Assembly Bill No. 334–Assemblywoman Buckley

CHAPTER.....

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

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

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

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

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

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

(a) Written notice;

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

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

3. If the governmental agency determines that it would have to provide the notice required pursuant to subsection 1 to more than 500,000 persons, if the governmental agency does not have sufficient contact information to provide the notice by the methods described in subsection 2 or if the cost to the governmental agency of providing the notice by the methods described in subsection 2 would be more than $250,000, the governmental agency may provide the notice required pursuant to subsection 1 by:

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

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

(c) Any statewide publication or broadcast.

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

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

6. As used in this section:

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

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

(1) The social security number of the person.

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

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

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

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

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

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

➥ any other data, information, image, program, signal or sound contained in a computer, system or network without the knowledge or consent of the person who owns the other data, information, image, program, signal or sound or the computer, system or network.

2. The term includes, without limitation:

(a) A virus, worm or Trojan horse; ~~[or]~~

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

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

3. As used in this section:

(a) "On-line bidding" has the meaning ascribed to it in NRS 332.047.

(b) "Spyware" does not include:

(1) An Internet browser;

(2) Software for transmitting messages instantly that informs the user whether other users are on-line at the same time;

(3) Software that is designed to detect or prevent the use of computer contaminants;

(4) Software that is designed to detect fraudulent on-line bidding;

(5) Software that is designed to prevent children from accessing pornography on the Internet;

(6) Software that conducts remote maintenance or repair of a computer or its systems;

(7) Software that is designed to manage or to perform maintenance on a network of computers;

(8) Software for media players; and

(9) Software that authenticates a user.

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

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

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

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

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

(a) Written notice;

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

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

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

(a) If the person doing business in this State has an electronic mail address for the owner or licensee of the information, or the

person whose personal information was, or is reasonably believed to have been, acquired by another person, electronic mail;

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

(c) Any statewide publication or broadcast.

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

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

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

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

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

(a) The social security number of the person.

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

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

Sec. 7. NRS 616C.310 is hereby amended to read as follows:

616C.310 1. The Chief of the Hearings Division of the Department of Administration:

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

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

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

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

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