**Sen. Daniel Biss**

# Filed: 4/17/2015



AMENDMENT TO SENATE BILL 1833

AMENDMENT NO. _____. Amend Senate Bill 1833 by replacing everything after the enacting clause with the following:

"Section 5. The Personal Information Protection Act is amended by changing Sections 5 and 10 and by adding Sections 45 and 50 as follows:

(815 ILCS 530/5)

Sec. 5. Definitions. In this Act:

"Data Collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

"Breach of the security of the system data" or "breach" means unauthorized acquisition of computerized data that

compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

"Consumer marketing information" means information related to a consumer's online browsing history, online search history, or purchasing history.

"Geolocation information" means information generated or derived from the operation or use of an electronic communications device that is sufficient to identify the street name and name of the city or town in which the device is located. "Geolocation information" does not include the contents of an electronic communication.

"Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's health insurance application and claims history, including any appeals records.

"Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional,

including health information provided to a website or mobile application.

"Personal information" means either of the following:

(1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

(A) ~~(1)~~ Social Security number.

(B) ~~(2)~~ Driver's license number or State identification card number.

(C) ~~(3)~~ Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(F) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

(G) Geolocation information.

(H) Consumer marketing information.

(I) Any 2 of the following data elements:

(i) home address, telephone number, or email address;

(ii) mother's maiden name;

(iii) month, day, and year of birth.

(2) user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

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

(Source: P.A. 97-483, eff. 1-1-12.)

(815 ILCS 530/10)

Sec. 10. Notice of Breach.

(a) Any data collector that owns or licenses personal information, excluding geolocation information and consumer marketing information, concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall

be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

(1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information":

(A) ~~(i)~~ the toll-free numbers and addresses for consumer reporting agencies; ~~,~~

(B) ~~(ii)~~ the toll-free number, address, and website address for the Federal Trade Commission; ~~,~~ and

(C) ~~(iii)~~ a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her username or password and security question or answer, as applicable, or to take other steps appropriate to protect

all online accounts for which the resident uses the same user name or email address and password or security question and answer.

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

(b-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data

collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.

(d) Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

(e) Notice to Attorney General.

(1) Any data collector that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents shall provide notice to the Attorney General of the breach, including:

(A) A description of the personal information compromised in the breach.

(B) The number of Illinois residents affected by such incident at the time of notification.

(C) Any steps the data collector has taken or plans to take relating to notification of the breach to consumers.

(D) The date and timeframe of the breach, if known at the time notification is provided.

Such notification must be made within 30 business days of the data collector's discovery of the security breach or

2 days before the data collector provides any notice to consumers required by this Section, whichever is sooner, unless the data collector has good cause for reasonable delay to determine the scope of the breach and restore the integrity, security, and confidentiality of the data system, or when law enforcement requests in writing to withhold disclosure of some or all of the information required in the notification under this Section. If the date or timeframe of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date or timeframe of the breach as soon as possible.

(2) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents shall notify the Attorney General of the following:

(A) A description of the personal information compromised in the breach.

(B) The number of Illinois residents affected by such incident at the time of notification.

(C) Any steps the data collector has taken or plans to take relating to notification of the owner or licensee of the breach and what measures, if any, the data collector has taken to notify Illinois residents.

(D) The date and timeframe of the breach, if known at the time notification is provided.

Such notification must be made within 30 business days of the data collector's discovery of the security breach or when the data collector provides notice to the owner or licensee of the information pursuant to this Section, whichever is sooner, unless the data collector has good cause for reasonable delay to determine the scope of the breach and restore the integrity, security, and confidentiality of the data system, or when law enforcement requests in writing to withhold disclosure of some or all of the information required in the notification under this Section. If the date or timeframe of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date or timeframe of the breach as soon as possible.

(f) A data collector that suffers a breach subject to the breach notification standards established pursuant to the federal Health Information Technology Act, 42 U.S.C. Section 17932, shall be deemed to be in compliance with the provisions of this Section if that data collector does the following: (1) provides notification to individuals in compliance with the federal Health Information Technology Act and implementing regulations and (2) provides notification to the Attorney General pursuant to subsection (e).

(Source: P.A. 97-483, eff. 1-1-12.)

(815 ILCS 530/45 new)

Sec. 45. Data security.

(a) A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

(b) A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

(c) If a state or federal law requires a data collector to provide greater protection to records that contain personal information concerning an Illinois resident that are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this Section.

(d) A data collector that is subject to and in compliance with the security standards for the protection of electronic health information, 45 C.F.R. Parts 160 and 164, established

pursuant to the federal Health Insurance Portability and Accountability Act of 1996 shall be deemed to be in compliance with the provisions of this Section.

(e) A data collector that is subject to and in compliance with the standards established pursuant to Section 501(b) of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801, shall be deemed to be in compliance with the provisions of this Section.

(815 ILCS 530/50 new)

Sec. 50. Posting of privacy policy.

(a) As used in this Section:

"Conspicuously post" means posting the privacy policy through any of the following:

(1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site.

(2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word "privacy". The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.

(3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is

located on the homepage or first significant page after entering the Web site, and if the text link does one of the following:

(A) Includes the word "privacy".

(B) Is written in capital letters equal to or greater in size than the surrounding text.

(C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.

(4) Any other functional hyperlink that is displayed in a noticeable manner.

(5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for a consumer of the online service.

"Operator" means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personal information from a consumer residing in Illinois who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner.

(b) An operator of a commercial Web site or online service

that collects personal information through the Internet about individual consumers residing in Illinois who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site or online service. An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.

(c) The privacy policy required by subsection (b) shall, at a minimum, do the following:

(1) Identify the categories of personal information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personal information.

(2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personal information that is collected through the Web site or online service, provide a description of that process.

(3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.

(4) Identify its effective date.

(5) Disclose how the operator responds to Web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personal information about an individual consumer's online activities over time and across third-party Web sites or online services, if the operator engages in that collection.

(6) Disclose whether other parties may collect personal information about an individual consumer's online activities over time and across different Web sites or online services when a consumer uses the operator's Web site or online service.

An operator may satisfy the requirement of paragraph (5) by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice.".