



INFORMATION LAW AND PRIVACY UPDATE

The Information Law and Privacy Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers.

Sidley provides services in the following areas:

Privacy and Internet Litigation and Regulatory Advice

Data Breach, Incident Response, and Cybercrime Advice

Global Data Protection and Information Security

International Data Transfer Solutions

Outsourcing and Cross-Border Issues

Gramm-Leach-Bliley and Financial Privacy

HIPAA and Healthcare Privacy

Workplace Privacy and Employee Monitoring

Cyberlaw, E-Commerce, and Internet Issues

Unfair Competition and Consumer Protection

Trademark and Copyright Litigation and Counseling

Website Policies and Domain Name Protection

Records Retention and Electronic Discovery

For more information, please visit

www.sidley.com/cyberlaw, or contact:

Alan Charles Raul

202.736.8477

araul@sidley.com

Edward R. McNicholas

202.736.8010

emcnicholas@sidley.com

To receive future copies of the Information Law and Privacy Update via email, please send your name, company or firm name and email address to rduncan@sidley.com

Attorney Advertising - For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, 212.839.5300 and One South Dearborn, Chicago, IL 60603, 312.853.7000. Prior results do not guarantee a similar outcome.

New Laws Significantly Restrict Handling of Social Security Numbers

In response to public fears of identity theft and the absence of federal legislation, a growing number of States have enacted statutory restrictions on the use or dissemination of Social Security Numbers (SSNs). As of January 1, 2008, twenty-nine States have laws affecting the handling of SSNs, and Minnesota has a law that will become effective July 1, 2008. The States that currently have such legislation in place are Arizona, Arkansas, California, Colorado, Connecticut, Georgia, Hawaii, Illinois, Indiana, Kansas, Maine, Maryland, Massachusetts, Michigan, Missouri, Montana, Nebraska, New Jersey, New Mexico, New York, North Carolina, Oklahoma, Oregon, Pennsylvania, Rhode Island, Texas, Tennessee, Vermont and Virginia.¹

General Types of Restrictions on Use of SSNs and SSN-Derived Numbers

Some of the specific provisions that are common to most of the state statutes include prohibitions on:

- Publicly displaying, intentionally communicating or otherwise making a SSN available to the general public;
- Intentionally printing a SSN on any card required to access goods or services;
- Requiring an individual to transmit his or her SSN over the Internet, unless the connection is secure or the SSN is encrypted;
- Requiring an individual to use their SSN to access a website, unless a password, unique pin or other authentication is also required; or

¹ ARK. CODE ANN. § 4-86-107; ARIZ. REV. STAT. § 44-1373; CAL. CIV. CODE § 1798.85.2; COL. REV. STAT. § 6-1-715; CONN. GEN. STAT. § 42-470; GA. CODE ANN. § 10-1-393.8; HAW. REV. STAT. §§ 487J-2 TO 487J-3; 815 ILL. COMP. STAT. 505/2RR; IND. CODE §§ 24-4-14-1 TO 24-4-14-8; KAN. STAT. ANN. § 75-3520; MD. CODE ANN., COMM. LAW §§ 14-3401 TO 3404; ME. REV. STAT. ANN. TIT. 10 § 1272-B; MASS. GEN. LAWS CH. 167B, § 14 & § 22; MICH. COMP. LAWS §§ 445.81 TO 445.87; MINN. STAT. § 325E.59; MO. REV. STAT. § 407.1355; MONT. CODE ANN. § 30-14-1702, § 30-14-1703; NEB. REV. STAT. § 48-237; N.J. STAT. ANN. § 56:8-164; N.M. STAT. ANN. § 57-12B-4; N.Y. GEN. BUS. LAW § 399-DD (2007); N.C. GEN. STAT. §§ 75-62; 40 OKLA. STAT. TIT. 40, § 173.1, 2007 ORE. ALS 759; 74 PA. STAT. ANN. §§ 201 TO 204; R.I. GEN. LAW § 6-13-17; TENN. CODE ANN. § 47-18-2110; TEX. BUS. & COM. CODE ANN. § 35.58; 9 VER. STAT. ANN. §§ 2030, 2440; and VA. CODE ANN. § 59.1-443.2. In addition, some States may have specialized restrictions on specific uses of SSNs, such as part of data collections by business entities.

This **Information Law and Privacy Update** has been prepared by Sidley Austin LLP for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

- Printing a SSN on any materials that are mailed to the individual, unless required by law.

The net effect of these provisions may well be to force companies to minimize the use of SSNs to the greatest extent practicable and to maintain strict controls on the uses made of SSNs. In light of the practical necessity for using SSNs for certain tasks, the state measures include various exceptions for the collection, use, or release of SSNs “as required by state or federal law,” as well as for the use of an SSN for “internal verification, fraud investigation or administrative purposes or for any business function specifically authorized by 15 U.S.C. § 6802 [exceptions in the Gramm-Leach-Bliley Act],” such as for uses in connection with authorized consumer transactions, uses with the consent of the consumer, and for consumer credit reports.

