WHITE & CASE

Articles

Developments in Data Privacy Legislation

November 2011
Technology Newsflash
Daren M. Orzechowski, Allison M. Dodd, Imtiaz Yakub

Technology Newsflash

On September 15, 2011, the Obama administration renewed its calls for comprehensive data privacy legislation which would establish basic online data protection guidelines. These policy statements were made during a hearing held by the Subcommittee on Commerce, Manufacturing, and Trade concerning the impact of the European Union's (EU) privacy and data collection regulations on the Internet economy.[1] The U.S. Department of Commerce stated that the current lack of a baseline privacy framework is hurting the competitiveness of American companies in the global marketplace, and urged the development of data privacy legislation. According to the U.S. Department of Commerce, although many American companies currently rely on the U.S.-E.U. Safe Harbor Framework[2], this framework is too inflexible, and therefore, data privacy legislation needs to be implemented in the U.S. that is flexible enough to adapt to rapidly changing technologies.[3]

A number of data privacy bills have already been introduced in Congress in recent months, such as the Commercial Privacy Bill of Rights legislation introduced by Senators John Kerry and John McCain[4], which was discussed in our previous posting, and the Personal Data Privacy and Security Act ("PDPSA"), the most recent version of which was introduced by Senator Patrick Leahy (D-Vt.) on June 7, 2011.[5] The Senate Judiciary Committee, on September 22, 2011, approved an amended version of the PDPSA, along with amended versions of two other breach notification bills: (1) The Data Breach Notification Act of 2011, introduced by Senator Dianne Feinstein (D-CA) (the "Feinstein Proposal");[6] and (2) The Personal Data Protection and Breach Accountability Act of 2011, introduced by Senator Richard Blumenthal (D-CT) (the "Blumenthal Proposal").[7] Each of the three bills, summarized in more detail in this posting, if passed, would (with some limited exceptions) replace state data breach notification laws in lieu of a federal standard that requires notification to individuals be provided where a breach results in, or is reasonably likely to result in, the unauthorized access or acquisition of sensitive personally identifiable information ("SPII"). In short, the legislators recognize that the United States is in need of a significant update to its privacy and data protection laws.

The Personal Data Privacy and Security Act

The PDPSA, if implemented, would require (1) business entities that are engaged in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of SPII[8] in electronic or digital form on 10,000 or more U.S. residents to implement a comprehensive personal data privacy and security program to safeguard such SPII (the "Data Security Section");[9] and (2) federal agencies and business entities that are engaged in interstate commerce that involves using, accessing, transmitting, storing, disposing of or collecting SPII to notify any U.S. resident whose SPII has been or is reasonably believed to have been accessed or acquired following the entity's discovery of a security breach[10] of such SPII (the "Security Breach Notification Section").[11] These provisions would not apply to (1) financial institutions that are subject to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.); and (2) entities that are regulated by the data security requirements of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1301 et seq., "HIPAA"), including business associates in compliance with the applicable HIPAA requirements.[12] The Data Security Section specifically excludes service providers of third party electronic communications that are exclusively engaged in the transmission, routing or temporary storage of the communications.[13] Service providers[14] that become aware of security breaches containing SPII of another business entity, however, are required to notify the business entity if it can be reasonably identified.[15] The PDPSA also contains proposed amendments to the Computer Fraud and Abuse Act, which would increase penalties and narrow the scope of actionable violations to exclude technical violations such as violations of acceptable use policies or terms of

use. The amended version of the PDPSA no longer includes a provision from the original bill that would have imposed additional privacy requirements on "data brokers,"[17] including giving consumers the opportunity to access and correct their personal information held by data brokers.[18]

Data Security Section

Under the Data Security Section, a qualifying business entity would be required to implement a comprehensive personal data privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the business entity and the nature and scope of its activities.[19] The PDPSA specifies that this data security program should be designed to ensure the confidentiality, security and privacy of SPII and protect against any identified entity-specific risks, anticipated vulnerabilities in SPII security and unauthorized access of SPII that could create a significant risk of harm to an individual.[20] It further provides that qualifying business entities should conduct regular employee training, systems and procedural vulnerability testing, and should periodically assess their program and adjust it as appropriate in light of changes in technology, risks, or the nature of the SPII or business entity.[21] Qualifying business entities would also be required to adopt measures that (1) control access to systems containing SPII; (2) detect, record, and preserve information concerning unauthorized access or alteration of SPII and trace access to records so that the business entity can determine who accessed SPII records; (3) protect SPII during transmission, storage, disposal or other use through widely accepted industry practices, including encryption or redaction; (4) ensure that no third party is authorized to access SPII unless the business entity has performed sufficient due diligence to determine with reasonable certainty that the third party seeks the SPII for a valid legal purpose, and that third party is required by contract to implement its own data privacy and security program; and (5) ensure the proper destruction and disposal of SPII.[22]

