

ASSEMBLY BILL NO. 334—ASSEMBLYWOMAN BUCKLEY

MARCH 21, 2005

Referred to Committee on Government Affairs

SUMMARY—Provides for protection of social security numbers and certain other personal information.
(BDR 19-874)

FISCAL NOTE: Effect on Local Government: Increases or Newly Provides for Term of Imprisonment in County or City Jail or Detention Facility.
Effect on the State: Yes.

~

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

AN ACT relating to privacy; requiring a governmental entity, except in certain circumstances, to ensure that social security numbers in its books and records are maintained in a confidential manner; prohibiting the inclusion of social security numbers in certain documents that are recorded, filed or otherwise submitted to a governmental agency; requiring a governmental agency or certain persons who do business in this State that own, license or maintain computerized data to notify certain persons if personal information included in that data was, or is reasonably believed to have been, acquired by an unauthorized person; expanding the types of prohibited computer contaminants to include spyware; requiring the Chief of the Hearings Division of the Department of Administration to adopt regulations to provide for the redaction of personal identifying information of a person filing a claim for certain compensation from certain documents; and providing other matters properly relating thereto.



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

Section 1. Chapter 239 of NRS is hereby amended by adding thereto a new section to read as follows:

Except as otherwise required to carry out a specific statute, a governmental agency shall ensure that the social security number of a person in its books and records is maintained in a confidential manner.

Sec. 2. Chapter 239B of NRS is hereby amended by adding thereto the provisions set forth as sections 3 and 4 of this act.

Sec. 3. 1. *Except as otherwise provided in subsection 2, a person shall not include and a governmental agency shall not require a person to include the social security number of a person on any document that is recorded, filed or otherwise submitted to the governmental agency on or after January 1, 2007.*

2. *If the social security number of a person is required to be included in a document that is recorded, filed or otherwise submitted to a governmental agency on or after January 1, 2007, pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant, a governmental agency shall ensure that the social security number is maintained in a confidential manner and may only disclose the social security number as required:*

(a) To carry out a specific state or federal law; or

(b) For the administration of a public program or an application for a federal or state grant.

3. *A governmental agency shall take necessary measures to ensure that notice of the provisions of this section is provided to persons with whom it conducts business. Such notice may include, without limitation, posting notice in a conspicuous place in each of its offices.*

4. *A governmental agency may require a person who records, files or otherwise submits any document to the governmental agency to provide an affirmation that the document does not contain the social security number of any person. A governmental agency may refuse to record, file or otherwise accept a document which does not contain such an affirmation when required and any document which contains the social security number of a person.*

5. *On or before January 1, 2017, each governmental agency shall ensure that any social security number contained in a document that has been recorded, filed or otherwise submitted to the governmental agency before January 1, 2007, which the governmental agency continues to hold is maintained in a*



1 confidential manner or is obliterated or otherwise removed from
2 the document. Any action taken by a governmental agency
3 pursuant to this subsection must not be construed as affecting the
4 legality of the document.

5 6. As used in this section, "governmental agency" mean an
6 officer, board, commission, department, division, bureau, district
7 or any other unit of government of the State or a local
8 government.

9 Sec. 4. 1. Except as otherwise provided in subsection 4,
10 upon discovery of any breach of the security of any of its computer
11 systems, a governmental agency that:

12 (a) Owns or licenses computerized data that includes personal
13 information shall notify, in the manner set forth in subsection 2,
14 any resident of this State whose personal information included in
15 that data was, or is reasonably believed to have been, acquired by
16 an unauthorized person.

17 (b) Maintains computerized data that includes personal
18 information that the governmental agency does not own shall
19 notify, in the manner set forth in subsection 2, the owner or
20 licensee of the data if the personal information included in that
21 data was, or is reasonably believed to have been, acquired by an
22 unauthorized person.

23 2. Except as otherwise provided in subsection 3, the notice
24 required pursuant to subsection 1 must be provided as soon as
25 practicable, but not less than 30 days after the governmental
26 agency knows or should have known of the breach, by:

27 (a) Written notice;

28 (b) If the notice is consistent with the provisions regarding
29 electronic records and signatures set forth in 15 U.S.C. § 7001,
30 electronic notice; or

31 (c) Any other method established by the governmental agency
32 as part of a policy for the security of its computer systems that
33 provides for notification as soon as practicable, but not less than
34 30 days after the governmental agency knows or should have
35 known of the breach, to the owner or licensee of the data that
36 includes the personal information, or to persons whose personal
37 information included in that data was, or is reasonably believed to
38 have been, acquired by another person.

