



**Chris Zoladz**

Founder  
Navigate LLC

### The Massachusetts Privacy Law – Lion or Lamb?

It has now been over 4 months since the Massachusetts General Law Chapter 93H and the accompanying regulation, (201 CMR 17.00: Standards for the Protection of Personal Information of Resident of the Commonwealth)<sup>1</sup> went into effect on March 1, 2010. Some viewed this new regulation as being a potential “game changer.” Despite the significant media coverage leading up to this new regulation there has been conspicuous silence since.

Chris Zoladz is the Founder of Navigate LLC (www.navigatellc.net), a consultancy that provides a broad range of strategic and tactical information protection & privacy services.

#### **Nymity: What are the key requirements of MA General Law Chapter 93H and the accompanying regulation, 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth?**

**Zoladz:** The regulation requires that certain policies, procedures and technology controls be in place to protect personal information of a Massachusetts resident on a continuous basis. Major requirements of this regulation require affected companies to:

- Maintain a Written Information Security Program (WISP);
- Designate one or more employees to maintain the information security program;
- Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks as exist in the company and at service providers<sup>2</sup>;
- Provide on-going training, including temporary and contract employees, for the proper use of the computer security system and the importance of personal information security;
- Implement policies with disciplinary action for non-compliance;
- Have a means for preventing and detecting system security failures;
- Develop security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises;
- Take reasonable steps to select and retain third-party service providers who are capable of, and agree in contract to, maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations;
- Limit the collection, access to, and storage of personal information;
- Implement reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers;
- Regularly monitor to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to, or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks;
- Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and
- Maintain an incident response plan.

<sup>1</sup> <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

<sup>2</sup> Defined in the regulation as “any person that receives, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation; provided, however, that “Service provider” shall not include the U.S. Postal Service.”

There are also specific computer system security requirements included in the regulation as summarized below. Companies that electronically store or transmit personal information pertaining to a Massachusetts resident must:

- Control user IDs and other identifiers that provide access to computer systems;
- Have a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
- Control system passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- Restrict access to active users and active user accounts only (e.g., no terminated employee should continue to have system access);
- Block access to the systems after multiple unsuccessful attempts to gain access, or place limitations on access to the particular system;
- Restrict access to records and files containing personal information to those individuals who need such information to perform their job duties;
- Assign unique identifiers plus passwords, (reasonably designed to maintain the integrity and security of the access controls) to each person with computer access. These should not be vendor supplied default passwords.
- Encrypt all transmitted records and files containing personal information that will travel across public networks, and encrypt all personal information to be transmitted wirelessly;
- Implement a process for the reasonable monitoring of systems, for unauthorized use of or access to personal information;
- Encrypt all personal information stored on laptops or other portable devices;
- Implement reasonably up-to-date firewall protection and operating system security patches, designed to maintain the integrity of the personal information in any files on a system that is connected to the Internet; and
- Maintain reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

**Nymity: Who does this law and regulation apply to?**

**Zoladz:** This law is applicable to any person or company that owns or licenses personal information about a resident of the Commonwealth. From a practical perspective, this law has a broad impact as many companies do business with residents of the Commonwealth. It is not just relevant to those businesses located in Massachusetts.

**Nymity: What makes this regulation different vs. other privacy laws?**

**Zoladz:** Unlike other privacy laws, this law contains much more detail regarding specific security and administrative controls that are required to be in place to protect personal information. Other privacy laws are more general in this regard and do not prescribe specific controls that need to be implemented, or at least to the extent required in this law.

**Nymity: Have other states followed suit with similar regulations?**

**Zoladz:** To date there are no other states that have enacted a similar regulation. However, as was the case several years ago when California enacted the first data security breach law and almost every other state followed, Massachusetts may well have the set the stage for other states to follow.