New York Law Became Effective January 1, 2008

The New York law contains each of the provisions that are common in other States, but it merits special attention because it defines “Social Security Number” expansively, so as to include any number that is a derivative of a SSN.² Any truncated or partial SSN is thus treated as if it were the entire SSN, under the stringent New York law. Accordingly, companies doing business in New York will need to revisit their systems to ensure that use of even partial SSNs are legally compliant, although the New York law allows uses required by state or federal law or necessary for “internal verification, fraud investigation or administrative purposes or for any business function specifically authorized by 15 U.S.C. § 6802 [exceptions in the Gramm-Leach-Bliley Act].”³

The New York law also includes information security requirements for businesses. It generally requires not only

“reasonable measures to ensure that no officer or employee has access to [a SSN] for any purpose other than for a legitimate or necessary purpose” but also that businesses provide “necessary or appropriate” safeguards to preclude unauthorized access, and to “protect the confidentiality” of the number.

Variations Among Laws, Including Restrictions That Apply to Truncated SSNs

The New York law exemplifies perhaps the most significant variation among the laws between States whose laws prohibit actions only with respect to an entire SSN, versus those that restrict the use of partial, derivations, or truncated SSNs, such as New York. Several States, like Nevada, explicitly limited the application of their law to entire SSNs. A handful of other States, including Arizona, Illinois, Michigan, Nebraska, New Jersey and New York, restrict use of partial SSNs, such as the last four digits of a SSN that are frequently used for identification purposes.

Several States have also enacted unique protections. For instance, in North Carolina, it is prohibited to “sell, lease, loan, trade, rent, or otherwise intentionally disclose a Social Security Number to a third party without written consent to the disclosure, when the party making the disclosure knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks a legitimate purpose for obtaining the Social Security Number.”⁴ And in Nebraska, it is prohibited for an employer to “require an employee to use more than the last four digits of his or her Social Security Number as an employee number for any type of employment-related activity.”⁵

In addition to the specific provisions of these SSN protection laws, some statutes require a general level of “reasonable security” to protect the numbers. For many other States, SSNs

² “As used in this section ‘social security account number’ shall include the number issued by the federal social security administration and any number derived from such number. Such term shall not include any number that has been encrypted.” § 399-dd(1).

³ The New York law incorporates the exception in GLBA for uses “with the consent or at the direction of the consumer.” § 6802(e)(2). Such consent must be legitimately obtained, however, given that § 399-dd(5) of the New York law states that “Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.”

⁴ N.C. GEN. STAT. §§ 75-62

⁵ NEB. REV. STAT. § 48-237

will also be protected under personal information protection acts, or generic information security statutes, which can range from imposing general mandates for reasonable and appropriate security measures,⁶ to requiring specific security requirements such as encryption.⁷ These types of laws are increasingly common as state legislatures seek to address the risks of identity theft.⁸ Such laws require businesses to take stock of the way they are collecting, transmitting and storing personal information and SSNs.

Penalties for Non-Compliance

Penalties for violations vary, but include the following: state Attorney General actions for fines, as in Massachusetts, private rights of action by affected individuals, such as in Michigan, enforcement through unfair and deceptive acts and practices statutes, as in Illinois, or some combination thereof. For example, N.Y. GEN. BUS. LAW § 399-dd(6) authorizes the Attorney General to seek an injunction for violations of the Act. In addition, courts may also impose civil penalties of not more than \$1000 per violation and not more than \$100,000 for multiple violations resulting from a single incident. Repeat violations may incur a civil penalty of not more than \$5000 per violation and not more than \$250,000 for multiple violations resulting from a single incident.

Check List of SSN Uses

As a first step to compliance with these new provisions, many businesses find it useful to catalogue where they store and use SSNs, the relevant information security policies, the protections they provide when transmitting SSNs over the Internet, and the

disclosures made when collecting and sharing SSNs with necessary authorized parties. The best practice is to minimize the use of SSNs overall so that they are collected, used, and transmitted only when truly necessary. When systems have already been programmed to use nine-digit numbers for unique identification, the use of a unique random number in lieu of the SSN may allow for compliance without costly re-programming of equipment.

As part of this process, businesses may wish to consider whether they use or solicit SSNs or truncated SSNs for any of the following:

- Employee ID numbers
- ID Cards
- Website access
- Payroll checks
- Pay stub data
- Customer identification
- Claim forms
- Periodic statements
- Transmission of tax information
- Authentication
- Credit or financial applications
- Background checks

⁶ See, e.g., CAL. CIV. CODE § 1798.81.5.

⁷ A new Nevada law, NEV. REV. STAT. 597.970, which shall be effective October 1st, 2008, mandates encryption for all personal information “in transit.”

⁸ At least fourteen States have passed some version of a personal information protection law, including Maryland and Oregon as the latest-incorporating data breach notifications, general security mandates and specific prohibitions as to the use of Social Security Numbers, both of which became effective January 1st, 2008. See MD. CODE ANN., COM. LAW §§ 14-3501 to 14-3508; Oregon SB 583, available at <http://www.leg.state.or.us/07reg/measures/sb0500.dir/sb0583.intro.html>