39 3. If the governmental agency determines that it would have
40 to provide the notice required pursuant to subsection 1 to more
41 than 500,000 persons, if the governmental agency does not have
42 sufficient contact information to provide the notice by the methods
43 described in subsection 2 or if the cost to the governmental agency
44 of providing the notice by the methods described in subsection 2



1 would be more than \$250,000, the governmental agency may
2 provide the notice required pursuant to subsection 1 by:

3 (a) If the governmental agency has an electronic mail address
4 for the owner or licensee of the data containing the personal
5 information, or the person whose personal information was, or is
6 reasonably believed to have been, acquired by another person,
7 electronic mail;

8 (b) If the governmental agency maintains an Internet website,
9 posting the notice in a conspicuous place on its Internet website;
10 and

11 (c) Any statewide publication or broadcast.

12 4. If a law enforcement agency determines that the notice
13 required pursuant to subsection 1 may impede a criminal
14 investigation, the governmental agency shall delay such notice
15 until the law enforcement agency determines that the notice will
16 not compromise the criminal investigation.

17 5. A person who has suffered injury as the proximate result
18 of a violation of this section may commence an action against the
19 governmental agency for the recovery of his actual damages, costs
20 and reasonable attorney's fees, subject to any applicable
21 limitations set forth in NRS 41.0305 to 41.039, inclusive. An
22 action described in this subsection must be commenced not later
23 than 2 years after the person who suffered the injury discovers the
24 facts constituting the violation of this section.

25 6. As used in this section:

26 (a) "Governmental agency" means an officer, board,
27 commission, department, division, bureau, district or any other
28 unit of government of the State or a local government.

29 (b) "Personal information" means the name of a person and
30 one or more of the following types of information:

31 (1) The social security number of the person.

32 (2) The driver's license number or identification card
33 number of the person.

34 (3) The bank account number, credit card number or debit
35 card number of the person in combination with any required
36 security code, access code or password that would allow access to
37 the related account or other personal information of the person.

38 **Sec. 5.** NRS 205.4737 is hereby amended to read as follows:

39 205.4737 1. "Computer contaminant" means any data,
40 information, image, program, signal or sound that is designed or has
41 the capability to:

42 (a) Contaminate, corrupt, consume, damage, destroy, disrupt,
43 modify, record or transmit; or

44 (b) Cause to be contaminated, corrupted, consumed, damaged,
45 destroyed, disrupted, modified, recorded or transmitted,



1 ↳ any other data, information, image, program, signal or sound
2 contained in a computer, system or network without the knowledge
3 or consent of the person who owns the other data, information,
4 image, program, signal or sound or the computer, system or
5 network.

6 2. The term includes, without limitation:

7 (a) A virus, worm or Trojan horse; ~~to~~

8 (b) *Spyware that tracks computer activity and is capable of*
9 *recording and transmitting such information to third parties; or*

10 (c) Any other similar data, information, image, program, signal
11 or sound that is designed or has the capability to prevent, impede,
12 delay or disrupt the normal operation or use of any component,
13 device, equipment, system or network.

14 **Sec. 6.** Chapter 603 of NRS is hereby amended by adding
15 thereto a new section to read as follows:

16 1. *Except as otherwise provided in subsections 4 and 6, upon*
17 *discovery of any breach of the security of his computer system, a*
18 *person doing business in this State that:*

19 (a) *Owns or licenses computerized data that includes personal*
20 *information shall notify, in the manner set forth in subsection 2,*
21 *any resident of this State whose personal information contained in*
22 *that data was, or is reasonably believed to have been, acquired by*
23 *an unauthorized person.*

24 (b) *Maintains computerized data that includes personalized*
25 *information that the person doing business in this State does not*
26 *own shall notify, in the manner set forth in subsection 2, the*
27 *owner or licensee of the data if personal information contained in*
28 *that data was, or is reasonably believed to have been, acquired by*
29 *an unauthorized person.*

