MORRISON | FOERSTER

Legal Updates & News

Bulletins

New Connecticut Privacy Law Imposes Up to $500,000 in Civil Penalties for Misuse of Personal Information

June 2008
by Miriam Wugmeister, Christine E. Lyon, Joyita R. Basu

Related Practices:

- Privacy and Data Security

Privacy Update, June 19, 2008

Effective October 1, 2008, Connecticut's new Act on the Confidentiality of Social Security Numbers (the "Act") [1] will impose substantial new obligations on businesses that collect Social Security numbers ("SSNs") and other personal information—and substantial new penalties for privacy violations. The Act is not expressly limited to businesses located in Connecticut or the personal information of Connecticut residents, which creates uncertainty about how broadly its requirements will be applied by Connecticut courts. Companies doing business in Connecticut or collecting personal information from individuals in Connecticut should evaluate their potential obligations under these laws, as well as the growing number of similar laws developing in other states.

Mandatory Posting of Privacy Protection Policy. The Act requires any person who collects SSNs in the course of business to create a privacy protection policy that: (1) protects the confidentiality of SSNs; (2) prohibits the unlawful disclosure of SSNs; and (3) limits access to SSNs. These obligations to create a privacy policy are similar to obligations found in other states such as Michigan,[2] Texas,[3] and New Mexico.[4] Unlike those state statutes,[5] however, the Connecticut Act provides that the privacy policy must be "published" or "publicly displayed." The Act provides that: "'public display' includes, but is not limited to, posting on an Internet web page." The statutory language does not define the term "published" nor does it specify if posting a privacy policy on an organization's Intranet would be sufficient. Please note that these requirements are in addition to existing Connecticut laws that already restrict the display and use of SSN information.[6]

Data Security Obligations for Personal Information. The Act also creates additional data security obligations with respect to personal information. For purposes of the Act, the term "personal information" is defined very broadly to include any "information capable of being associated with a particular individual through one or more identifiers."[7] Unlike other state statutes requiring the protection of personal information (such as the California[8] or North Carolina[9] statutes), the Connecticut Act does not limit personal information to information that in fact identifies any individual, but also includes information that is "capable" of being associated with an individual. The Act does provide a list of examples of personal information, which includes, but is not limited to, SSN, driver's license number, state identification card number, account number, credit or debit card number, passport or alien registration number, or a health insurance identification number. The Act does not apply to publicly available information. Notably, the Act is not limited to computerized data but may cover personal information maintained in any form.

The Act requires any person who possesses personal information of another to safeguard the data from misuse by third parties, and to destroy, erase or make unreadable such data prior to disposal. This means that any electronic file or document that contains *any* personal information must be safeguarded and made unreadable when it is disposed.

Any intentional violation of the Act may be subject to a civil penalty of $500 for each violation, up to $500,000 for any single violation.

Practical Implications. The Act underscore the importance of maintaining up-to-date privacy policies that comply with the evolving requirements under applicable state laws. As a practical matter, the provisions in the Act that require a business to publish its privacy policy impose an additional burden on any business entity that is required to comply with the Act. To avoid any misperceptions, the entity must ensure that its current privacy policy complies with the relevant state laws and is published or publicly displayed and that its personnel are

substantially complying with the published privacy policy.

Footnotes:

[1] H.B. 5658, 2008 Gen. Assem., Feb. Sess. (Conn. 2008).

[2]Mich. Comp. Laws § 445.84.

[3] Tex. Bus. & Com. Code Ann. § 35.581.

[4] N.M. Stat. Ann. § 57-12B-3.

[5] Mich. Comp. Laws § 445.84 ("A person that creates a privacy policy . . . shall publish the privacy policy in an employee handbook, in a procedures manual, or in 1 or more similar documents, which may be made available electronically.").

[6] *See* Conn. Gen. Stat. § 42-470.

[7] However, "personal information" does not include "publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media." Act, § 1(c).

[8] *See* Cal. Civ. Code § 1798.81.5. The California statute defines "personal information" as unencrypted or unredacted information that includes an individual's first name or first initial and last name in combination with: SSN; driver's license number or California identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or medical information. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

[9] N.C. Gen. Stat. §§ 75-61, 14-113.20(b). North Carolina law defines personal information as an individual's first name or first initial and last name in combination with: SSN or employer taxpayer identification number; driver's license, state identification card, or passport numbers; checking account numbers; savings account numbers; credit card numbers; debit card numbers; personal Identification number (PIN) Code as defined; electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names; digital signatures; any other numbers or information that can be used to access a person's financial resources; biometric data; fingerprints; passwords; or parents' legal surnames prior to marriage. Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.