JOURNAL OF INTERNET LAW
VOLUME 17
NUMBER 2
AUGUST 2013
EDITED BY DLA PIPER

Data Security Laws and the Cybersecurity Debate

By Corey M. Dennis and David A. Goldman

The ever-increasing threat of data security breaches and cyber terrorism has given rise to an intense debate over the nation's cybersecurity laws and has become a top concern for companies in the U.S. and abroad.[1] In fact, the head of the United States Cyber Command and Director of the National Security Agency, General Keith B. Alexander, recently warned that cyber-attacks have resulted in the "greatest transfer of wealth in history."[2]

Due to both government and private industry concerns, numerous federal data security bills have been proposed, but few have actually been enacted. Most recently, given congressional inaction in this area, President Obama issued a Cybersecurity Executive Order. This article discusses the existing state and federal data security regulatory schemes in the United States, the Cybersecurity Executive Order, and the debate surrounding recent cyber-security bills.

STATE DATA SECURITY AND BREACH NOTIFICATION LAWS

Data breach notification laws have been enacted in 46 states, as well as the District of Columbia, Puerto Rico, the U.S. Virgin Islands,

Continued on page 9

Corey M. Dennis *is an Associate at Governo Law Firm LLC in Boston, where he advises companies on compliance with data privacy and security laws, and represents companies in litigation matters. He is a Certified Information Privacy Professional (CIPP/US) and has published numerous legal articles on data privacy and security, social media, and other subjects. He can be reached at* cdennis@governo.com. ***David A. Goldman*** *is a Partner at Governo Law Firm LLC, where he advises companies on compliance with data privacy and security laws, and represents companies in litigation matters. He is a Certified Information Privacy Professional (CIPP/US) and has over two decades of litigation experience. He can be reached at* dgoldman@governo.com.

Wolters Kluwer
Law & Business

JOURNAL OF INTERNET LAW

EDITORIAL OFFICES

400 Hamilton Avenue
Palo Alto, CA 94301
(650) 328-6561

76 Ninth Avenue
New York, NY 10011
(212) 771-0600

JOURNAL OF INTERNET LAW (ISSN# 1094-2904) is published monthly by Aspen Publishers, 76 Ninth Avenue, New York, NY 10011. Telephone: 212-771-0600. One year subscription (12 issues) price: $552. Single issue price: $55. To subscribe, call 1-800-638-8437. For customer service, call 1-800-234-1660. **Purchasing reprints:** For customized article reprints, please contact *Wright's Media* at 1-877-652-5295 or go to the *Wright's Media* Web site at *www.wrightsmedia.com* Postmaster: Send address changes to JOURNAL OF INTERNET LAW, Aspen Publishers, 7201 McKinney Circle, Frederick, MD 21704.

Wolters Kluwer
Law & Business

Data Security Laws from page 1

and Guam.[3] Alabama, Kentucky, New Mexico, and South Dakota have no such equivalent laws. Though the data breach notification laws vary by jurisdiction, they generally require companies to notify consumers whose personal information has been compromised by a security breach "in the most expedient time possible" or "without unreasonable delay."[4]

A minority of states—including Massachusetts, California, Connecticut, Rhode Island, Oregon, Maryland, and Nevada—have also enacted data security laws requiring companies to maintain data security safeguards to protect state residents' personal information from being compromised.[5] These laws, intended to prevent data breaches and identity theft, typically require companies to implement and maintain reasonable security measures.

The Massachusetts data security regulations, 201 CMR 17.00 *et seq.*, effective as of March 2010, are among the most comprehensive and burdensome of the state data security laws. The Massachusetts regulations go beyond most other state data security laws by requiring every "person" or entity—including companies both inside and outside of Massachusetts—holding, processing, or otherwise accessing personal information of Massachusetts residents to:

- Develop a comprehensive written policy outlining its physical, administrative, and technical information security measures;
- Maintain extensive computer system security requirements (*e.g.*, secure user authentication protocols/passwords, secure access control measures, monitoring of systems, up-to-date firewalls, and virus/malware protection);
- Encrypt all records containing personal information transmitted over wireless networks or stored on portable devices;
- Require third-party service providers (*e.g.*, payroll providers, outsourcers) receiving personal information, by contract, to maintain security measures in compliance with the regulations;
- Train employees on compliance with data security policies; and
- Regularly monitor and review security measures, at least annually, to ensure they are preventing unauthorized access to personal information.

