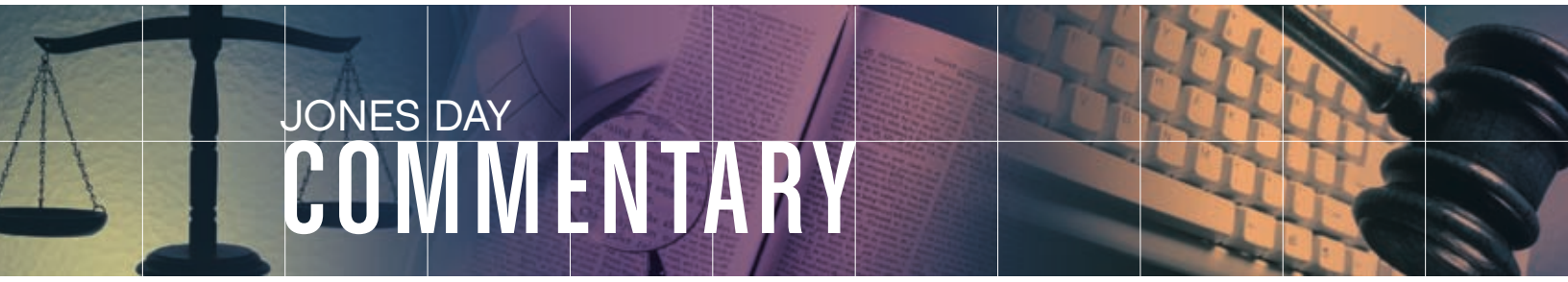
JONES DAY

OCTOBER 2006



NEW YORK ENACTS SOCIAL SECURITY NUMBER PROTECTION LAW

Consistent with the New York state government's attempt to counteract the growing threat of identity theft, on September 26, 2006, Governor Pataki enacted legislation placing limits on the use and dissemination of Social Security account numbers (the "NY Social Security Number Protection Law"). Enacted alongside two other measures aimed at thwarting identity theft, the NY Social Security Number Protection Law will impose harsh penalties on companies that fail to protect the confidentiality of Social Security numbers in their possession. These obligations become effective January 1, 2008. This *Commentary* provides a brief overview of the NY Social Security Number Protection Law.

SOCIAL SECURITY NUMBER PROTECTION STATUTE

The NY Social Security Number Protection Law applies to all nongovernmental bodies, including individuals, corporations, and partnerships. Generally, the legislation restricts the use and communication of Social Security numbers in order to maintain their confidentiality and make it more difficult for criminals to acquire the nine-digit number that uniquely identifies almost all Americans. The statute defines "Social Security number" as the unique number issued to citizens and residents of the United States by the federal Social Security Administration. The statutory definition also encompasses any number derived from an individual's Social Security number.

The impact of this broad definition is far-reaching. For example, records containing only part of the nine-digit Social Security number also fall under the law's scope. A great number of businesses currently use the last four digits of a Social Security number. These businesses will have to implement new policies in order to ensure compliance. Generally, the statute regulates two activities: (i) the communication of Social Security numbers; and (ii) the maintenance of records containing Social Security numbers.

COMMUNICATIONS CONTAINING SOCIAL SECURITY NUMBERS

A Social Security number is the No. 1 identifier used by criminals in identity theft. Not surprisingly, the increasing use and dissemination of Social Security numbers by businesses in their communications with current and prospective customers have come under fire. Criminals attempt to intercept various communication paths and retrieve confidential information, including Social Security numbers, in order to garner the data needed to steal an identity. The NY Social Security Number Protection Law regulates five realms of communication to minimize the interception of sensitive information by criminals: (i) communications to the public; (ii) access cards used for services, benefits, and products; (iii) transmission over the internet; (iv) internet access and authentication; and (v) mail correspondence.

First, the statute makes it illegal to intentionally communicate a Social Security number to the general public (although it permits individuals to disclose their own Social Security numbers as they deem appropriate). This provision is technology-neutral and encompasses all forms of communication, both oral and written.

The second aspect of the legislation prohibits making the access of services, benefits, or products contingent on the use of access cards or tags printed with an individual's Social Security number. Typical violations include healthcare providers issuing membership cards printed with the cardholder's Social Security number and employers issuing building-access cards with the employee's Social Security number, or even a portion thereof.

