InsideCounsel.com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
April 25, 2014

The gathering storm: What to expect in the future of cybersecurity litigation

By focusing on new standards that might emerge, we hope to provide a guide for future-proofing current in-house practices

BY RICHARD MARTINEZ

Navigating the fast-moving and quickly-evolving area of privacy and cybersecurity (PCS) litigation is no easy task. Not only are the technological challenges emerging at a lightning-quick pace, but the legal landscape is also changing — a perfect storm for in-house counsel. In the last article, we focused on the liability standards that companies today are likely to confront in litigation over a data breach. In this article, we expand on that theme by focusing on new standards for liability that businesses may face in the future given the legislative proposals now being considered on the federal and state levels.

By focusing on new standards that might emerge, we hope to provide a guide for future-proofing current in-house practices. Given the intense media attention and public scrutiny, it is very likely that some of the proposals under consideration will be adopted. As an overview, pending legislation has the following common themes:

- Early disclosure to consumers
- Expanded private liability for data breaches
- Compensation to consumers for data breaches
- An increasing role for state and federal regulatory agencies in data privacy and cybersecurity issues

On the federal level, Congress is considering a variety of bills to increase the liability of businesses that fail to safeguard consumer information or promptly report data breaches to consumers and law enforcement. For example, under the **Data Security and Breach Notification Act of 2014** proposed by Senators Dianne Feinstein (D-Calif.) and John Rockefeller (D-W.Va.), businesses would be legally obligated to notify every person in the United States believed to have been compromised by a data breach within 30 days of the business discovering the breach. Failure to comply with this requirement would trigger hefty civil fines of up to $100,000 a day, with a maximum total penalty of $1 million for a single breach.

Data breach notification is also a significant feature of the **Personal Data Privacy and Security Act of 2014** proposed by Senator Patrick Leahy (D-Vt.). In particular, the Act would require that that businesses notify law enforcement of data breaches no less than 10 days after discovery of the breach if the breach involves more than 5,000 individuals or a database containing information about more than 500,000 individuals. In turn, the Federal Trade Commission, the U.S. Attorney General, and state attorneys general would each be empowered to enforce this notification requirement and penalize violators with fines of up to $11,000 per day per data breach (with a cap of $1 million per breach).

State legislatures are no less eager than Congress to impose new liabilities on businesses that own or maintain the personal information of their customers. For example, on April 10, 2014, Kentucky became the 47th state to enact a data breach notification law, leaving Alabama, New Mexico and South Dakota as the only states to still not have such a law on the books. Additionally, according to the National Conference of State Legislators, "[a]t least 19 states have introduced or are considering security breach legislation in 2014."

In this regard, while much of new legislation being considered at the state level merely serves to amend pre-existing laws, **several of these bills would expand private liability for data breaches in significant ways**. For example, in a bill now before the Minnesota state legislature (H.F. 2253, introduced in February 2014), any entity conducting business in the state would be required to inform customers of a data breach affecting the customer's personal information within 48 hours of the business discovering or being notified of the breach. Businesses would also be required to compensate consumers whose information had been breached by providing these consumers with both one year's worth of free credit monitoring services, made available within 30 days of the breach, and repayment of any charges or fees incurred by the consumer as a result of the breach. Retailers of consumer goods and services would additionally be required to provide a $100 gift card to each consumer whose information was breached.

New laws are not the only source of new liability in the world of PCS litigation. Indeed, **federal and state agencies** are capable of raising the bar for businesses through their rulemaking authority and their public proclamations. Consider the following April 2014 announcement by the Federal Financial Institutions Examination Council (FFIEC) addressing the recently revealed "Heartbleed" vulnerability in the encryption code used by many businesses to safeguard consumer transactions online: "Financial institutions should operate with the assumption that encryption keys used on vulnerable servers are no longer viable for protecting sensitive information and should therefore strongly consider requiring users and administrators to change passwords after applying the OpenSSL patch." Such language is bound to be cited by plaintiffs in asserting negligence-related claims against financial institutions and other businesses that suffer Heartbleed-related data breaches in the wake of the FFIEC's advice.

In PCS litigation, preparing for tomorrow means understanding not only where the law is right now but also the direction in which the law is headed. On this score, Congress and state legislatures are considering a bevy of new laws that will significantly increase the obligations and liabilities that businesses must face in the wake of a data breach. It is therefore critical that in-house counsel maintain a constant awareness of these developments if they are to provide their clients with effective advice on how to best prepare for this brave new world.

About the Authors

Richard Martinez
Richard Martinez is a trial attorney at Robins, Kaplan, Miller & Ciresi L.L.P. Rick's practice focuses substantially on technology, primarily in the areas of intellectual property litigation. His practice is also active in matters before the International Trade Commission, and in the areas of cyber security, data privacy, and information law.