JONES DAY

COMMENTARY

PROTECTING SOCIAL SECURITY NUMBERS: FEDERAL LEGISLATION IN SIGHT

Privacy remains a top issue in today's faltering economy. On January 6, 2009, the first day of the 111th Congress, Senator Dianne Feinstein (D–CA) reintroduced a bill, "Protecting the Privacy of Social Security Numbers Act" (the "Bill"),[1] to safeguard Social Security numbers ("SSNs"). Various versions of this bipartisan measure, cosponsored by Senators Judd Gregg (R–NH) and Olympia Snowe (R–ME), have been introduced in every Congress since 2002. However, unlike past attempts, the Senate Judiciary Committee is expected to approve the bill, and the new Congress may be poised to pass it. In preparation for federal legislation in this area, companies should begin to review and update their data protection policies.

THE BILL

The current proposal would amend Title 18 of the United States Code to prohibit the sale or display of SSNs to the general public without an individual's consent. Along with related data breach bills,[2] the Bill is intended to curb the growing epidemic of identity theft or identity fraud[3] by making it harder for criminals to steal SSNs. It further requires government agencies, including the Federal Trade Commission ("FTC"), to take steps to protect SSNs from being displayed or accessed without consent.

The Bill covers "any individual, partnership, corporation, trust, estate, cooperative, association, or any other entity."[4] If passed, the legislation would:

- Prohibit the sale, purchase, or display of an SSN by any person without the SSN holder's consent.
- Restrict the display of SSNs on public records in printed or electronic form.
- Limit circumstances where businesses could ask customers for SSNs.
- Restrict incarcerated persons from employment that would give them access to SSNs.

The Bill would permit business and government uses of SSNs in limited circumstances, such as for credit checks, law enforcement, public health, and other purposes authorized under federal law. It also would impose harsh punishment on entities and individuals who misuse SSNs. Violators will face a variety of civil and criminal penalties, while victims will receive a private right of action for injunctive relief and actual or statutory damages of up to $500 per violation.[5]

WHY PASSAGE IS POSSIBLE

Since its inception in 1936 for tracking contributions to the Social Security system, the SSN has proliferated in use. At the moment, public and private entities use SSNs for a wide range of non-Social Security purposes, such as in employee files, medical records, health insurance accounts, credit and banking accounts, university identification cards, utility accounts, etc., partially because such entities assume that no one but the person to whom the SSN was issued will know the unique identifying number. These uses of SSNs as a de facto identifier or authenticator make the numbers highly desirable to identity thieves. Advancing technology has also raised the stakes in protecting SSNs stored in electronic form since security breaches may expose millions of people to misuse of their SSNs.

A notable instance of identity fraud occurred in 2006 when a commercial data broker that compiles personal and financial information, including SSNs, for sale to government agencies and private companies allegedly sold or leaked personal data relating to approximately 163,000 consumers to a crime ring. The company paid $15 million to settle FTC charges that it failed to protect consumer personal information. The incident also triggered a flurry of data loss disclosures from an assortment of corporations and other organizations that affected more than 50 million Americans.

Washington's concern over identity theft has intensified in recent years. After the above incident, Congress announced a number of hearings and proposals for combating identity theft, calling it an economy-wide problem. President Bush created an Identity Theft Task Force that, among other actions, encouraged an extensive FTC investigation. In December 2008, the FTC reported that annual victims of identity theft numbered in the millions and out-of-pocket losses, primarily to businesses, amounted to billions of dollars. The agency's principal recommendation was that Congress establish national standards for data protection and breach notification, including requiring all businesses to authenticate customers without using SSNs.

EXISTING LEGAL LANDSCAPE

Although several federal laws, including the Fair Credit Reporting Act,[6] the Health Insurance Portability and Accountability Act,[7] and the Gramm-Leach-Bliley Act,[8] have imposed privacy and security requirements on use and disclosure of SSNs, states continue to be at the forefront of data security legislation in this area.

An increasing number of states actively regulate how and when organizations must protect personal information. The following states have adopted laws restricting or prohibiting the collection, use, or disclosure of SSNs by private entities:

Alaska[9]	Maine[20]	Oklahoma[31]
Arizona[10]	Maryland[21]	Ohio[32]
Arkansas[11]	Massachusetts[22]	Oregon[33]
California[12]	Michigan[23]	Pennsylvania[34]
Colorado[13]	Minnesota[24]	Rhode Island[35]
Connecticut[14]	Missouri[25]	South Carolina[36]
Georgia[15]	Nebraska[26]	Tennessee[37]
Hawaii[16]	New Jersey[27]	Texas[38]
Idaho[17]	New Mexico[28]	Utah[38]
Illinois[18]	New York[29]	Vermont[40]
Kansas[19]	North Carolina[30]	Virginia[41]

These laws generally prohibit use of SSNs in a manner that provides public view or access, although many state laws provide exemptions for entities covered by federal legislation. These state laws vary in scope and the extent to which organizations must maintain the security of SSNs.

At least six of the states—Connecticut,[42] Massachusetts,[43] Michigan,[44] New Mexico,[45] New York,[46] and Texas[47]—impose additional requirements for organizations to develop policies to safeguard SSNs and, in some instances, to make their SSN protection policies available to the public or to their employees.

HOW TO PREPARE FOR FEDERAL LEGISLATION

Assuming passage in its current form, federal SSN protecting legislation will affect the daily activities of nearly every American and every type of organization. To comply, companies subject to the new law will need to:

- Perform internal audits and implement new policies and procedures for restricted and secure collection, storage, use, and disposal of SSNs in online or printed form.
- Review policies of and contracts with third-party service providers to determine the extent of their ability to access or use SSNs.
- Create systems to identify individuals, customers, and employees that are not related to or derived from SSNs, *e.g.*, using unique alphanumeric identifiers.

