ARE LAW FIRMS READY TO TACKLE DATA PRIVACY?

As Society Becomes More Digital—and Cyberattacks Become More Sophisticated—Lawyers Must Have the Technology to Protect Their Information

By Maryam Meseha

Technology continues to develop and modernize the way businesses interact with each other and the world. The extensive and ongoing integration of technology in the workplace requires a contemporary understanding of data privacy and the laws that govern digitally stored information. As e-commerce and information technology sectors continue to expand, cybercrimes continue to increase.[1]

The American Bar Association publishes its annual Techreport, which gathers information from across the nation and sorts it based on attorney demographics, location and other categories. In its 2019 Legal Technology Survey, the American Bar Association asked its members various questions in order to determine how they were using information technology in their practice. These American Bar Association surveys are regarded as the most comprehensive surveys pertaining to law firm budgeting and use of technology. Although 60% of all firms budget for IT, 60% of solo practitioners stated that they did not budget for it.[2] Comparatively, only 44% of firms with two to nine attorneys stated that they did not budget for technology. The largest segment of the legal marketplace is composed of solo and small firms, and many of them do not budget for technology. Since IT is an essential part of running any organization in the 21st century, companies must be vigilant in protecting its business and client information against data breaches.

New Jersey has recognized the need for comprehensive regulations and regulatory bodies that address cybercrime and data security. Thus, New Jersey has created several organizations tasked with developing procedures for proper digital security systems use, as well as general oversight regarding data security systems used in businesses. The New Jersey Office of Information Technology, pursuant to N.J.S.A. 52:18a-230b, is responsible for the standards and policies governing state agencies' use of technology. It is the exclusive government provider of information technology services for New Jersey's executive branch, aimed at protecting the integrity and confidentiality of its information systems, as well as, protecting the privacy of its clients and their data. The office provides for certain enterprise services to manage the day-to-day maintenance and operation of IT services concerning data security.

The New Jersey Cyber Security & Communications Integration Cell is another organization concerned with proper cybersecurity and data handing. The cell provides for cybersecurity information sharing, incident reporting and threat analysis for local, state, federal and industrial institutions.[3] In its weekly bulletin, the NJCCIC publishes statistics regarding malicious activity and threats targeting New Jersey networks. These statistics show where breaches are perpetrated, the nature of any breaches, whether the breaches were carried out by organized groups and what businesses were impacted by any breaches. The NJCCIC also gathers information from the IBM X-Force Threat Intelligence Index and Proofpoint Quarterly Threat Reports in compiling the information used in its bulletins.

The New Jersey Office of the Attorney General's Division of Law also recently announced its newly created Data Privacy and Cybersecurity office, a section within the Affirmative Civil Enforcement—Newark Practice Group.[4] This office will conduct security investigations regarding internet privacy and data security on behalf of the State of New Jersey and the Division of Consumer Affairs.[5] Collectively, these organizations provide the foundation for cybersecurity and digital privacy regulation in New Jersey.

The New York and California Approach to Data Privacy

Other states have also recognized the need for more comprehensive data security regulations. California was one of the first states to enact legislation that specifically addressed the concerns many citizens have regarding business's use of client information and its susceptibility to data breaches.

In 2018, California enacted the California Consumer Privacy Act (Cal Civ Code §§ 1798.100-1798.199). This act creates consumer rights regarding the collection, sharing, deletion and accessibility of personal information collected

MARYAM M. MESEHA *is the Co-Chair of the Cyber Security & Data Privacy Practice Group at Scarinci & Hollenbeck LLP in Lyndhurst. As a seasoned litigator, Maryam is uniquely qualified to address privacy laws in varying industries and applications.*

by businesses.[6] Under this act, the Attorney General is permitted to bring enforcement action where business fail to comply with regulations and procedures for proper data management and storage. A consumer has the right to request "categories and specific pieces of personal information the business has collected" with regard to that consumer.[7] These businesses must meet a revenue threshold requirement to fall within the jurisdiction of this act.[8] The Attorney General will be permitted to bring enforcement actions beginning in July 2020.

In May 2019, state Sen. Kevin Thomas introduced the New York Privacy Act. This legislation differs from the California Consumer Protection Act insofar as it allows persons to file lawsuits against companies, where they suffer injury due to a company's violation of the proposed act.[9] Under this act, residents would be permitted to access information companies collect on them, as well as request the deletion or modification of any such information.[10] Additionally, whereas the California Consumer Protection Privacy Act has a revenue requirement for defendant companies, the New York Privacy Act has no such revenue jurisdictional requirement.

Data Privacy and Cybersecurity Litigation

While some firms have taken measures to upgrade their data security, many organizations have been slow to implement preventative data security measures. Failure to observe proper data security procedure could make organizations more susceptible to cyberattacks. In the last decade some of the nation's largest companies have been defendants to lawsuits concerning their data privacy and cybersecurity systems.

Target Corporation fell victim to a cyber attack in November 2013. More than 100 million credit and debit card users, all of whom made purchases at Target between November and December 2013, had their financial information compromised. Target ultimately agreed to pay an $18.5 million multistate settlement for this breach, which affected more than 41 million Target customers' payment accounts on record.

