The Biggest Risk with CCPA May Be Cybersecurity, Not Privacy: 10 Things Companies Are Doing Now to Prepare

By Avi Gesser, Matthew Kelly, Will Schildknecht & Clara Y. Kim on July 1, 2019

By now, most major U.S. companies are generally aware of the **new privacy requirements** that will be imposed by the California Consumer Privacy Act ("CCPA") when it goes into effect on January 1, 2020, including data access and deletion rights for consumers as well as restrictions on selling personal information. But, at least in the short term, it is likely that the CCPA's cybersecurity requirements will have the most significant impact on companies.

Unfortunately, the CCPA does not spell out its cybersecurity requirements explicitly. Rather, **it creates a private right of action** for California consumers against companies that have experienced a cyber breach if their personal information has been taken by an unauthorized person. A successful action requires that the exfiltration or disclosure be of unencrypted personal data and result from the company's violation of its duty to implement and maintain reasonable security procedures and practices. § 1798.150(a)(1).

Unlike the class action data breach cases going **up and down the federal court system**, plaintiffs in CCPA cyber breach cases will likely not be required to prove harm, because the law provides for statutory damages at a minimum of $100 and a maximum of $750 per consumer per incident. In many cases, the only viable defense to such an action will be that the company upheld its "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." § 1798.150(a)(1).

But proving that a company had reasonable cybersecurity measures can be difficult and costly. Many companies face very sophisticated cyber attacks, and even firms with state-of-the-art cybersecurity programs can experience breaches that compromise consumers' personal data. And the analysis of whether a company's cybersecurity procedures were reasonable, and therefore whether it has a viable defense, will be done in the context of a breach where a significant amount of consumer data has been compromised. In short, companies will be confronting an uphill battle.

The CCPA does provide another defense to cyber breach class actions, but it is not likely to be of much assistance to companies in most cases. Before bringing action for statutory damages, the consumer is required to provide the company with 30 days' written notice identifying the specific provision that has been violated. If the company cures the noticed violation and provides the consumer with an express written statement stating that the violations have been cured and no further violations will occur, then the consumer can no longer bring action. § 1798.150(b). But a cure may be unavailable in data breaches where, for example, hackers have already taken the consumer's personal data and sold it on the dark web.

All of this means that, in addition to data mapping and other privacy preparations for CCPA compliance, many companies are also taking steps to shore up their cybersecurity to prove that they meet the reasonableness standard needed to defend a data breach class action. Even if not completely successful in avoiding liability, such measures will likely reduce losses because the statute provides that in assessing the appropriate amount of statutory damages, courts should consider, among other factors, "the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth." § 1798.150(a)(2).

Some of the steps companies are taking to shore up their cybersecurity in anticipation of the CCPA include:

1. Encrypting personal information. The section granting consumers the right to private action in the CCPA only applies to "nonencrypted or nonredacted personal information." So, many companies are encrypting the personal information of California residents, both in transit and at rest.
2. Multifactor Authentication. To protect against unauthorized use of employee login credentials, companies are implementing multifactor authentication for remote logins to their networks, and discontinuing access through webmail programs.
3. Access Controls. Companies are granting employees access only to the parts of the network that they need to do their work. They are also limiting the number of individuals within their company who have administrative computer privileges, as well as the length of time that individuals are granted access privileges beyond what they need for their daily work. And when someone leaves or changes roles, companies are ensuring that access privileges are updated immediately.
4. Employee Training. Recognizing that most breaches result from employees' actions, companies are intensifying the sophistication and frequency of their training for employees on topics such as how to spot potential phishing and spoofed emails.
5. Vendor Management. Companies are limiting the number of vendors who have access to their sensitive information and are conducting audits of those vendors' cybersecurity measures. They are also requiring those vendors to notify them quickly and cooperate in the event of a breach.
6. Patch management and software updates. Companies are also devoting additional resources to keeping track of security alerts and software updates, to make sure their computer systems have the latest protection.
7. Penetration testing and vulnerability assessments. Companies are increasingly utilizing outside experts to assess and improve their cybersecurity through penetration testing, vulnerability assessments, and **bug bounty programs**.
8. Network monitoring. Companies are also investing in **continuous monitoring of their networks**, including for unauthorized activity by employees, such as the mailing of large amounts of sensitive company materials to personal email accounts.
9. Cyber policies for incident response and data management. Many regulatory regimes, such as the New York DFS Cybersecurity Regulation, require companies to have policies on incident response and data management. To shore up their cybersecurity measures, many companies are updating and testing these policies through **tabletop exercises**.
10. Arbitration Clauses. Finally, in an effort to reduce CCPA class action risk, some companies are including arbitration clauses and class action waivers in the terms and conditions pages of their websites. Although the CCPA prohibits such waivers, § 1798.192, federal law under the Federal Arbitration Act, which requires arbitration agreements be treated with the same weight as all other contracts, likely preempts this section of the CCPA. The Supreme Court has held, for instance, that a Kentucky court's ruling that singled out an arbitration agreement for disfavored treatment violated the FAA. **Kindred Nursing Centers Ltd. P'ship v. Clark**, 137 S. Ct. 1421 (2017). This suggests that the CCPA's attempt to cabin arbitration clauses and waivers will be unsuccessful.

One more general hedge against these risks is cyber insurance. In preparation for CCPA and other cybersecurity regulatory developments, companies are increasing their cyber insurance coverage and making sure that they know what their policies will and will not cover.

Of course, each company must implement cybersecurity measures that are appropriate for its own risks, and what is reasonable will depend on factors like the size of the company, the kind of data it has, and the threats it faces. The **Davis Polk Cyber Portal** is available for clients to meet their evolving cybersecurity and privacy obligations. We will continue to monitor updates on the CCPA closely here at the Davis Polk Cyber Blog.

This article has also been posted at the Compliance & Enforcement **blog** sponsored by **NYU Law's Program on Corporate Compliance and Enforcement**.