Debevoise
& Plimpton

Debevoise Update D&P

# Seven Tips for Reducing CCPA Litigation Risks – Lessons from the First 18 Months

**June 22, 2021**

Since the implementation of the California Consumer Privacy Act ("CCPA") 18 months ago, more than 75 lawsuits have been filed seeking damages using the Act's private cause of action. The CCPA provides a cause of action to "[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures." Consumers can seek damages for any harm actually incurred as well as statutory damages ranging from $100 to $750 per consumer per incident.

Not surprisingly, in these early days of CCPA private actions, plaintiffs are trying to push the boundaries of the law and testing who, when, and why a CCPA claim may be brought. In this Debevoise Data Blog post, we offer practical tips for reducing CCPA risk based on a review of the cases filed to date and the treatment of those cases in the courts.

**1. Protect or Delete the Sensitive Personal Information That Triggers Civil Liability**: Not all personal information triggers liability under the CCPA. In *Rahman v. Marriott Int'l, Inc., et al.*, Marriott successfully dismissed a proposed class action on the basis that the breach did not contain "sensitive" data such as social security numbers or credit card information. The court held that loyalty numbers and other personal information not covered by California's data breach notification statute were an insufficient basis to bring a private right of action under CCPA.

Accordingly, companies should take extra care to avoid their employees having large amounts of unencrypted credit card numbers, social security numbers, passports, driver's licenses, and other sensitive personal information that would trigger liability under the CCPA or state data breach notification laws in their emails. In addition, efforts should be made to only collect sensitive personal information that is necessary, and to the extent that such data is no longer needed for a legitimate business purpose or legal reason, it should be deleted as part of a sensible data minimization program. Where companies have a business reason to collect and use sensitive personal information, they should consider taking reasonable steps to encrypt or redact this information both a rest and prior to sending by email.

**2. Properly Configure Websites and Cloud Services**: The CCPA provides a private right action where nonencrypted and nonredacted personal information is subject to "unauthorized access and exfiltration, theft, or disclosure." Although some would argue the private right of action is intended to apply when a company has had its systems breached, Plaintiffs have seized on the term "disclosure" and successfully argued against dismissal in at least two cases that the right of action includes not only data breaches of corporate networks, but also unauthorized access to personal information or individual user accounts.

In *Stasi v. Inmediata Health Group Corp.*, personal and medical information associated with over 1.5 million individuals was inadvertently made publicly available on the Internet due to a misconfiguration within Inmediata's webpage. Inmediata sought to dismiss the CCPA class action because Plaintiffs had not specifically alleged that unauthorized actors actually accessed the data. The District Court rejected Inmediata's argument, finding that the complaint did allege that the data was viewed by unauthorized persons and that, in any event, there was no requirement that plaintiffs must "plead theft or unauthorized access in order to plead a plausible violation of the CCPA" – mere disclosure on the Internet was sufficient. The parties in this matter appear to have entered into settlement negotiations.

Misconfigurations on websites or cloud services that expose information intended to be internal are not uncommon. Companies should review and test their website and application code, as well as cloud configurations, to defend against misconfigurations potentially resulting in inadvertent data exposure.

**3. Adopt Measures against Credential Stuffing and Account Takeovers**: In a separate action, Plaintiffs alleged that the Defendant company maintained inadequate security practices after attackers, potentially through the use of information in other data breaches, accessed approximately 2,000 customer accounts without authorization. The District Court largely denied the Defendant's motion to dismiss finding that there were sufficient allegations that inadequate security procedures allowed an authorized party to "view, use, manipulate, exfiltrate, and steal the nonencrypted or nonredacted personal information of Plaintiffs" even though there was no showing that the Defendant's internal network experienced a data breach. The Defendant has filed a second motion to dismiss following the Plaintiff's filing of a second amended complaint.

Because plaintiffs and regulators are increasingly focused on customer account attacks, such as account takeovers and credentials stuffing, companies should consider preventative controls to reduce such risks, such as a trusted device program, dark web monitoring, multifactor authentication or CAPTCHA for certain actions, secure password recovery, and suspicious behavior detection.

**4. Ensure Compliance with CCPA's Privacy Provisions**: In *McCoy v. Alphabet*, the Plaintiff alleged that Alphabet used an internal program to monitor and collect sensitive personal data associated with users from non-Google applications while using an Android smartphone. Pointing to Alphabet's Privacy Policy, Plaintiff claimed that Alphabet and Google did not adequately disclose or seek user consent to "monitor, collect, or use Android smartphone user's sensitive personal data" and used this data to gain a competitive advantage. The District Court handily dismissed the CCPA claim in this case because Plaintiff conceded dismissal of this count at the hearing because there was no allegation of a data breach.

But Plaintiffs continue to test whether the courts will expand the CCPA private right of action to privacy violations by including CCPA counts in class-action privacy complaints. In *L.P. v. Shutterfly, Inc.*, the Plaintiff alleged that Shutterfly extracted and stored biometric identifiers from user-uploaded photographs of children without proper notice under the CCPA, alleging that "the sale of personal information of minors equates to that of a data breach" because it was an unauthorized disclosure. Named plaintiffs dismissed the case with prejudice following mediation. Similarly, in *Sweeney v. Life on Air & Epic Games*, the Plaintiff alleged that the failure to notify users that their personal data was shared with third parties and the failure to provide notice of users' right to opt-out, constituted a violation of the CCPA. Epic Games moved to compel arbitration based on its terms of service, which the court granted.