Violators who fail to meet these requirements may be subject to civil penalties of up to $5,000 per violation per day while such a violation exists, with a maximum of $500,000 for each violation and for all violations resulting from the same or related acts.[23] Additionally, if a court determines that such violations were intentional or willful, the court may impose an additional penalty of up to $500,000.[24] The Data Security Section excludes any private right of action, and instead authorizes the FTC to enforce the Data Security Section of the PDPSA.[25] The Data Security Section, however, authorizes state attorney generals to bring civil actions for violations that threaten or adversely affect an interest of the residents of that state.[26] The Data Security Section does not allow for simultaneous enforcement for violations by the FTC and a state attorney general, and in the event of a conflict, the FTC's enforcement powers take precedence over those of the state attorney general.[27] The Data Security Section preempts state laws, but specifically does not amend or supplant the Gramm-Leach-Bliley Act or HIPAA.[28]

Security Breach Notification Section

Under the Security Breach Notification Section, any business entity or federal agency that uses, accesses, transmits, stores, disposes of or collects SPII in interstate commerce must notify individuals whose SPII is compromised by a security breach, "without unreasonable delay,"[29] which in any case must be within 60 days following the discovery of the security breach, unless an extension is granted by the FTC, or the U.S. Secret Service or the Federal Bureau of Investigation determines that the notification would impede a criminal investigation or a national security activity.[30] The business entity or federal agency must also notify the owner or licensee of the information.[31] If the owner or licensee provides the required notice to the person who is the subject of the SPII, the business entity is relieved from its obligation to provide what would be a duplicative notice.[32] This exemption, however, does not apply to federal agencies.[33]

The Security Breach Notification Section does not require that individuals be notified of all security breaches to a system.[34] If a risk assessment by the business entity or federal agency determines that there is no significant risk that a security breach has resulted in or will result in identify theft, or economic or physical harm, the results of the risk assessment are provided to the FTC in writing within 45 days of discovery of the security breach, and the FTC does not disagree with the assessment within 10 business days, the entity will be exempt from the notice requirement.[35] This safe harbor provision also establishes a rebuttable presumption that a security breach would not be considered a significant risk if the SPII is encrypted or rendered unreadable.[36]

Security breach notifications may be made by mail, telephone, email or through a major media outlet if the security breach affects more than 5,000 individuals in a jurisdiction.[37] These notices must contain a description of the categories of SPII that was accessed without authorization, a toll free number of the business entity or federal agency for use by individuals to request the types of SPII being maintained about them, and the toll free numbers and addresses of the major credit reporting agencies.[38]

Violators under the Data Breach Notification Section would be subject to civil penalties of up to $11,000 per violation per day, with a maximum of $1,000,000 for all violations resulting from the same or related act,[39] and both the U.S. Attorney General and the FTC would be authorized to bring civil actions for violations.[40] The FTC would be able to enforce violations as unfair or deceptive acts under the FTC Act.[41] However, the FTC would not be allowed to initiate an investigation if the U.S. Attorney General determines that such an investigation would impede an ongoing criminal investigation or national security activity.[42] State attorney generals could also bring civil actions for violations that threaten or adversely affect an interest of the residents of that state.[43] The Security Breach Notification Section does not allow for simultaneous enforcement for violations by the U.S. Attorney General and a state attorney general, and in the event of a conflict, the U.S. Attorney General's enforcement powers take precedence over those of the state attorney general.[44] The Security Breach Notification Section preempts all state and federal laws other than GLBA and HIPAA; provided, however, that state authority is reserved to additionally require that notices include information regarding victim assistance protection offered by the state.[45]

Senator Feinstein's and Senator Blumenthal's Proposed Security Breach Notification Bills

