Published on *The National Law Review* https://natlawreview.com

Some Thoughts on the Year in Privacy and Data Security Law

Article By:

Edward J. McAndrew

David M. Stauss

As we turn the page on 2018, let's reflect on some of the key privacy and cybersecurity issues that will continue to occupy our hearts and minds in 2019.

Owning the Mega-Breach

2018 was the year in which data breaches in mergers and acquisitions became the iceberg in full view. This fuller realization of cyber risk in transactions, though, actually has its origin in September 2016 – when Yahoo and Marriott were in the midst of deals that would involve some of the largest data breaches on record.

While negotiating its sale to Verizon back in September 2016, Yahoo first disclosed a massive breach of its user database – which would grow to include its entire population of approximately 3 billion users. Also in September 2016, Marriott purchased Starwood Hotels & Resorts Worldwide, Inc., including the largest hotel reservation system in the world. Unbeknownst to Marriott, that system was then under an active hacking campaign that began in 2014 and would continue until September 2018

How liability for such massive breaches can change hands during major transactions became clear in 2018. Verizon purchased Yahoo's breached networks and Marriott purchased Starwood's breached reservation system. A key difference between the two situations is in the timing of the disclosures and the hacking incidents themselves relative to the deals. Verizon (and the world) learned of the Yahoo breaches before the transaction closed, and was able to ensure that the hacking incidents had been contained and remediated. Marriott did not learn of the Starwood breaches until two years *after* the deal closed – during which time the hacking incident continued until Marriott discovered it on its own. Going forward, heightened due diligence related to cybersecurity needs to become a much greater priority in deals.

The SEC Steps into Cybersecurity

2018 was the year in which the U.S. Securities and Exchange Commission squarely inserted itself into cybersecurity regulatory compliance.

In February 2018, the SEC released its first Commission-level Interpretive Guidance relating to public company disclosures of cybersecurity risks and incidents. Two key compliance takeaways are: (1) investor risk related to known cyber incidents must be fully and timely disclosed; and (2) public companies must police insider trading based on information related to undisclosed cyber incidents. Whether a cyber incident is material and requires disclosure will depend on a host of factors, including the nature, extent, and potential magnitude of the incident. This includes consideration of the type of compromised information (personally identifiable information, intellectual property or other confidential business information); the incident's impact on operations; the harm to a company's reputation, financial performance, customer/vendor relationships; and potential liabilities in civil litigation or regulatory enforcement actions. To avoid even the appearance of improper trading, companies "should consider whether and when it may be appropriate to implement restrictions on insider trading" during the investigation and assessment of significant cybersecurity incidents.

Just a month after issuing its Interpretive Guidance, the SEC penalized Yahoo $35 million for failing to timely disclose its data breaches. The cease and desist order was the SEC's first against a public company for failing to disclose known cyber incidents in its public filings. From 2014-2016, the SEC alleged, Yahoo filed a number of reports and statements with the SEC that misled investors about Yahoo's cybersecurity history. For instance, in its 2014-2016 annual and quarterly reports, the SEC found that Yahoo included risk factor disclosures stating that the company "faced the risk" of potential future data breaches, "without disclosing that a massive data breach had in fact already occurred." Yahoo filed a July 2016 proxy statement relating to its proposed sale to Verizon that falsely denied knowledge of any such massive breach. It also filed a stock purchase agreement that it knew contained a material misrepresentation as to the non-existence of the data breaches.

Finally, in October 2018, the SEC released a "Report of Investigation" into whether nine public companies violated U.S. securities laws "by failing to have sufficient accounting controls" to prevent approximately $100 million in losses as a result of "business email compromises" (BECs) targeting their personnel. The Report was prompted by the SEC's investigation The nine companies were victimized by one of two variants of the BEC scheme—involving spoofed or compromised emails from a person purporting to be a either a company executive or a vendor.

The SEC advised companies to "pay particular attention to the obligations imposed by Section 13(b)(2)(B) to devise and maintain internal accounting controls that reasonably safeguard company and, ultimately, investor assets from cyber-related frauds." The SEC emphasized that these fraud schemes were widely successful because they used "technology to search for both weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective." The victimized issuers had policies and procedures requiring different authorization levels for payments; management approval of outgoing wires; and verification of changes to vendor data. The critical flaw was in employee interpretation of these controls as capable of being satisfied solely through electronic communications—along with their failure to recognize obvious indications of fraud in the emails.