Companies that have delayed their compliance with the privacy provisions of the CCPA should take note that they may be vulnerable to not only enforcement by the California Attorney General but also by private attorneys general as long as the case law is not fully settled on these issues.

**5. Be Sure Your Privacy Policy Doesn't Overstate Your Data Security Measures**: Plaintiffs often point to data security promises made in a Company's privacy policy and terms of use in data breach cases to assert unfair and deceptive practices claims or breach of contract claims. In *Vennerholm v. GEICO*, in which Defendants have yet to file a responsive pleading, Plaintiffs allege that they relied on the assurances in GEICO's Privacy Policy and Internet Security Policy that stated, among other things, that GEICO used "[p]hysical safeguards, procedural controls and data access controls protect your data from unauthorized access. We continually monitor our systems to prevent unauthorized attempts at intrusion." Similarly, in *Mehta v. Robinhood Financial LLC*, plaintiffs pointed to Robinhood's website which stated that it was "[d]edicated to maintaining the highest security standards" which the District Court found was non-actionable puffery under California's unfair acts and deceptive practices statute.

Companies should therefore consider periodically reviewing their cybersecurity representations and make sure that they align with current practices.

**6. Maintain a Robust Vendor Management Program**: The expansive reading of "disclosure" under the CCPA in *Stasi* and *Robinhood* suggests that courts might be willing to extend that broad reading of the CCPA to hold companies liable when third-party vendors experience security incidents. At least one lawsuit seeks to do this. In *Doe v. Health Net of California*, Plaintiffs allege that Health Net failed to implement reasonable cybersecurity practices to protect customer PII/PHI stored in a third-party file share that was then exposed when external actors exploited a vulnerability in that third party's systems. Companies should therefore consider identifying third parties with access to the company's sensitive personal data and implement software patches and updates on a regular cadence as well as to ensure that these third parties are maintaining reasonable cybersecurity practices. As of this writing, Defendants have yet to file a responsive pleading.

**7. Implement the Hallmarks of Reasonable Cybersecurity**: To recover in a CCPA civil suit, plaintiffs must show that the company in question failed to "maintain reasonable security procedures and practices appropriate to the nature of the information[.]" Some of the cybersecurity measures imposed on companies in settlements of CCPA civil actions provide useful examples of reasonable cybersecurity measures that can be implemented in advance of any breach to reduce the risk of CCPA civil liability.

- **Conduct Cybersecurity Risk Assessments and Penetration Tests**: As part of the CCPA civil settlement in *Barnes v. Hanna Andersson*, the company agreed to conduct a risk assessment consistent with the National Institute of Standards and Technology's Cybersecurity Framework. Similarly, the parties in *Atkinson v. Minted, Inc*. agreed that Minted would undergo a System and Organization Control 2, or SOC 2, audit, which emphasizes internal risk management and governance. These settlements also require the companies to conduct penetration tests and vulnerability scans, and ensure that processes are in place to promptly patch or remediate servers and workstations when vulnerabilities are identified. Conducting this kind of testing and promptly addressing the highest-risk vulnerabilities that are found could be helpful in showing that a company's cybersecurity measures were, in fact, reasonable in the event of a breach that leads to CCPA litigation.

- **Implement Threat Detection and Monitoring Tools**: In *Hanna Andersson*, the unauthorized access to the network occurred in September, but Hanna Andersson did not identify the unauthorized access until November. The Plaintiffs alleged that the company failed to adequately monitor the platform and provide notice of these practices to customers. Consequently, as part of the settlement, Hanna Andersson has agreed to implement additional intrusion and detection tools, malware detection, antivirus, and monitoring tools within its environment. These tools can significantly reduce the time between the incident occurring and detection, which can reduce the harm to the company and its customers. Companies should therefore consider evaluating their detection controls periodically, including those to identify malware, unauthorized access, and exfiltration, to ensure that they have the appropriate visibility within their network and can promptly respond to potential security events;

- **Have Dedicated Cybersecurity Personnel**: In *Hanna Andersson*, the company agreed to hire a Director of Cyber Security and additional technical staff. Depending on the size of the organization, having individuals who are exclusively focused on cybersecurity can be an important indicator of the companies' efforts to protect customers' information;

- **Conduct Cybersecurity Training**: Many significant cyber breaches begin with a successful phishing attack against an employee. Both the Hanna Andersson and Minted, Inc. settlements require the companies to build out their training programs, including increased phishing exercises for employees and secure coding training for developers.

To subscribe to the Data Blog, please click here.

**NEW YORK**

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

Alexandra P. Swain
apswain@debevoise.com

**SAN FRANCISCO**

H Jacqueline Brehmer
hjbrehmer@debevoise.com

Christopher S. Ford
csford@debevoise.com