When the Massachusetts data security regulations became effective, some speculated that the regulations might become a model data security standard nationally. Although several states—including Connecticut, Vermont, and Texas—have been active in amending their breach notification laws in the past few years, none have adopted the comprehensive requirements of the Massachusetts data privacy regulations.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

The Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard established in 2004 by the major credit card companies that contractually requires merchants accepting credit, debit, and other payment cards to safeguard cardholder data. The PCI standards set forth extensive security requirements, including:

- Build and maintain a secure network (*e.g.*, maintain firewalls and secure passwords);
- Protect cardholder data (*e.g.*, through encryption);
- Maintain a vulnerability management program (including updated antivirus software and secure systems/applications);
- Maintain strong access control measures;
- Regularly monitor and test networks;
- Maintain a written information security policy;
- Train employees on compliance with data security policies;
- Maintain an incident response plan; and
- Monitor the PCI DSS compliance status of any service providers with whom cardholder data is shared, at least annually.

Some states, such as Nevada, have incorporated the PCI standards, including the encryption requirement, into their state data security laws.[6] The failure to comply with state data security laws or the PCI standards could give rise to regulatory enforcement actions under state unfair and deceptive acts statutes.

FEDERAL DATA SECURITY LAWS

Congress has enacted a number of laws governing data security in certain specific contexts, including:

- The Gramm-Leach-Bliley Act (GLBA), which mandates data security requirements for "financial institutions" (broadly defined to include banks, mortgage companies, insurance companies, financial advisors, investment firms, etc.);
- The Health Insurance Portability and Accountability Act (HIPAA), which requires health care providers to maintain security standards for protected health information;
- The Health Information Technology for Economic and Clinical Health (HITECH) Act, which strengthens penalties for HIPAA violations and extends HIPAA violation liability to "business associates" to whom protected health information is disclosed (*e.g.*, third-party administrators, accounting firms providing services to health care providers);
- The Children's Online Privacy Protection Act (COPPA), which requires covered Web site operators to maintain reasonable procedures to protect the personal information of children;
- The Fair Credit Reporting Act (FCRA), which imposes requirements for the collection, disclosure, and disposal of data collected by consumer reporting agencies; and
- The FTC's Red Flags Rule, which requires financial institutions and creditors holding consumer accounts to maintain a written identity theft prevention program.

Although many other data security bills have been proposed over the past few years, most were never enacted. Examples of recent legislative proposals include:

- The Cyber Intelligence Sharing and Protection Act (CISPA) and the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2013 (SECURE IT Act), which would promote voluntary sharing of cyber threat information between private companies and the government, and provide liability protections for companies engaging in such information sharing;
- The Cybersecurity Act of 2012, which would create "cybersecurity performance requirements" and voluntary cyber threat information sharing standards among private sector companies operating critical infrastructure (e.g., energy, water, transportation); and
- The Data Security and Breach Notification Act of 2012, which would require companies to maintain "reasonable" security measures to protect personal information and establish a uniform breach notification law.

There is currently no federal statute imposing general data security standards on companies in all industries. However, the FTC—taking the position that it has general authority over "unfair and deceptive practices" related to data security—has brought numerous enforcement actions against companies alleging data security violations under Section 5 of the FTC Act, which bars "unfair or deceptive acts or practices in or affecting commerce."[7]

There have been few challenges to the FTC's authority to enforce data security laws, since prior cases have settled by consent orders before any significant litigation activity. However, a recent case, *FTC v. Wyndham Worldwide Corporation*,[8] raises the unresolved question of the scope of the FTC's authority to regulate data security in the absence of specific legislation. In this case, Wyndham moved to dismiss the FTC's enforcement action on the ground that the Commission has no authority to establish and enforce data security standards under the "unfairness" prong of Section 5. A decision in Wyndham's favor would undermine the FTC's authority in the area of data security going forward.