The third and fourth components of the legislation specifically target the use and dissemination of Social Security numbers over the internet. The statute prohibits companies from requiring an individual to transmit his or her Social Security number over the internet unless the connection is secure or the Social Security number itself is encrypted. The lack of clarity in the statute's requirements for encrypted transfers and secure connections provides incentive for companies to ensure that their current encryption and security protocols are, at a minimum, on par with current industry standards.

Furthermore, the new law does not permit the use of Social Security numbers for authentication purposes only. For example, companies are prohibited from requiring a Social Security number as a password to access a web site. Website accessibility must not be based solely on a Social Security number, or even a partial derivative of one. This ensures that potentially sensitive online information cannot be accessed by compromised Social Security numbers – a protection that benefits both consumers and businesses. In conjunction with the identifying Social Security number, web sites must use a unique password, PIN, or similar authentication device in order to establish and authenticate the identity of the user. By reducing, or even eliminating, the use of Social Security numbers for accessing online services, businesses can minimize their risk exposure to the new law.

The fifth and final communication element of the statute regulates the use of Social Security numbers in mail correspondence with individuals. Although the statute places a blanket prohibition on mailing material printed with an individual's Social Security number, numerous exceptions apply. Documents printed with an individual's Social Security number may be mailed if mandated by federal or state law. Additionally, forms or applications, including those used to establish or cancel accounts, may still contain an individual's Social Security number if the number is contained inside a sealed envelope and cannot be viewed unless the envelope is opened. This necessarily means that any type of postcard or similar document containing a Social Security number that is plainly viewable can no longer be sent in the mail without first being placed in an envelope. Mail-order catalogues, magazines, and similar marketing devices are particularly at risk in this category because mailing labels may contain a subscriber's partial or entire Social Security number. Companies should be aware that even a number based on an actual Social Security number exposes them to liability under the new law.

ACCESS TO SOCIAL SECURITY NUMBERS

In addition to regulating communications containing an individual's Social Security number, the NY Social Security Number Protection Law requires companies to adopt

reasonable measures to limit access to Social Security numbers in their possession. Specifically, employees accessing Social Security numbers must have a legitimate business purpose for doing so. Unfortunately, the statute does not define these reasonable measures. In light of the overall objective of the legislation, companies will need to ensure that employee access to Social Security numbers be kept to an absolute minimum. Moreover, companies must store Social Security numbers in a manner designed to preclude unauthorized access and to ensure confidentiality. Adherence to these security measures is a defense against alleged violations of the unsecured communication obligations noted above.

STATUTORY EXCEPTIONS AND DEFENSES

The NY Social Security Number Protection Law specifically exempts encrypted Social Security numbers from its scope. Proper use of encryption techniques and operational controls may permit companies to safely store and transmit Social Security numbers outside the purview of the statutory requirements. Additionally, the statute expressly exempts the collection, use, or release of an individual's Social Security number if it is required by federal or state law and for a company's general administrative purposes, internal verification, or fraud investigation. Moreover, use of a Social Security number in relation to a business function authorized by the Gramm-Leach-Bliley Act (15 U.S.C. § 6802) is exempt from the NY Social Security Number Protection Law.

CONSEQUENCES OF NONCOMPLIANCE

Companies and individuals that violate the NY Social Security Number Protection Law face several penalties. The statute authorizes the New York state attorney general to initiate a claim against suspected violators and to seek a judicially imposed suspension of the violating practices for the duration of the proceeding. If these practices are unlawful, the court may permanently suspend the violating activities. Furthermore, a court has the discretion to levy civil fines for violations of any of the five statutory provisions relating to the communication of Social Security numbers. First-time violators face a penalty of $1,000 per violation, up to a maximum of $100,000 for multiple violations resulting from a single incident, such as when a hacker gains access to multiple Social Security numbers at once. Second-time violators face penalties of $5,000 per violation, with a maximum of $250,000 for multiple violations resulting from a single incident. Imposition of these penalties can occur even if the individual whose Social Security number was compromised did not suffer personal harm. Although the new law does not give a cause of action to individuals nor allow them to compel the attorney general to sue, other laws exist that may expose companies to additional liability.

