MORRISON | FOERSTER

## Legal Updates & News

**Bulletins**

# State Statutes Restricting or Prohibiting the Use of Social Security Numbers

November 2007
by Joyita R. Basu

**Privacy Bulletin, November 8, 2007**

Currently, more than 25 states have adopted laws restricting or prohibiting the collection, use or disclosure of an individual's Social Security number ("SSN"), and these laws generally apply to all commercial entities.[1] In addition to the SSN disclosure laws discussed in this article, other state laws also may regulate the collection, use or disclosure of SSN data; for example, this article does not address state laws that regulate the collection, use or disclosure of SSN data by insurance entities, given the specialized nature of those laws.

In response to perceived abuses arising from the widespread use of SSNs as identifiers,[2] California enacted legislation in 2001 that imposes significant restrictions on the use of SSNs by businesses and, in certain circumstances, state and local agencies.[3] Like the California law, the SSN disclosure laws of a majority of the states generally apply to any person or entity doing business in the state.[4] However, some state laws, such as those in Nebraska[5] and Oklahoma,[6] apply to employers who use employees' SSNs. In addition, the laws of some states exempt certain entities from the SSN disclosure laws. For example, the Colorado law exempts entities covered by the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") [7] and the Pennsylvania law exempts a financial institution covered by the Gramm-Leach-Bliley Act ("GLBA"), a "licensee" regulated under Pennsylvania law, a covered entity under HIPAA or any entity subject to the Fair Credit Reporting Act ("FCRA").[8]

### Type of Information Covered

The state SSN disclosure laws typically do not define the term "Social Security number" and thus do not specifically address whether the law applies to the use of the entire SSN, or to truncated or redacted numbers. Some states laws, however, include specific language regarding truncated or redacted numbers, even though those laws do not define a "Social Security number." For example, the SSN disclosure laws of Hawaii[9] and New Mexico[10] specify that the prohibitions apply to the use of the "entire" SSN, while the Arizona,[11] Michigan,[12] Nebraska,[13] New Jersey,[14] North Carolina,[15] and Vermont[16] laws specifically permit the use of truncated or redacted numbers. In this regard, the New York SSN disclosure law appears to be the most stringent. The New York law applies to a "Social Security Account Number" ("SSAN"), which is defined as "includ[ing] 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."[17] Therefore, in order to reduce the risk of making disclosures barred by the New York law, an entity might consider employing an alternative identification number which replaces, but is not derived from, the individual's SSN.

### Prohibited Activities

The state SSN disclosure laws generally prohibit using SSNs in a manner that provides access to a SSN to view by the general public. For example, the California SSN disclosure law prohibits any person or entity from (1) publicly displaying an individual's SSN; (2) printing an individual's SSN on any card used to access products or services provided by the person;
(3) encoding or embedding a SSN in or on a card or document; (4) requiring an individual to transmit his or her SSN via the Internet unless the connection is secure or the SSN is encrypted; (5) requiring an individual to use his or her SSN to access an Internet Website unless an additional password or personal identification number ("PIN") is also required; or (6) printing an individual's SSN on any materials mailed to him or her without a federal or state law requirement that the SSN be included, except for applications or forms sent by mail as part of an application or enrollment process.[18] Several other state laws contain similar prohibitions.[19]

Even when an entity is permitted to mail an individual's SSN, the SSN should not be printed, in whole or in part, on a postcard or other mailer not using an envelope, and should not be visible on the envelope or without the envelope having been opened.[20] Unlike the California SSN disclosure law, which does not specifically reference the transmission of SSNs via electronic mail or facsimile, the Maryland law[21] specifically prohibits the inclusion of an individual's SSN on any material that is electronically transmitted or transmitted by facsimile to the individual. In addition, some state laws, such as those in Minnesota,[22] North Carolina,[23] and Vermont,[24] specifically prohibit a person or entity from selling an individual's SSN to a third party. The Michigan[25] and Minnesota[26] SSN disclosure laws also prohibit the use of SSNs as an account number.

