

Privacy & Security Task Force ADVISORY

October 7, 2008

States Adopting Aggressive New Privacy and Data Security Laws and Regulations

This advisory summarizes selected state legislative and regulatory developments regarding corporate data privacy and security obligations. Please do not hesitate to contact your Alston & Bird attorney or any member of our [Privacy and Security Task Force](#) if you have additional questions regarding these or other state law privacy and security obligations.

Overview

State legislatures and regulatory agencies are challenging businesses in these difficult economic times to put in place broad new information security policies and procedures. A series of new laws and regulations enacted in recent months require, among other things: (a) encryption of personal information on laptops, PDAs and portable media, including flash drives; (b) encryption of personal information transmitted over the Internet; (c) development and publication of Social Security Number (SSN) privacy protection policies; and (d) specific measures to protect the confidentiality and security of employee SSNs. These laws and regulations carry significant statutory penalties for violations and, in some states, the possibility of businesses facing private rights of action for noncompliance. Below we provide a brief update on these developments in the states of Massachusetts, New York, Nevada, Connecticut and Texas.

Massachusetts

New Massachusetts Regulation Requires Encryption of Personal Information on Laptops and Other Portable Media and During Transmission over Public Networks

- On January 1, 2009, a sweeping new Massachusetts regulation will go into effect, requiring businesses that own, license or maintain personal information about Massachusetts residents to implement a written comprehensive information security program that meets certain detailed requirements.
- The regulation also requires businesses to encrypt all personal information transmitted via a wireless network or a public network, such as the Internet or cellular networks. In addition, businesses must encrypt personal information about Massachusetts residents that is stored on laptops, PDAs (including Blackberry devices) and portable media such as flash drives. The regulation defines “personal information” as a first and last name combined with an SSN, driver’s license number, financial account number or credit or debit card number.
- Non-compliance with the regulation is subject to a civil penalty up to \$5,000 per violation.
- Link to Massachusetts Regulation (201 Mass.Code Regs. 17.00): http://www.mass.gov/?pageID=ocamodulechunk&L=1&L0=Home&sid=Eoca&b=terminalcontent&f=idtheft_201cmr17&csid=Eoca

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

New York

New York Enacts Strong Protections for Employee Personal Information

- New York enacted legislation in July 2008, effective January 3, 2009, that will impose strict limitations on the use and communication of employee personal information, defined as an employee's SSN, home address or telephone number, personal email address, Internet name or password, driver's license number or parent's surname prior to marriage. The law also prohibits employers from using employee SSNs as identification numbers for occupational licensing purposes.
- The new law further prohibits employers from: (a) publicly posting or displaying an employee's SSN, (b) visibly printing an employee's SSN on any identification badge, access card or time card, (c) placing an employee's SSN in any files with unrestricted access, or (d) communicating an employee's personal information to the general public.
- Civil penalties may be imposed for "knowing" violations of the law. A violation is presumed to be "knowing" if the employer "has not put in place any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions." We recommend, as a result, that businesses assess the risk of violating the new law based upon the business's operations, procedures and track record. If there is a quantifiable risk, then it may be advisable to establish new procedures (or, if possible, identify existing qualifying procedures) and notify personnel based in New York of the new law. Of course, a business may also decide to undertake these measures even if there is only a remote risk of a violation.
- Other provisions, effective January 1, 2010, place restrictions on the use and communication of SSNs by the state and its political subdivisions.
- Link to New York Law (N.Y. Labor Law § 203-d): <http://www.alston.com/files/docs/NY203-d.pdf>

Nevada

Nevada Law Imposes Encryption Requirements on Electronic Transmissions

- Nevada enacted a new statute that went into effect October 1, 2008, that requires businesses in the state to encrypt every electronic transmission containing personal information about a customer that is directed outside the business's own "secure system."
- The statute defines "personal information" as a person's first and last name joined with an SSN, driver's license number, or a financial account number or credit or debit card number (if combined with a security code required to access the account). The law does not define the term "secure system." But the term would appear to mean a network and associated information systems behind a business's firewall. This means that businesses operating in Nevada are now required to encrypt emails sent outside the business and other communications over the Internet if they contain personal information.
- Link to Nevada Law (Nev. Rev. Stat. § 597.970): <http://www.leg.state.nv.us/NRS/NRS-597.html#NRS597Sec970>