30 2. *Except as otherwise provided in subsection 3, the notice*
31 *required pursuant to subsection 1 must be provided as soon as*
32 *practicable, but not less than 30 days after the governmental*
33 *agency knows or should have known of the breach, by:*

34 (a) *Written notice;*

35 (b) *If the notice is consistent with the provisions regarding*
36 *electronic records and signatures set forth in 15 U.S.C. § 7001,*
37 *electronic notice; or*

38 (c) *Any other method established by the person doing business*
39 *in this State as part of a policy for the security of his computer*
40 *system that provides for notification as soon as practicable, but not*
41 *less than 30 days after the governmental agency knows or should*
42 *have known of the breach, to the owner or licensee of the data*
43 *containing the personal information and to persons whose*
44 *personal information was, or is reasonably believed to have been,*
45 *acquired by another person.*



1 3. If the person doing business in this State determines that
2 he would have to provide the notice required pursuant to
3 subsection 1 to more than 500,000 persons, the person does not
4 have sufficient contact information to provide the notice by the
5 methods described in subsection 2 or the cost of providing the
6 notice by the methods described in subsection 2 would be more
7 than \$250,000, the person doing business in this State may provide
8 the notice required pursuant to subsection 1 by:

9 (a) If the person doing business in this State has an electronic
10 mail address for the owner or licensee of the information, or the
11 person whose personal information was, or is reasonably believed
12 to have been, acquired by another person, electronic mail;

13 (b) If the person doing business in this State maintains an
14 Internet website, posting the notice in a conspicuous place on his
15 Internet website; and

16 (c) Any statewide publication or broadcast.

17 4. If a law enforcement agency determines that the notice
18 required pursuant to subsection 1 may impede a criminal
19 investigation, the person doing business in this State shall delay
20 such notice until the law enforcement agency determines that the
21 notice will not compromise the criminal investigation.

22 5. In addition to the notification required pursuant to
23 subsection 1, if a person doing business in this State determines
24 that he must provide such notification to more than 1,000 persons
25 as a result of the breach, the person doing business in this State
26 must, without unreasonable delay, inform each consumer
27 reporting agency, as defined in 15 U.S.C. § 1681a(p), in writing, of
28 the timing, distribution and contents of that notification.

29 6. The provisions of this section do not apply to any person
30 doing business in this State that is subject to the provisions of the
31 Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et. seq., or any
32 regulations adopted pursuant thereto.

33 7. A person who has suffered injury as the proximate result
34 of a violation of this section may commence an action against the
35 person doing business in this State for the recovery of his actual
36 damages, costs and reasonable attorney's fees and, if the violation
37 of this section was willful or intentional, for any punitive damages
38 that the facts may warrant. An action described in this subsection
39 must be commenced not later than 2 years after the person who
40 suffered the injury discovers the facts constituting the violation of
41 this section.

42 8. As used in this section, "personal information" means the
43 name of a person and one or more of the following types of
44 information:

45 (a) The social security number of the person.



1 ***(b) The driver's license number or identification card number***
2 ***of the person.***

3 ***(c) The bank account number, credit card number or debit***
4 ***card number of the person in combination with any required***
5 ***security code, access code or password that would allow access to***
6 ***the related account or other personal information of the person.***

7 **Sec. 7.** NRS 616C.310 is hereby amended to read as follows:
8 616C.310 1. The Chief of the Hearings Division of the
9 Department of Administration:

10 (a) May by regulation provide for specific procedures for the
11 determination of contested cases.

12 (b) Shall develop a format to be used by hearing officers to
13 indicate their findings in contested cases.

14 ***(c) Shall adopt regulations to provide for the redaction of***
15 ***personal identifying information of a person filing a claim for***
16 ***compensation from a document relating to the contested case of***
17 ***the person, unless the identity of the person is at issue. As used in***
18 ***this paragraph, "personal identifying information" means any***
19 ***information which would identify a person, including, without***
20 ***limitation, an address, a birth date or a social security number.***

21 2. An insurer or employer may be represented in a contested
22 case by private legal counsel or by any other agent.

23 **Sec. 8.** This act becomes effective on January 1, 2007.