**Exceptions**

A majority of the state SSN disclosure laws include some exceptions for the use of SSNs. For example, the California law provides an exception for documents that are required to be open to the public pursuant to other specified provisions of California law or records that are required by statute, case law, or California Rule of Court, to be made available to the public by certain entities under the California constitution.[27] Moreover, the California SSN disclosure law does not prevent the collection, use or release of SSNs as required by state or federal law or the use of SSNs for internal verification or administrative purposes.[28]

Under the Michigan law, an entity may use more than four sequential digits of the SSN as the primary account number or include the SSN on any information mailed to a person if the use is for an administrative purpose in the ordinary course of business to:

1. Verify an individual's identity, identify an individual, or accomplish a similar administrative purpose related to a current or proposed account, transaction, product, service, or employment;
2. Investigate an individual's claim, credit, criminal, or driving history;
3. Detect, prevent, or deter identity theft or other crime;
4. Lawfully pursue or enforce a person's legal rights;
5. Lawfully investigate, collect, or enforce a child or spousal support obligation or tax liability; or
6. Provide or administer employee or health insurance or membership benefits, claims, or retirement programs or to administer the ownership of shares of stock or other investments.[29]

Moreover, a use of all or more than four sequential digits of a SSN as a primary account number is permitted by the Michigan law if the use began before the effective date of the act and the use is ongoing, continuous, and in the ordinary course of business; but if the use is stopped for any reason, this exemption no longer applies.[30]

Under the New York law, the prohibitions do not prevent the collection, use, or release of a SSAN as required by state or federal law or the use of the number for internal verification, fraud investigation, or administrative purposes, or for any business function specifically authorized by certain provisions of the GLBA.[31] Other states include a more expanded list of exceptions to the prohibitions against the use of SSN. For example, the Hawaii, North Carolina and Vermont SSN disclosure laws permit: use of a SSN in an application or in documents related to an enrollment process, or to establish, amend, or terminate an account, or to confirm the accuracy of the SSN for the purpose of obtaining a credit report pursuant to the FCRA (a SSN that is permitted to be mailed under this exception may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.);[32] the collection, use, or release of a SSN for internal verification or administrative purposes; the opening of an account or the provision of, or payment for, a product or service authorized by an individual; the collection, use, or release of a SSN related to prevention and investigation of fraud, background checks, social or scientific research, collection of debt, obtaining a credit report from or furnishing data to a consumer reporting agency pursuant to the FCRA, or other permissible purpose enumerated under GLBA, or locating an individual who is missing; business activities pursuant to a court order, warrant, subpoena, or when otherwise required by law; a business providing the SSN to a federal, state, or local government entity, including a law enforcement agency, court, or their agents or assigns; a SSN that has been redacted.[33] However, the North Carolina statute requires a business covered by these provisions to make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements are implemented.[34]

**Additional Requirements**

In addition to the various prohibitions on the use of SSNs and exceptions to the prohibitions, a number of state laws include additional requirements. For example, the Michigan law requires a person who obtains one or more SSNs in the ordinary course of business to create a privacy policy that must, at a minimum, (1) ensure, to the extent practicable, the confidentiality of the SSN; (2) prohibit unlawful disclosure of SSN; (3) limit access to information that contains SSN; (4) describe the proper disposal of documents containing SSN; and (5) establish penalties for the violation of the privacy policy.[35] The privacy policy must be published in an

employee handbook, procedures manual, or other similar document.[36] The Texas law also obliges an entity that requires an individual to disclose his or her SSN to adopt a privacy policy and make the privacy policy available to the individual.[37] Similarly, the New York statute requires any person who is in possession of the SSN of any individual, to the extent that such SSN is maintained for the conduct of business or trade, to take reasonable measures to ensure that no officer or employee has access to the SSN for any purpose other than for a legitimate or necessary purpose related to the conduct of such business or trade and to provide safeguards necessary or appropriate to preclude unauthorized access to the SSN and to protect the confidentiality of the SSN.[38] However, the New York law provides a defense to an alleged violation. Specifically, the New York SSN disclosure law provides that no person shall be deemed to have violated the provisions of the law if the person can show, by a preponderance of the evidence, that the violation was not intentional and resulted from a bona fide error made notwithstanding the maintenance of procedures reasonably adopted to avoid such error.[39]

**Conclusion**

To comply with the requirements of such state SSN disclosure laws, covered entities may need to consider modifying aspects of their operations. For example, changes may include (1) creation of alternate identification numbers for individuals; (2) reprogramming of computer systems to replace references to SSNs with alternative identifiers; (3) removal of SSNs from identification cards; or (4) removal of SSNs from correspondence, claims forms and statements. In addition, covered entities may wish to evaluate their use of SSNs to ensure that they are consistent with the requirements imposed by the various state SSN disclosure laws. The Office of Privacy Protection within the California Department of Consumer Affairs ("Office of Privacy Protection") has published recommended practices for complying with the law.[40] In particular, the Office of Privacy Protection recommends that entities reduce their efforts to collect SSNs; provide information to individuals when SSNs are collected explaining the purpose, the intended use, whether the SSN must be provided, and the consequences of failing to provide the SSN; eliminate the public display of SSNs; control access to SSNs; protect SSNs with appropriate security measures; and implement accountability procedures to monitor the handling of SSNs.[41]

---

[1] States that have enacted legislation regulating the use of SSNs include Arizona, Arkansas, California, Colorado, Connecticut, Georgia, Hawaii, Illinois, Kansas, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, New Jersey, New Mexico, New York, North Carolina, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, and Virginia. Although most of these state statutes generally apply to persons doing business in the state, some state laws, such as the Oklahoma and Nebraska law, apply specifically in the employment context. These state statutes have varying effective dates.