**Nymity: What has been the effect of this regulation?**

**Zoladz:** It is difficult to say at this point. My experience is that companies affected by this law fall into one of the following categories:

- Those that are not aware that the law affects their company, in some cases because they incorrectly believe it applies only to businesses located in Massachusetts, and thus they have not conducted any type of compliance assessment.
- Those that are aware of the law and the requirements and are addressing any compliance gaps.
- Those that are aware of the law and generally aware of the requirements but have not taken any action due to other priorities or resource constraints.

**Nymity: What additional security and privacy enhancement activities have companies initiated as a result of this regulation?**

**Zoladz:** It ranges from nothing to initiating significant technology and/or business process changes and everything in between. While the requirements in the regulation are arguably fairly straightforward and basic, they are not trivial, especially for a large company. For example, deploying encryption to all laptops that contain personal information in a large company can take months and require a significant investment. The amount of change really depends on the company's current state of compliance and the commitment that the security and privacy teams can obtain to drive compliance.

**Nymity: What investigations or enforcements have occurred?**

**Zoladz:** None that I am aware of. If there have been any they have certainly been inconspicuous.

**Nymity: Has the lack of enforcement to date resulted in companies delaying compliance efforts? Are companies at a greater risk if they delay compliance?**

**Zoladz:** The lack of apparent enforcement of the law certainly is not a call to action for most companies. The longer there is no enforcement the more difficult it may be for the security and privacy professionals to gain the support and resources needed to drive compliance. The longer companies delay compliance, the greater the risk that when enforcement commences, and it will, a non-compliant company may become the first major media story. Delaying compliance is like playing a game of chance, sometimes you win, other times you lose.

**Nymity: Is this regulation a lion or a lamb?**

**Zoladz:** I believe it is currently a lamb. Until there is active enforcement there is no burning platform to comply. However, if there is active enforcement, this regulation could be a lion or a "game changer."

**Nymity: What are the real world challenges companies are facing in complying?**

**Zoladz:** There is the ever present competition with other enterprise priorities balanced against limited and probably shrinking available resources. The current state of the economy makes it difficult for management to focus on activities that are not revenue generating or cost cutting. That's just a reality that has to be dealt with. However, legal requirements such as this can force the allocation of necessary resources to pursue compliance, but the lack of enforcement to date makes it easy to defer these compliance activities perhaps just a bit longer. In addition, depending on the company, compliance may not be inexpensive – there may be technology changes that are required, business process changes, or both, and change generally does not happen quickly and is not always embraced.

**Nymity: If a company cannot take steps to achieve full compliance, what can they do to mitigate the most significant risks?**

**Zoladz:** The most impactful action a company can take is also the most obvious – limit the amount of personal information that is subject to the regulation and needs to be protected. A core business practice should be to only collect the minimum amount of personal information required to execute the business transaction, manage your workforce, or meet any applicable legal requirement. The less personal information that is collected and stored, the less that has to be protected. However, this is a journey and requires business practice changes.

Next, focus on the requirements of the regulation that will have the most significant return on investment in terms of reducing the risk that there will be a reportable data breach or theft. I suggest this approach because enforcement of this regulation is likely to only occur when there is a data breach that requires disclosure. Therefore, if you are successful in avoiding a data breach of theft, your compliance with this regulation may never be questioned, which does not mean you should not take the necessary actions to comply.

**Nymity: What advice would you give companies that have not yet addressed their compliance risk?**

**Zoladz:** Do what you can as fast as you can. Regardless of your current state, any tasks no matter how modest that can be completed to strengthen your company's compliance are valuable. It is not always practical to complete all tasks as quickly as desired but delaying any action is not prudent.

**Nymity: In closing, what have you not discussed that would be meaningful for our readers to consider?**

**Zoladz:** While the regulation recognizes that compliance activities will vary depending on the size of the company and the amount of stored data, you should anticipate that a regulator will likely expect more of your organization than your own management. Actions taken to comply with this regulation will serve your company well as they should reduce the likelihood of a data breach or loss, protect your brand and customer/employee loyalty. In addition, it will also position your company well for the similar laws likely coming from other states or perhaps even at the Federal level.