This report follows on the heels of a July 2018 FBI Public Service Announcementthat it had tracked more than 78,000 BECs—totaling more than $12.5 billion in fraud losses—since October 2013. The FBI has identified more than 41,000 BEC victims in the United States—with more than $3 billion in fraud losses since 2013, and $1.6 billion in fraud losses since May 2016.

States Continue to Expand Data Security Laws

Last year saw the creation and significant expansion of data security laws in state houses across the

country. The new laws fall into two primary categories: (1) statutory requirements that all organizations must create and implement reasonable cybersecurity programs to protect personal information; and (2) more expansive data breach notification laws.

Data Security Laws

At least twenty states have adopted broadly applicable "data security" statutes that require virtually all organizations that collect or possess personal information to maintain reasonable cybersecurity programs. Delaware's new law is a good example. It requires "[a]ny person" conducting business and owning, licensing, or maintaining personal information to implement reasonable security measures "to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business." Other states – such as Alabama – enacted "data security" laws that are much more prescriptive, listing factors to be considered in assessing 'reasonableness.'

Data Breach Notification Laws

At least thirty-one states considered data breach legislation in 2018. With new legislation in South Dakota and Alabama, all fifty states now have data breach notification laws. The biggest changes in 2018 included broad expansions of the definition of protected "personal information;" specified timeframes for notification to consumers and state attorneys general; mandatory credit monitoring for certain types of breaches; and disclosure and investigative cooperation requirements imposed upon third party service providers.

A Landmark Mobile Privacy Decision

The Supreme Court's 2018 decision in *Carpenter v. United States* establishes broad digital privacy rights that are sure to extend beyond law enforcement investigations and locational information. The decision significantly expands the Court's dominant theme of this decade that "digital is different" when it comes to modern privacy law.

The decision itself holds that the Fourth Amendment requires the government to secure a search warrant to obtain a person's historical cell site location information from a cellular service provider. That undersells its import though. *Carpenter* remakes the foundational legal principles governing privacy in data shared between device users and their service providers.

It's how the Court got to that holding that is so groundbreaking. First, the Court declared that "[i]ndividuals have a reasonable expectation of privacy in the whole of their physical movements." The Court characterized the cell site location information at issue as "detailed, encyclopedic, and effortlessly compiled" – allowing the government (and the service providers) to conduct "near perfect surveillance" on users. Second, this "reasonable expectation of privacy" is not defeated simply because each device constantly shares its location with cellular service providers. Data that must be shared for the proper functioning of technology services does not lose its privacy protection simply because it is possessed by and compiled in the business records of third parties. The spark of this reasoning is sure to spread quickly across the digital legal landscape in 2019 and beyond.

California Continues Pushing the U.S. Forward

California has repeatedly been at the epicenter of privacy and data security legislation in the United

States, perhaps most notably by being the first state to enact a breach notification statute. This past year, California once again broke new legislative ground by enacting the California Consumer Privacy Act of 2018 (“CCPA”) and legislation directed at securing IoT devices.

If you are reading this blog post, there is very little chance that you are unfamiliar with the CCPA, such that there is no point in summarizing its provisions. In fact, if we could jump forward five years, the CCPA’s significance will likely not merely be what businesses will need to undertake in 2019 to drive compliance, but rather it will be as a harbinger for the enactment of other privacy-related legislation in this country. One can readily envision that the CCPA will lead either to the enactment of federal privacy legislation or to more state laws directed at privacy. It is not hyperbole to say that how this unfolds in 2019 will set the course for privacy legislation in this country for years to come.

Similarly, California’s enactment of first-in-the-nation legislation directed at IoT device security is significant not just for what the legislation says, but also for what it signals will happen in the coming years. If you have tracked the IoT marketplace, you have heard the projections about the rapid expansion in the number of IoT devices in the next five years. But, at the same time, manufacturers have little incentive to build information security and privacy into those devices. Most commentators seem to agree that this will have to change but it is anyone’s guess as to how. Will industry self-regulate? Will the European Union lead the charge? Will plaintiffs’ lawyers find success in bringing class actions against IoT device manufacturers? Will the federal government pass legislation?

The California legislation offers one potential answer, which is that states will begin to legislate in this field. Indeed, California’s legislation – which originated as a botnet prevention measure – focuses only on a small aspect of IoT device security, namely, passwords. There is fertile ground for states to take up other issues such as requiring manufacturers to provide devices that do not have existing security flaws and requiring manufacturers to provide security patches.

Copyright © by Ballard Spahr LLP

National Law Review, Volume IX, Number 4

Source URL:https://natlawreview.com/article/some-thoughts-year-privacy-and-data-security-law