CYBERSECURITY EXECUTIVE ORDER

On February 12, 2013, President Obama signed an Executive Order on *Improving Critical Infrastructure Cybersecurity*, which increases information sharing between the government and the private sector and establishes a "Cybersecurity Framework" to reduce cyber risks to critical infrastructure. The President also issued a related Policy Directive on *Critical Infrastructure Security and Resilience*.

The Executive Order is aimed at private sector companies operating critical infrastructure

(*e.g.*, energy, water, transportation, telecommunications, financial services), but also could apply to companies that are regulated by sector-specific agencies as well as other companies. The Executive Order:

1. Creates information-sharing mechanisms between private industry and government;
2. Requires the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework to reduce critical infrastructure cyber risks; and
3. Requires the Department of Homeland Security, in conjunction with sector-specific agencies, to establish a voluntary critical infrastructure cybersecurity program to support the adoption of the Cybersecurity Framework.

Although the Executive Order does not precisely designate the "critical infrastructure" subject to the Order, the Policy Directive identifies 16 critical infrastructure sectors:

1. Chemical;
2. Commercial facilities;
3. Communications;
4. Critical manufacturing;
5. Dams;
6. Defense industrial base;
7. Emergency services;
8. Energy;
9. Financial services;
10. Food and agriculture;
11. Government facilities;
12. Healthcare and public health;
13. Information technology;
14. Nuclear reactors, materials, and waste;
15. Transportation systems; and
16. Water and wastewater systems.

THE CYBERSECURITY DEBATE

In light of these developments, the cybersecurity debate has intensified in recent months. Some important questions raised include: Should further federal data security legislation be enacted? Should legislation providing for voluntary information sharing and liability protections for private industry related to cyber threats be enacted?

While generally Democrats have favored—and Republicans have opposed—such legislation in the past, many Republicans have supported the Cyber Intelligence Sharing and Protection Act (CISPA), which promotes voluntary information sharing between private industry and government, and provides liability protections for companies engaged in such information sharing. CISPA recently passed the House of Representatives, despite a veto threat from the Obama administration, but it is not expected to pass the Senate.

Nevertheless, more cybersecurity legislation is expected. In fact, President Obama declared in the State of the Union address earlier this year that "America must also face the rapidly growing threat from cyber-attacks," calling upon Congress to act by "passing legislation to give our government a greater capacity to secure our networks and deter attacks."[9] Cybersecurity will no doubt engender debate in the coming months, as both government and the private sector continue to grapple with escalating cyber threats.

NOTES

1. *See* Julia Boorstin, "Privacy vs. Cybersecurity: The Debate Heats Up," CNBC Media Money Blog (April 10, 2013), *http://www.cnbc.com/id/100632315*.
2. *See* David E. Sanger & Mark Landler, U.S. and China Agree to Hold Regular Talks on Hacking, The New York Times (June 1, 2013), *http://www.nytimes.com/2013/06/02/world/asia/us-and-china-to-hold-talks-on-hacking.html?pagewanted=all*.
3. *See* State Security Breach Notification Laws, National Conference of State Legislatures, *http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx*.
4. *See, e.g.*, Cal. Civ. Code § 1798.82; Mass. Gen. Laws ch. 93H, § 3; N.Y. Gen. Bus. § 899-aa; R.I. Gen. Laws 11-49.2-3.
5. *See* 201 CMR 17.00 *et seq.*; Cal. Civ. Code § 1798.81.5; Conn. Gen. Stat. § 42-471; R.I. Gen. Laws § 11-49.2-2; Or. Rev. Stat. § 646A.622; Md. Code, Comm. Law § 14-3501; Nev. Rev. Stat. § 603A.210.
6. *See* Nev. Rev. Stat. § 603A.215.
7. 15 U.S.C. § 45.
8. *See* Federal Trade Comm'n v. Wyndham Worldwide Corp., No. 2:13-cv-01887 (D. N.J. 2013).
9. *See* Barack Obama, "The 2013 State of the Union," *http://www.whitehouse.gov/state-of-the-union-2013*.