is language proposed to be deleted in this amendment; (5) ~~orange double underlining~~ is deleted language in the original bill that is proposed to be retained in this amendment; and (6) *green bold underlining* is newly added transitory language.

JMM/MSN



Date: 5/30/2011

S.B. No. 267—Revises provisions governing personal information. (BDR 52-110)



SENATE BILL NO. 267—SENATOR WIENER

MARCH 18, 2011

Referred to Committee on Commerce, Labor and Energy

SUMMARY—Revises provisions governing personal information. (BDR 52-110)

FISCAL NOTE: Effect on Local Government: No.
Effect on the State: No.

~

EXPLANATION – Matter in ***bolded italics*** is new; matter between brackets ~~omitted material~~ is material to be omitted.

AN ACT relating to personal information; authorizing the Office of Information Security of the Department of Information Technology to adopt certain regulations relating to encryption; revising provisions governing the protection of personal information collected by a data collector; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law prohibits a data collector from moving any data storage device containing personal information beyond the control of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information. (NRS 603A.215) Section 5.5 of this bill authorizes the Office of Information Security of the Department of Information Technology, upon receipt of a well-founded petition, to adopt regulations which identify alternative methods or technologies which may be used by a data collector to encrypt certain data. Section 6 of this bill additionally prohibits a data collector from moving a data storage device which is used by or is a component of a multifunctional device beyond the control of the data collector, its data storage contractor or a person who assumes the obligation of the data collector to protect personal information unless the data collector uses encryption to ensure the security of the information.

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

Section 1. (Deleted by amendment.)

Sec. 2. (Deleted by amendment.)

Sec. 3. (Deleted by amendment.)

Sec. 4. (Deleted by amendment.)

Sec. 5. (Deleted by amendment.)

Sec. 5.5. Chapter 603A of NRS is hereby amended by adding thereto a new section to read as follows:

Upon receipt of a well-founded petition, the Office of Information Security of the Department of Information Technology may, pursuant to chapter 233B of NRS, adopt regulations which identify alternative methods or technologies which may be used to encrypt data pursuant to NRS 603A.215.

1 **Sec. 6.** NRS 603A.215 is hereby amended to read as follows:

2 603A.215 1. If a data collector doing business in this State accepts a
3 payment card in connection with a sale of goods or services, the data collector shall
4 comply with the current version of the Payment Card Industry (PCI) Data Security
5 Standard, as adopted by the PCI Security Standards Council or its successor
6 organization, with respect to those transactions, not later than the date for
7 compliance set forth in the Payment Card Industry (PCI) Data Security Standard or
8 by the PCI Security Standards Council or its successor organization.

9 2. A data collector doing business in this State to whom subsection 1 does not
10 apply shall not:

11 (a) Transfer any personal information through an electronic, nonvoice
12 transmission other than a facsimile to a person outside of the secure system of the
13 data collector unless the data collector uses encryption to ensure the security of
14 electronic transmission; or

15 (b) Move any data storage device containing personal information beyond the
16 logical or physical controls of the data collector, ~~for~~ its data storage contractor *or,*
17 *if the data storage device is used by or is a component of a multifunctional device,*
18 *a person who assumes the obligation of the data collector to protect personal*
19 *information,* unless the data collector uses encryption to ensure the security of the
20 information.

21 3. A data collector shall not be liable for damages for a breach of the security
22 of the system data if:

23 (a) The data collector is in compliance with this section; and

24 (b) The breach is not caused by the gross negligence or intentional misconduct
25 of the data collector, its officers, employees or agents.

26 4. The requirements of this section do not apply to:

27 (a) A telecommunication provider acting solely in the role of conveying the
28 communications of other persons, regardless of the mode of conveyance used,
29 including, without limitation:

30 (1) Optical, wire line and wireless facilities;

31 (2) Analog transmission; and

32 (3) Digital subscriber line transmission, voice over Internet protocol and
33 other digital transmission technology.

34 (b) Data transmission over a secure, private communication channel for:

35 (1) Approval or processing of negotiable instruments, electronic fund
36 transfers or similar payment methods; or

37 (2) Issuance of reports regarding account closures due to fraud, substantial
38 overdrafts, abuse of automatic teller machines or related information regarding a
39 customer.

40 5. As used in this section:

41 (a) "Data storage device" means any device that stores information or data
42 from any electronic or optical medium, including, but not limited to, computers,
43 cellular telephones, magnetic tape, electronic computer drives and optical computer
44 drives, and the medium itself.

45 (b) "Encryption" means the protection of data in electronic or optical form, in
46 storage or in transit, using:

47 (1) An encryption technology that has been adopted by an established
48 standards setting body, including, but not limited to, the Federal Information
49 Processing Standards issued by the National Institute of Standards and Technology,
50 which renders such data indecipherable in the absence of associated cryptographic
51 keys necessary to enable decryption of such data; ~~and~~

52 (2) Appropriate management and safeguards of cryptographic keys to
53 protect the integrity of the encryption using guidelines promulgated by an

1 established standards setting body, including, but not limited to, the National
2 Institute of Standards and Technology. ~~H~~; and

3 (3) Any other technology or method identified by the Office of
4 Information Security of the Department of Information Technology in
5 regulations adopted pursuant to section 5.5 of this act.

6 (c) "Facsimile" means an electronic transmission between two dedicated fax
7 machines using Group 3 or Group 4 digital formats that conform to the
8 International Telecommunications Union T.4 or T.38 standards or computer
9 modems that conform to the International Telecommunications Union T.31 or T.32
10 standards. The term does not include onward transmission to a third device after
11 protocol conversion, including, but not limited to, any data storage device.

12 (d) *"Multifunctional device" means a machine that incorporates the*
13 *functionality of devices, which may include, without limitation, a printer, copier,*
14 *scanner, facsimile machine or electronic mail terminal, to provide for the*
15 *centralized management, distribution or production of documents.*

16 (e) "Payment card" has the meaning ascribed to it in NRS 205.602.

17 ~~(e)~~ (f) "Telecommunication provider" has the meaning ascribed to it in NRS
18 704.027.