Unlike the data security provisions contained in the PDPSA, the Feinstein Proposal contains no data security protections similar to those included in the Data Security Section of the PDPSA and is instead limited to data breach notification requirements. The Feinstein Proposal's data breach notification provisions are almost identical to those of the PDPSA, and the Feinstein Proposal also contains similar safe harbor mechanisms, including an exemption from the notification requirement where a risk assessment establishes that there is no significant risk of harm to individuals.[46] The Feinstein Proposal does not grant enforcement authority to the FTC, and only the U.S. Attorney General or state attorney generals may bring civil actions for violations, with a maximum civil penalty of $1,000,000 for all violations resulting from the same or related acts, and an additional maximum limit of $1,000,000 if the violation was intentional or willful.[47]

The Blumenthal Proposal shares many similarities with the PDPSA and the Feinstein Proposal, including the safe harbor mechanisms found in both other bills.[48] The Blumenthal Proposal, however, is far more extensive than the other two proposed bills and reflects several key differences. The definition of SPII in the Blumenthal Proposal, unlike the other two bills, includes geo-location information obtained through use of a mobile device and "information regarding an individual's medical history, mental or physical medical condition, or medical treatment or diagnosis by a health care professional."[49] The Blumenthal Proposal thus would act as a gap-filler for entities that are not regulated as "covered entities" or "business associates" under HIPAA, but which otherwise handle medical information. The FTC would also have the authority to modify the definition of SPII through rulemaking in the future.[50] The Blumenthal Proposal addresses oversight of federal contracts with data brokers, a provision which was stripped from the PDPSA through the amendments approved on September 22.[51]

The Blumenthal Proposal reflects a significant departure from the other two proposals in respect of penalties for violations. It is the only proposed bill that grants individuals the right to bring a private cause of action against a business entity to recover for personal injuries sustained as a result of violations of the bill.[52] In such cases, a court could grant damages of up to $500 per day per individual up to a maximum of $20,000,000 in addition to punitive damages if the violation was intentional or willful.[53] The Blumenthal Proposal would also restrict the ability of businesses to enforce arbitration clauses related to the individual's right to bring a private cause of action.[54] In addition, the U.S. Attorney General, FTC or state attorney generals may also bring a civil suit against violators, with penalties of up to $500 per day per individual up to a maximum of $20,000,000.[55] Therefore, in comparison to the other two bills, the penalties contained in the Blumenthal Proposal would substantially increase the cost of non-compliance.

All three bills have been reported to the Senate floor and are currently awaiting placement on the Senate's Legislative Calendar to be brought before the full Senate for consideration.

---

1 - *Internet Privacy: The Impact and Burden of EU Regulation Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Energy and Commerce Comm.*, 112th Cong. (Sept. 15, 2011) (testimony of Hon. Nicole Lamb-Hale, Asst. Secretary, Int'l Trade Administration), energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=8905.

2 - The U.S.- EU Safe Harbor Framework is a data protection certification registry under which U.S. companies can transfer personally identifiable information outside of the European Union in compliance with the EU Data Protection Directive (95/46/EC) if they voluntarily commit to comply with EU privacy requirements. European Union Directive 95/46/EC of the European Parliament and of the Council, 1995 O.J. (L 281) 31.

3 - Testimony of Hon. N. Lamb-Hale, *supra* note 1.

4 - A bill to establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, and for other purposes, or the Commercial Privacy Bill of Rights Act of 2011, S.799, 112th Cong. (Apr. 12, 2011).

5 - A bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information, or the Personal Data Privacy and Security Act of 2011, S.1151, 112th Cong. (as approved by the Senate Judiciary Committee, Sept. 22, 2011).

6 - A bill to require federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information, or the Data Breach Notification Act of 2011, S.1408, 112th Cong. (as approved by the Senate Judiciary Committee, Sept. 22, 2011).

7 - A bill to protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information, or the Personal Data Protection and Breach Accountability Act of 2011, S.1535, 112th Cong. (as approved by the Senate Judiciary Committee, Sept. 22, 2011).

8 - The term "sensitive personally identifiable information" means "any information or compilation of information, in electronic or digital form that includes the following: (A) an individual's first and last name or first initial and last name in combination with any two of the following data elements: (i) home address or telephone number, (ii) mother's maiden name, (iii) Month, day, and year of birth; (B) A non-truncated social security number, driver's license number, passport number, or alien registration number or other government-issued unique identification number; (C) unique biometric data such as a fingerprint, voice print, a retina or iris image, or any other unique physical representation; (D) a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; (E) any combination of the following data elements: (i) An individual's first and last name or first initial and last name, (ii) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code, (iii) any security code, access code, or password, or source code that could be used to generate such codes or passwords." *Id.* at § 3(a)(11).