After ensuring compliance with government regulations, companies should properly budget for technology in company accounts. Proper budgeting for technology shows company awareness of cybercrime and the growing threat of data breaches.

Home Depot was the victim of an even larger breach from April to September 2014.[11] Home Depot announced that more than 50 million credit cards were compromised as a result of hackers obtaining third-party vendor user names and passwords, which they used to penetrate Home Depot's network.[12] Home Depot estimated that the breach cost it more than $60 million and amounting to a 7-cent-per-share loss from its 2014 earnings.[13]

There is also ongoing litigation involving Wawa, a New Jersey corporation with more than half of its stores located in Pennsylvania and New Jersey.[14] Wawa has been subject to a number of class action lawsuits which began in December 2019.[15] According to an open letter from Wawa's CEO at that time, the company suffered a breach in its credit card payment data systems. The breach was the result of malware which the company believes was present and active in the system since March of that year. Wawa has stated that all of its 850 locations may have been subjected to malware. Although Wawa has claimed that the breach did not disclose security codes or personal identification numbers, the malware did target cardholder names, debit and credit card numbers, and card expiration dates.[16] Both consumers and financial entities have brought lawsuits against Wawa alleging, *inter alia*, failure to observe best practices in data security and failure to observe Federal Trade Commission minimum security standards.

The above mentioned cases are just a few of the most recent instances of litigation arising from data breaches. Much of this litigation came in the form of class actions, with settlements reaching upwards of eight figures. Following the conclusion of these high profile cases, many companies are beginning to recognize the importance of proper data security and the risks associated with failure to implement sufficient data information and cybersecurity procedures. Although recognition of possible company exposure to data breach litigation is the first step toward improved information security, companies should also take proactive steps to ensure that business and client data is sufficiently protected.

Protecting Your Company

Companies can take substantial strides toward improving their cybersecurity and insulating themselves against potential data breaches. The first step is to make sure that the security system complies with any applicable state or federal laws. After ensuring compliance with government regulations, companies should properly budget for technology in company accounts. Proper budgeting for technology shows company awareness of cybercrime and the growing threat of

data breaches. This budgeting should not only focus on the use and maintenance of secure IT systems, but also proper training for employees. Properly trained employees will be able to identify potential scams which could provide hackers with access to company data.

Finally, companies should subscribe to organizations, such as the NJCCIC, that publish memorandums and notices concerning cyberattacks and information security in New Jersey. Many of these organizations provide for best practices in data security, and also suggest systems which companies may want to purchase. Companies who implement these suggested courses of action, will be well on their way to a secure data information system. ⚖

Justin Hill, a member of Rutgers School of Law's Class of 2020, contributed to this article.

Endnotes

1. A Glance at the United States Cyber Security Laws, Hardeep Singh (Jan. 7, 2016), appknox.com/blog/united-states-cyber-security-laws
2. Techreport 2019: Budgeting & Planning, Law Technology Today (Nov. 20, 2019), lawtechnologytoday.org/2019/11/techreport-2019-budgeting-planning/
3. Defending New Jersey's Digital Destiny, New Jersey Cybersecurity and Communications Integration Cell, cyber.nj.gov/about
4. Data Privacy & Cybersecurity, The State of New Jersey, Department of Law & Public Safety, Office of the Attorney General, nj.gov/oag/law/dpc.htm
5. Id.
6. Background on the CCPA & the Rulemaking Process, State of California Department of Justice, oag.ca.gov/privacy/ccpa
7. Cal. Civ. Code § 1798.100 (2018).
8. Proposed New York Bill Expands Scope of Data Privacy Debate, The Brookings Institution, Jack Karsten and Raj Gambhir (June 24, 2019), brookings.edu/blog/techtank/2019/06/24/proposed-new-york-bill-expands-scope-of-data-privacy-debate
9. Id.
10. Id.
11. With 56 Million Cards Compromised, Home Depot's Breach is Bigger than Target's, Forbes, Kate Vinton (Sept. 18, 2014), forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/#5671132a3e74
12. The Home Depot Reports Findings in Payment Data Breach Investigation, The Home Depot (Nov. 6, 2014), ir.homedepot.com/news-releases/2014/11-06-2014-014517315
13. See With 56 Million Cards Compromised, Home Depot's Breach is Bigger than Target's supra
14. Wawa Faces Group of Credit Card Class Actions over Breach, The Legal Intelligencer, Max Mitchell (Feb. 11, 2020), law.com/thelegalintelligencer/2020/02/11/wawa-faces-group-of-credit-card-class-actions-over-data-breach/; Wawa Data Breach Could Impact 30 Million Payment Cards, The Legal Intelligencer, Patrick McKnight (Feb. 20, 2020), law.com/thelegalintelligencer/2020/02/20/wawa-data-breach-could-impact-30-million-payment-cards/
15. See Wawa Faces Group of Credit Card Class Actions over Breach, supra
16. See Wawa Data Breach Could Impact 30 Million Payment Cards, supra