



Security and Privacy in 2011: How to Stay a Step Ahead



Tech Talk Tuesday

January 25, 2011

Colin J. Zick
Foley Hoag LLP
(617) 832-1275
czick@foleyhoag.com



List of U.S. Laws Impacting Data Privacy and Security

- U.S.A. Patriot Act (Pub. L. 107-56)
- Cable TV Privacy Act of 1984 (47 U.S.C. § 551)
- The Children's Online Privacy Protection Act (15 U.S.C. §§ 6501-6506)
- Communications Assistance for Law Enforcement Act of 1994 (47 U.S.C. §§ 1001-1010)
- Consumer Financial Protection Act of 2010 (Pub. L. No. 111-203, 124 Stat. 1376)
- Counterfeit Access Device and Computer Fraud Abuse Act of 1984 (18 U.S.C. § 1030)
- Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721)
- Electronic Communications Privacy Act (18 U.S.C. §§ 2510-21, 2701-11)
- Fair and Accurate Credit Transactions Act of 2003
- Fair Credit Reporting Act (15 U.S.C. §§ 1681-1681(u))
- Genetic Information Nondiscrimination Act (P.L. 110-233, 122 Stat. 881)
- Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801-6809)
- Health Insurance Portability and Accountability Act (42 U.S.C. § 1306)
- HITECH Act (Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5)
- Privacy Act of 1974 (5 U.S.C. § 552a)
- Right to Financial Privacy Act (12 U.S.C. § 3402)
- Telecommunications Act of 1996 (47 U.S.C. § 222)
- Telephone Consumer Protection Act of 1991 (47 U.S.C. § 227)
- Video Privacy Protection Act of 1998 (18 U.S.C. § 2710)

How Do You Find Your Way Through This Regulatory Maze?

Three principles to apply when dealing with federal and state security and privacy laws:

- When in doubt, don't let information out.
- Disclose the minimum necessary information for the task at hand.
- Encrypt data and secure devices that store, transmit or receive information.

Potential New Federal Legislation

- Congressman Cliff Stearns (R-FL) is reworking the online privacy legislation which he originally helped draft with former Congressman Rick Boucher (D-VA) last year.
- His bill is expected to seek to:
 - compel websites to notify users about the collection and use of their personal data, and
 - users would have to opt in before websites could collect certain particularly sensitive information, including health or financial data.
- Industry believes that the legislation would hamper the provision of free online content supported by ad revenue.
- Privacy advocates say it would not go far enough protect consumers.
- Other members of Congress have expressed a desire to introduce online privacy legislation, including Congressman Edward Markey (D-MA).

Yesterday's Developments



Background on Massachusetts law

- Most recent law in the Massachusetts in the area of data privacy and security – Mass. Gen. L. ch. 93H.
- Enacted after the TJX data breach was made public.
- Intended to protect Massachusetts residents from identity theft.
- Applies to any business entity that owns, licenses, maintains or stores the “**personal information**” of a Massachusetts resident.
- Regulations – 201 CMR 17.00 – most took effect on March 1, 2010, govern measures businesses must take to comply with new data security law.

What is “Personal Information”?

“**Personal Information**” is:

- A person’s first name and last name (or first initial and last name) **PLUS** any **one** of the following:
 - Social Security number
 - Driver’s license number (or other state issued ID card number)
 - A financial account number, or credit or debit card number, with or without any required security code, access code or PIN that would allow account access