[2] *See, e.g.*, Assembly Comm. on Judiciary: Personal Information: Confidentiality: Identity Theft, 2001 Leg. (Cal. 2001), available at *http://info.sen.ca.gov/pub/01-02/bill/sen/sb_0151-0200/sb_168_cfa_20010709_104555_asm_comm.html*.

[3] Cal. Civ. Code §§ 1798.85–1978.86.

[4] *See e.g.*, N.Y. Gen. Bus. Law § 399-dd(2); N.C. Gen. Stat. § 75-62(a); Tex. Bus. & Com. Code Ann. § 35.58(a).

[5] LB 674, 1st Sess. of the 100th Legis. (Neb. 2007).

[6] Okla. Stat. tit. 40, § 173.1(A)(1).

[7] Colo. Rev. Stat. § 6-1-715(4)(b).

[8] 74 Pa. Stat. Ann. § 204.

[9] Haw. Rev. Stat. Ann. § 487J-2(a).

[10] N.M. Stat. Ann. § 57-12B-4(A).

[11] Ariz. Rev. Stat. § 1373.02.

[12] Mich. Comp. Laws § 445.83.

[13] LB 674, 1st Sess. of the 100th Legis. (Neb. 2007).

[14] N.J. Rev. Stat. § 56:8-164(a)(1).

[15] N.C. Gen. Stat. § 75-62(b)(7).

[16] Vt. Stat. Ann. tit. 9, § 2440(c)(7).

[17] N.Y. Gen. Bus. Law § 399-dd(1) (emphasis added).

[18] Cal. Civ. Code §§ 1798.85(a)(1)–1798.85(a)(5), 1798.85(f).

[19] *See e.g.*, 815 Ill. Comp. Stat. § 505/2QQ(a); N.J. Stat. Ann. § 56:8-164(a); Tex. Bus. & Com. Code § 35.58 (a).

[20] *See e.g.*, Cal. Civ. Code § 1798.85(a)(5); Colo Rev. Stat. § 6-1-715(1)(e); 815 Ill. Comp. Stat. § 505/2QQ (a)(5).

[21] Md. Code Ann. Com. Law § 3402(a)(6).

[22]Minn. Stat. § 325E.59(a)(7).

[23]N.C. Gen. Stat. § 75-62(a)(6).

[24] Vt. Stat. Ann. tit. 9, § 2440(a)(6).

[25] Mich. Comp. Laws § 445.83(1)(b).

[26]Minn. Stat. § 325E.59(a)(6).

[27] Cal. Civ. Code § 1798.85(c).

[28] Cal. Civ. Code § 1798.85(b).

[29] Mich. Comp. Laws § 445.83(3)(a).

[30] Mich. Comp. Laws § 445.83(3)(b).

[31] N.Y. Gen. Bus. Law § 399-dd(3).

[32] N.C. Gen. Stat. § 75-62(b); Haw. Rev. Stat. Ann. § 487J-2(b)(1); Vt. Stat. Ann. tit. 9, § 2440(c)(1).

[33] N.C. Gen. Stat. § 75-62(b); Haw Rev. Stat. Ann. § 487J-2(b)(2)-(10); Vt. Stat. Ann. tit 9, § 2440(c)(2)-(7).

[34] N.C. Gen. Stat. § 75-62(c).

[35] The privacy policy requirements do not apply to persons that obtain an individual's SSN in the ordinary course of business and in compliance with the FCRA or subtitle A of Title V of the GLBA. Mich. Comp. Laws § 445.84(3).

[36] Mich. Comp. Laws § 445.84.

[37] Tex. Bus. & Com. Code Ann. § 35.581(a).

[38] N.Y. Gen. Bus. Law § 399-dd(4).

[39] N.Y. Gen. Bus. Law § 399-dd(6).

[40] Recommended Practices for Protecting the Confidentiality of Social Security Numbers, Office of Privacy Protection, California Dept. of Consumer Affairs (2007), available at http://www.privacy.ca.gov/recommendations/recomend.htm.

[41] *Id*.