It is important to note that the NY Social Security Number Protection Law makes any waiver void and unenforceable. However, there are some defenses available. Companies may assert as a defense that the violation was unintentional or that it resulted from a bona fide error. Also, as previously noted, a company can demonstrate that it had implemented reasonable measures to restrict access to the Social Security numbers, in which case it may avoid liability.

STRATEGIES FOR COMPLIANCE

The effects of this new legislation will likely be far-reaching and involve a wide array of companies, partnerships, and individuals. Business organizations should follow a three-part strategy to ensure full compliance by January 1, 2008. Phase One involves an assessment of how, when, and where Social Security numbers are used. The exact audit procedures will be specific to each organization, but some common examples include:

- Evaluating all standard operating procedures to determine how Social Security numbers are gathered, stored, and used.

- Examining current customer and employee records to determine whether Social Security numbers are being used as ID numbers to facilitate access to web sites, facilities, services, or benefits.

- Reviewing all third-party service providers and contracts to determine the extent of their ability to access or use Social Security numbers.

- Assessing current marketing, accounting, and any other business functions making use of online and traditional mail correspondence, in order to restrict the use of Social Security numbers in any such communication.

Phase Two should involve a determination of whether the use of Social Security numbers is necessary. Where such use is necessary, companies should establish managerial procedures and controls to avoid violating the law. Procedures and controls include:

- Limiting employee access to Social Security numbers to a "need to know" basis, using passwords and other techniques.

- Training employees on the importance of ensuring the confidentiality of Social Security numbers as well as the costs associated with the use or dissemination of such information in violation of the law.

- Implementing policies and controls to monitor access to records containing Social Security numbers and protect them from unauthorized access.

Lastly, companies should employ technological measures to use, store, and communicate Social Security numbers in full compliance with the legislation. Such measures may include:

- Storing all Social Security numbers and their derivatives in encrypted form to ensure data security.

- Ensuring secure connections when accessing Social Security numbers over a local network or the internet.

- Implementing a system that uniquely identifies customers, web-site users, and employees by means of a proprietary alphanumeric format not related to Social Security numbers or other sensitive personal information.

- Electronically logging all authenticated and unauthenticated access to records containing Social Security numbers, as well as any attempts to access those records.

- Ensuring the use of adequate encryption algorithms for any Social Security number that is accessible over a local network or the internet.

CONCLUSION

The NY Social Security Number Protection Law is the latest attempt by the New York state government to thwart the rapid increase in identity-theft crimes by implementing robust legislation that places the onus of data protection on companies. New York is not alone in this regard; several other states have enacted similar legislation aimed at countering identity theft. In 2005, Arizona implemented a law nearly identical to the New York legislation. California, typically an innovator in privacy legislation, has similar restrictions on the use and dissemination of Social Security numbers. Colorado similarly passed Social Security number protection legislation governing not only the activities of individuals and corporations, but also those of the government itself. In Georgia, privacy laws apply to Social Security numbers in addition to other information commonly collected by companies, including driver's license numbers, dates of birth, and credit information. Additionally, Texas, Connecticut, and Illinois have all enacted legislation limiting private-sector use of Social Security numbers. Companies are encouraged to initiate their compliance strategies quickly to ensure organizationwide acquiescence prior to government enforcement.

RELATED JONES DAY TECHNOLOGY *COMMENTARIES*

- Security Breach Notification Requirements: Guidelines and Securities Law Considerations – March 2006
- Ohio Enacts Security Breach Notification Law – February 2006
- Personal Information Protection Law in Japan – November 2005
- New York Enacts Data Security and Notification Law – August 2005
- New HIPAA Rules for Group Health Plans and Health Insurers – February 2005
- The Federal CAN-SPAM Act—New Requirements for Commercial E-Mail – February 2004
- California First State to Require Online Privacy Policies – January 2004

LAWYER CONTACT

For further information, please contact your principal Firm representative or the lawyer listed below. We invite you to visit our web site for additional information on privacy topics. General e-mail messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Mauricio Paez
1.212.326.7889
mfpaez@jonesday.com