9 - *Id.* at §§ 201, 202.

10 - "Security breach" is defined as a "compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that result[s] in, or that there is a reasonable basis to conclude has resulted in (i) the unauthorized acquisition of [SPII]; and (ii) access to [SPII] that is for an unauthorized purpose, or in excess of authorization." Excluded from this definition are (i) good faith acquisitions of SPII by entities if the SPII is not subject to further unauthorized disclosure; (ii) the release of a public record or information obtained from a public record; and (iii) lawfully authorized activities of law enforcement or intelligence agencies. *Id.* at § 3(a)(11).

11 - *Id.* at § 211.

12 - *Id.* at §§ 201(c), 211(e).

13 - *Id.* at §§ 201(c)(3).

14 - The term "service provider" means a business entity that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the business entity providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and the business entity transmits, routes, stores, or provides connections for personal information in a manner that personal information is undifferentiated from other types of data that such business entity transmits, routes, stores, or provides connections. Any such business entity is treated as a service provider only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage or connections. *Id.* at § 3(a)(13).

15 - *Id.* at §§ 211(b)(4).

16 - *Id.* at Title 1.

17 - The term "data broker" means a business entity which for monetary fees or dues regularly engages in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to non-affiliated third parties on an interstate basis. Unamended PDPSA at § 3(5), leahy.senate.gov/imo/media/doc/BillText-PersonalDataPrivacyAndSecurityAct.pdf

18 - *Id.* at § 201.

19 - PDPSA, *supra* note 5 at §§ 201, 202.

20 - *Id.*

21 - *Id.*

22 - *Id.*

23 - *Id.* at § 203(a), as amended by Amendment ALB11713, judiciary.senate.gov/legislation/upload/Leahy-Manager-s-ALB11713.pdf.

24 - *Id.*

25 - *Id.* at § 203(b), (d).

26 - *Id.* at § 203(c).

27 - *Id.* at § 203(c)(3).

28 - *Id.* at § 204(b).

29 - Reasonable delay includes time necessary to determine the extent of the breach, conduct risk assessments, prevent further disclosures, restore the reasonable integrity of the data system, and provide notice to law enforcement when required. *Id.* at § 204(c)(2).

30 - *Id.* at §§ 212(a), (c), (d).

31 - *Id.* at § 211(b)(1).

32 - *Id.* at § 211(b)(3).

33 - *Id.*

34 - *Id.* at § 212(b)(1).

35 - *Id.*

36 - *Id.* at § 212(b)(2).

37 - *Id.* at § 213. If the business entity or Federal agency is required to provide notice to more than 5,000 individuals, it will also have to notify all national consumer reporting agencies. *Id.* at § 215. Furthermore, if a security breach: (1) affects more than 5,000 individuals; (2) involves a database containing the SPII of more than 500,000 individuals nationwide; (3) involves databases owned by the Federal Government or; (4) primarily SPII of Federal Government employees or contractors involved in national security or law enforcement, the business entity or Federal agency would be required to notify a Federal Government entity to be designated by the Department of Homeland Security. *Id.* at § 216(b).

38 - *Id.* at § 214(a)(2).

39 - *Id.* at § 217(b), as amended by Amendment ALB11713, judiciary.senate.gov/legislation/upload/Leahy-Manager-s-ALB11713.pdf.

40 - *Id.* at § 217(a).

41 - Federal Trade Commission Act, § 5, 15 U.S.C. § 45 (2006); PDPSA, *supra* note 5 at § 217(d).

42 - PDPSA, *supra* note 5 at § 217(e).

43 - *Id.* at § 218(a).

44 - *Id.* at § 218(b).

45 - *Id.* at § 219.

46 - Feinstein Proposal, *supra* note 6 at § 3(b).

47 - *Id.* at §§ 8, 9.

48 - Blumenthal Proposal, *supra* note 7 at §212(b)(1).

49 - *Id.* at § 3(a)(15).

50 - *Id.* at § 3(b).

51 - *Id.* at § 301.

52 - *Id.* at § 220.

53 - *Id.* at § 220(c).

54 - *Id.* at § 220(e).

55 - *Id.* at §§ 218, 219.
