Westlaw Journal
GOVERNMENT CONTRACT
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 30, ISSUE 12 / OCTOBER 10, 2016

EXPERT ANALYSIS

Emerging Trends in Privacy and Cybersecurity

By Stuart D. Levi, Esq.
Skadden, Arps, Slate, Meagher & Flom

In 2016, the relentless stream of cyberattacks has continued unabated, having become a "business as usual" reality to which companies must adapt. All companies, regardless of size or industry, are potential targets, and the pool of attackers is expanding. Below is an overview of the key themes that emerged in 2016 and what we expect to continue seeing.

BEST PRACTICES FOR CYBERSECURITY PREPAREDNESS

A number of regulators, including the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE), have issued guidance and alerts about cybersecurity preparedness. The good news for companies, whether regulated or not, is that consistent themes are emerging as to what constitutes best practices. They include:

- Conducting a risk assessment. Cybersecurity preparedness needs to start with assessing the company's risks and designing a plan that addresses those risks.
- Strong governance. A cybersecurity plan must involve the active participation of senior management, and where applicable, the board.
- Data access. Employees should be able to access only the data they require, with appropriate authentication steps, and the company should have a means of tracking and reviewing that access.
- Training. Many attacks prey on employees who may unknowingly surrender their passwords or click on malware links. Regular employee training on cybersecurity is therefore critical.
- Vendor management. Attacks are often launched through a third-party vendor that has access to the company's system for business purposes. Companies must have robust cybersecurity requirements for vendors. These requirements should be based on the level of access a vendor has to the company's system, not the value of the contract.
- Incident response plan. All companies should have incident response plans to deal with cyberattacks that are regularly updated, and should conduct regular tabletop exercises to walk through different scenarios.
- Cyber insurance. Cyber insurance is emerging as an important component of any risk mitigation strategy. Given that this is a nascent area of coverage, companies should consult with insurance experts to review their policies and make sure they are getting appropriate coverage.
- Information sharing. Companies across multiple industries have begun to appreciate that sharing cyberthreat information and best practices with their competitors is a critical tool to reduce risks. The White House has been encouraging this practice, and in February 2015, President Barack Obama issued an executive order encouraging the development and

formation of Information Sharing and Analysis Organizations. Companies should consider joining an information-sharing group in their industry.

OUTLOOK ON LEGISLATION

As in previous years over the past decade, Congress attempted to enact various privacy or cybersecurity legislation. These initiatives were expected to gain more traction following President Obama's release of a number of proposed bills in January 2015, including a federal data breach notification law and information-sharing legislation.

However, the only piece of legislation that was enacted was the Cybersecurity Act of 2015, a bill that made it through Congress at the end of the year as part of the 2016 omnibus spending bill. The act creates a voluntary framework for real-time sharing of "cyber threat indicators" and "defensive measures" and provides liability protections and an antitrust exemption for such sharing.

Cybersecurity preparedness needs to start with assessing the company's risks and designing a plan that addresses those risks.

It is very unlikely, especially given the election cycle, that any other meaningful privacy or cybersecurity legislation will be enacted in 2016. Indeed, state attorneys general responded to widespread calls for a federal data breach notification law by urging Congress to preserve state authority in this area.

THE ROLE OF THE FTC

The Federal Trade Commission (FTC) has long been the most active regulator in the areas of privacy and cybersecurity.

In 2015, the FTC won a significant victory when the U.S. Court of Appeals for the Third Circuit held in *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015), that the agency has authority to deem a company's cybersecurity practices unfair under Section 5 of the FTC Act, and that companies had fair notice as to what practices could violate that section.

However, as the year drew to a close, the FTC was handed a defeat when its own administrative law judge held in the *LabMD* case that the FTC must show more than the mere "possibility" of harm from a cybersecurity incident in order to sustain a Section 5 case. *LabMD Inc.*, 2015 WL 7575033 (F.T.C. Nov. 13, 2015).