Connecticut and Texas

Connecticut and Texas Laws Guard Confidentiality of Social Security Numbers

- Connecticut Public Act No. 08-167 was signed into law on June 10, 2008, and went into effect on October 1, 2008. The Connecticut legislature passed the law quickly following a series of highly publicized data security incidents involving residents of the state. The law requires businesses to: (a) safeguard “personal information” in their possession, (b) dispose of records containing personal information in accordance with certain standards, and (c) publish and enforce an SSN privacy protection policy if the company collects SSNs “in the course of business”.
- The safeguarding and safe disposal requirements are consistent with other state laws. But Connecticut has staked out new ground by requiring companies that collect SSNs in the course of business to establish a “privacy protection policy” and to publish or publicly display the policy. The policy must “(a) protect the confidentiality of SSNs, (b) prohibit unlawful disclosure of SSNs, and (c) limit access to SSNs.”
- There is an argument that the new statute regulates the collection of SSNs from customers, but not from employees. While the law broadly applies to companies that collect SSNs in the course of business, the law is enforceable by the Department of Consumer Protection and Connecticut state agencies that license businesses that are not subject to that Department’s authority, such as insurance companies. These agencies do not regulate the relationship between employers and employees. We nevertheless recommend that companies independently consider whether to apply the law’s requirements to transactions with their employees.
- The Connecticut law is enforceable at the administrative level in the state and each violation is subject to a civil penalty of \$500. The maximum penalty for a single event is \$500,000.
- On April 1, 2009, a Texas law will go into effect that resembles and expands upon the Connecticut law. The Texas law prohibits businesses from requiring a customer to submit an SSN unless the business has adopted and made available a privacy policy that identifies how and when the information will be used, how it is protected, who will have access to it, and the planned method of its disposal.
- The Texas law will also prevent non-governmental use of SSNs on cards or for website access absent additional protections specified in the law.
- Link to Connecticut Law (Conn. Pub. Act No. 08-167): <http://www.cga.ct.gov/2008/ACT/PA/2008PA-00167-R00HB-05658-PA.htm>
- Link to Texas Law (Tex. Bus. & Com. Code §§ 501.001-102): <http://tlo2.tlc.state.tx.us/statutes/docs/BC/content/pdf/bc.011.00.000501.00.pdf>

If you would like to receive future *Privacy & Security Task Force Advisories* electronically, please forward your contact information including e-mail address to Privacy.Post@alston.com. Be sure to put “**subscribe**” in the subject line.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of our [Privacy & Security Task Force](#) attorneys.

Andria E. Beeler-Norrholm
andria.beeler-norrholm@alston.com
404.881.4933

Edward Britan
edward.britan@alston.com
202.756.3364

Angela T. Burnette
angie.burnette@alston.com
404.881.7665

Clare H. Draper, IV
clare.draper@alston.com
404.881.7191

Christopher D. Ford
chris.ford@alston.com
202.756.3371

Gina Ginn Greenwood
gina.greenwood@alston.com
404.881.4698

William J. Helmstetter, III
bill.helmstetter@alston.com
404.881.7942

Amy S. Heppner
amy.heppner@alston.com
404.881.7272

John R. Hickman
john.hickman@alston.com
404.881.7885

Romulus A. Johnson
romulus.johnson@alston.com
202.756.3411

Paul J. Kaplan
paul.kaplan@alston.com
404.881.4684

David C. Keating
david.keating@alston.com
404.881.7355

Pamela Keeney Lina
pamela.lina@alston.com
404.881.4935

Robert C. Lower
bob.lower@alston.com
404.881.7455

Kathryn J. Marks
kathryn.marks@alston.com
202.756.3479

Paul G. Martino
paul.martino@alston.com
202.756.3439

Naotaka Matsukata
nao.matsukata@alston.com
202.756.5591

Gerald L. Mize, Jr.
gerald.mize@alston.com
404.881.7579

Eric A. Shimp
eric.shimp@alston.com
202.756.3409

Dwight C. Smith, III
dwight.smith@alston.com
202.756.3325

Katherine M. Wallace
katherine.wallace@alston.com
404.881.4706

Michael Zweiback
michael.zweiback@alston.com
213.576.1163

ATLANTA

One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404.881.7000

CHARLOTTE

Bank of America Plaza
Suite 4000
101 South Tryon Street
Charlotte, NC 28280-4000
704.444.1000

DALLAS

Chase Tower
Suite 3601
2200 Ross Avenue
Dallas TX 75201
214.922.3400

LOS ANGELES

333 South Hope Street
16th Floor
Los Angeles, CA 90071-3004
213.576.1000

NEW YORK

90 Park Avenue
New York, NY 10016-1387
212.210.9400

RESEARCH TRIANGLE

Suite 600
3201 Beechleaf Court
Raleigh, NC 27604-1062
919.862.2200

SILICON VALLEY

Two Palo Alto Square
Suite 400
3000 El Camino Real
Palo Alto, CA 94306-2112
650.838.2000

VENTURA COUNTY

Suite 215
2801 Townsgate Road
Westlake Village, CA 91361
805.497.9474

WASHINGTON, D.C.

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202.756.3300

www.alston.com

© Alston & Bird LLP 2008