If a company determines that the use of SSNs is necessary and permissible, it should institute the following procedures to avoid violating the law:

- Provide information, when obtaining written or electronic consent, to individuals when SSNs are collected to explain the purpose, intended use, and scope of transactions permitted by the consent.
- Establish mechanisms, techniques, or technologies to protect SSNs from unauthorized access, disclosure, and use.
- Limit internal and third-party access to SSNs to a "need to know" basis, using passwords, encryption, and other techniques.
- Monitor and control access to records containing SSNs, such as documenting when employees can keep, view, and transport SSNs outside of company premises.
- Train employees on the importance of ensuring the confidentiality of SSNs as well as the costs associated with use or dissemination of such information in violation of the law.
- Provide for confidential and secure disposal of SSNs.
- Implement accountability procedures to monitor and control the handling of SSNs.
- Impose penalties for violations of the SSN protection policy.

In addition, companies may adopt technologies to ensure and facilitate full compliance by:

- Storing all SSNs and their derivatives in encrypted form to ensure data security.
- Ensuring secure connections and adequate encryption algorithms for accessing SSNs over local networks or the internet.
- Electronically registering all authenticated and unauthenticated access to records containing SSNs, as well as any attempts to access those records.

In applying each of these approaches, it is important to keep in mind that a business may collect SSNs not only from its customers but also from its employees and vendors who use SSNs as tax identification numbers.

CONCLUSION

The Bill is the latest attempt by Congress to control the alarming increase in identity-theft crimes. Businesses must comply with an array of state and federal laws for the protection of sensitive personal data, such as SSNs. Because the scope and underlying requirements of each state law differ, organizations must separately evaluate their potential obligations under each law. Federal legislation will establish uniformity in at least one area of privacy regulation,[48] while placing greater data protection responsibilities on all organizations. Companies should anticipate the possibility of federal legislation protecting SSNs and prepare compliance strategies for rapid organization-wide compliance with such legislation.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Steven C. Bennett
1.212.326.3795
scbennett@jonesday.com

Mauricio F. Paez
1.212.326.7889
mfpaez@jonesday.com

ENDNOTES

1. S. 141, 111th Cong. (2009).
2. *See, e.g.*, S. 139, 111th Cong. (2009) (requiring any agency or business entity engaged in interstate commerce that is in possession of sensitive personally identifiable information to notify the subjects of such information when security breaches are discovered).
3. Identity theft is typically defined as the fraudulent use of an individual's personal information to open financial accounts, incur debts, or transact other business in the victim's name.
4. SSN Bill § 3(a)(1)(a)(3).
5. SSN Bill § 10.
6. 15 U.S.C. § 1681 et seq.
7. 42 U.S.C § 201 et seq.
8. 15 U.S.C. § 6801 et seq.
9. H.B. 65, 2008 Leg., 25th Sess. (Alaska 2008) (effective July 1, 2009).
10. Ariz. Rev. Stat. § 1373.02.
11. Ark. Stat. § 4-86-107.
12. Cal. Civ. Code §§ 1798.85-86.
13. Colo. Rev. Stat. § 6-1-715.
14. Conn. Stat. § 42-470.
15. Ga. Stat. § 10-1-393.8.
16. Haw. Rev. Stat. Ann. § 487J-2.
17. Idaho Stat. § 28-52-108.
18. Ill Stat. ch. 815, § 505/2RR.
19. Kan. Stat. § 75-3520.
20. Me. Rev. Stat. Ann. tit. 10, ch. 208-A.
21. Md. Code Ann. Com. Law § 3402.
22. Mass. Gen. Laws ch. 167B, § 14.
23. Mich. Comp. Laws § 445.83.
24. Minn. Stat. § 325E.59.
25. Mo. Rev. Stat. § 407.1355.
26. L.B. 674, 100th Leg., 1st Sess. (Neb. 2007) (effective Sept. 1, 2008).
27. N.J. Rev. Stat. § 56:8-164.
28. N.M. Stat. Ann. §§ 57-12B-3, 4.
29. N.Y. Gen. Bus. Law § 399-dd; N.Y. Lab. Law. § 203-d (effective Jan. 3, 2009).
30. N.C. Gen. Stat. § 75-62.
31. Okla. Stat. tit. 40, § 173.1.
32. Ohio Stat. § 1349.17.
33. Or. Rev. Stat. § 646A.620
34. 74 Pa. Stat. Ann. § 204.
35. R.I. Stat. § 6-13-8, 1-17, 19.
36. S.B. 453, 117th Sess. (S.C. 2008).
37. Tenn. Stat. § 47-18-2110.
38. Tex. Bus. & Com. Code Ann. § 35.58, 581.
39. Utah Code Ann. §§ 13-45-301, 35A-4-312.5, 76-6-1102.
40. Vt. Stat. Ann. tit. 9, § 2440.
41. Va. Code Ann. § 59.1-443.2.
42. H.B. 5658, 2008 Gen. Assem., Reg. Sess. (Conn. 2008).
43. 201 Mass. Code Regs. §§ 17.01-04 (2008) (effective May 1, 2009).
44. Mich. Comp. Laws § 445.84.
45. N.M. Stat. §§ 57-12B-2, 3.
46. N.Y. Gen. Bus. Law § 399-dd(4).
47. Tex. Bus. & Com. Code § 35.581 (effective through March 31, 2009); Tex. Bus. & Com. Code § 501.051-53 (effective April 1, 2009).
48. The extent of state preemption will depend on the final language of the federal law.