Many wondered whether this decision would in any way curtail the FTC's efforts in this area. Any doubt was, however, fairly quickly eliminated, when the FTC commissioners rejected the judge's decision that the commission had to show actual or probable harm to consumers in order to bring a claim that the company had engaged in unfair practices under the FTC Act. *LabMD Inc.*, 2016 WL 4128215 (F.T.C. July 28, 2016).

According to the commissioners, the legal standard for unfairness includes claims where the impact of an injury is large even if the likelihood of such injury is low.

This ruling signals that the FTC will have a low bar for finding injury in a data breach case, and that companies should be familiar with the types of cases the FTC is bringing in order to understand the issues on which the agency is focused.

EU EMERGES AS A FORCE TO BE RECKONED WITH

Although the European Union has had a robust privacy regime for close to 20 years, the impact on U.S. companies has been relatively limited. A dramatic shift in this equation occurred last year.

In December 2015, the EU announced completion of a new General Data Protection Regulation (GDPR), which will replace and significantly broaden the current EU Data Protection Directive. The GDPR was adopted in April 2016 and will go into effect in April 2018. The impact on any company doing business with European residents — even if not situated in Europe — will be significant.

The expanding impact of the EU was also felt in October 2015, when the Court of Justice of the European Union invalidated the U.S.-EU Safe Harbor framework on which thousands of companies had relied to send personal data from the EU to the U.S.

The court also empowered local data protection authorities to decide for themselves whether personal information was being protected by international agreements. These developments suggest a far more activist European privacy regime than had been in place — one that could have a significant impact on global commerce in 2016 and beyond.

Indeed, the Privacy Shield, which has been proposed as the replacement for the Safe Harbor, has been criticized by data protection authorities as not going far enough to protect EU residents against data access by the US government.

While we anticipate the Privacy Shield will be enacted in 2016, it remains to be seen whether companies embrace it, and whether it is subject to the same legal challenges as the Safe Harbor.

One of the latest developments has been a request by the Irish data protection commissioner that the Court of Justice of the European Union determine the validity of the "model contracts" used by thousands of companies to send data outside the EU.

If the court were to decide that model contracts may no longer be used as a transfer mechanism, companies could be left with few practical alternatives for transfer of such data, which could significantly disrupt business activities until a new transfer mechanism is approved.

Cyber insurance is emerging as an important component of any risk mitigation strategy.

CLASS ACTION LAWSUITS MUST REMAIN PART OF A COMPANY'S RISK CALCULUS

Most data breaches result in multiple class action lawsuits against the victim company. The gating issue has been whether the plaintiffs' alleged injury is sufficiently concrete and imminent to establish Article III standing, especially since these plaintiffs often have not suffered any monetary loss or other tangible injury.

Cases from the past year offered little clarity on this issue. For example, a Seventh Circuit panel ruled in mid-April in *Lewert v. P.F. Chang's China Bistro*, 819 F.3d 963 (7th Cir. 2016), that customers affected by a data breach involving credit card information have standing to sue, despite not suffering any actual out-of-pocket financial harm.

However, the next month, a Maryland federal court dismissed a putative class action brought by CareFirst policyholders affected by data breaches, holding that the plaintiffs lacked standing because the complaint did not allege facts showing "certainly impending" harm or a "substantial risk that the harm will occur" as a result of the breaches. *Chambliss v. CareFirst Inc.*, No. 15-cv-2288, 2016 WL 3055299 (D. Md. May 27, 2016).

We anticipate that these cases will continue to be decided on a case-by-case basis in the near term.

Stuart D. Levi is a partner and co-head of **Skadden, Arps, Slate, Meagher & Flom**'s intellectual property and technology group and coordinates the firm's outsourcing and privacy practices. He is based in New York. A version of this expert analysis previously appeared in Skadden Arps' 2016 Insights compendium of attorney-authored articles. Reprinted with permission.