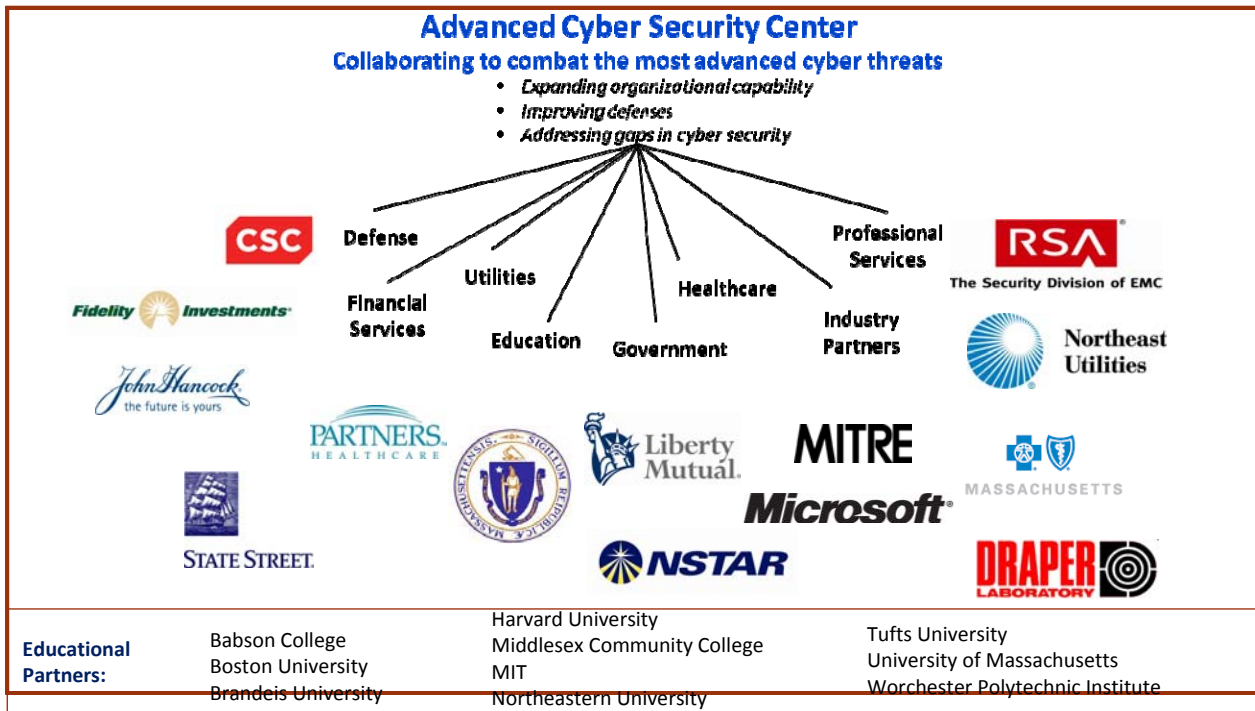
Key Requirements in the Massachusetts Regulations

- Designate an individual who will be responsible for your information security program.
- Develop a written information security policy.
- Identify what personal information your business possesses, where it is kept and who has access to it.
- Place reasonable restrictions on access to personal information: physical restrictions for hard copy files; log-in and password protection for electronic files.
- Take steps to ensure that third party service providers have the capacity to protect personal information.
- Prevent terminated employees from accessing personal information.
- Regular monitoring and updating of security measures.
- Document responsive actions taken in connection with any incident involving a breach of security.

Scope of the Federal Red Flags Rule v. the Massachusetts Data Security Rules

- Red Flags Rule focus on establishment of a system to identify, detect and mitigate identity theft.
- Massachusetts rules seek to prevent access to and breach of existing accounts.
- The federal Red Flags Rule are narrower than the Massachusetts rules:
 - The federal rules relate to creditors only.
 - Massachusetts rules apply to any person or legal entity.
- Both the Red Flags Rule and the Massachusetts Rules provide flexibility in how you meet their requirements. Key differences:
 - Red Flags Rule let you take account of the “complexity” of your business in designing solutions, Massachusetts does not.
 - Massachusetts permits you to take account of your available resources, but Red Flags Rule do not.

Getting Ahead of the Game: Is Industry Collaboration the Answer?



Special Partners:

Lincoln Laboratory, M.I.T.
Federal Reserve Bank of Boston
© 2011 Foley Hoag LLP. All Rights Reserved.

Resource:

PRICEWATERHOUSECOOPERS

Counsel:

FOLEY HOAG LLP

T3: 1/23/2011 10

