The Coming Wave Of Privacy Actions In The Wake Of COVID-19: Six Things To Know

As the world moves online during the COVID-19 pandemic, companies' privacy and security practices are coming under increased scrutiny. Because class actions often follow such scrutiny, as demonstrated by lawsuits recently filed against Google and Zoom, companies should keep the following six developments on their radar as they rush to meet the demands of our new virtual reality.

1

Multiple putative class action lawsuits have been filed against online companies in the wake of COVID-19.

Multiple putative class action lawsuits have recently been filed against online companies following intensified scrutiny of data privacy and security practices. For example, a series of lawsuits bringing claims under various California laws as well as federal securities laws against Zoom challenge the company's data-sharing practices, advertising regarding end-to-end encryption, and so-called "Zoombombing" where unauthorized attendees enter a meeting.[1] Google has also been hit with a putative class action lawsuit in the Northern District of California alleging that it collects biometric information in connection with its educational software in violation of Illinois's Biometric Information Privacy Act and the federal Children's Online Privacy Protection Act.[2]

2

The scope of the new California Consumer Privacy Act will be tested in court.

The recent Zoom class actions are also among the first to assert claims under the California Consumer Privacy Act (CCPA) — a new law, effective January 1, 2020, that governs companies' handling of personal information of California residents. These cases may help clarify the contours of this untested law.

Notably, the CCPA expressly authorizes a private right of action, including statutory damages, only in the narrow case of data breaches affecting specific types of unredacted or unencrypted personal information and where the breach resulted from the business's failure to maintain reasonable security procedures. *See* Cal. Civ. Code §

[1] *See Drieu v. Zoom Video Communications, Inc.*, Case No. 20-cv-02353 (N.D. Cal. Apr. 7, 2020); *Ohlweiler v. Zoom Video Communications, Inc.*, Case No. 20-cv-03165 (C.D. Cal. Apr. 3, 2020); *Taylor v. Zoom Video Communications Inc.,* Case No. 20-cv-02170 (N.D. Cal. Mar. 31, 2020); *Cullen v. Zoom Video Communications Inc.*, Case No. 20-cv-02155 (N.D. Cal. Mar. 30, 2020).
[2] *See H.K. and J.C. v. Google LLC*, Case No. 20-cv-02257 (N.D. Cal. Apr. 2, 2020).

1798.150(a). The Zoom class actions, however, do not allege any data breach. And the types of personal information covered by the CCPA's private right of action are limited, including (for example) a user's social security number, credit card number, and medical data — information that does not appear to be at issue in these class actions. Zoom may thus be expected to seek dismissal on these grounds.

How (and how quickly) courts respond to the CCPA claims will instruct future plaintiffs' attempts to push the CCPA's boundaries.

3

Regulators also are paying close attention.

Multiple attorneys general have raised concerns over data privacy and cybersecurity risks in the wake of this pandemic. For example, the New York Attorney General sent a March 30 letter to Zoom broadly inquiring about its security practices. Senators have also begun calling for investigation into Zoom's practices. The FBI has warned of Zoombombings. The California Attorney General, who is authorized to enforce the CCPA starting July 1, 2020, has rejected industry appeals to delay the enforcement deadline in light of COVID-19. With widespread online presence as well as public awareness of privacy and security risks becoming the new norm, companies should not expect to see regulators hold back on bringing privacy and cybersecurity regulatory investigations involving online platforms.

4

COVID-19 may eventually prompt greater government oversight over the technology sector.

Technology companies face mounting pressure for greater transparency with respect to the steps they are taking to protect users' privacy and online security. The now-universal reliance on technology to remain connected during this pandemic may bring consumer privacy protection into even sharper focus. This may eventually invite greater government oversight, including future initiatives by other states to enact laws like — or even broader than — the CCPA, as well as calls for a federal privacy law.

5

Technology companies should be aware of existing regulations as they expand into regulated industries.

As companies in regulated industries — such as education, financial services, and healthcare — rush to transition a broader swath of their operations online, technology companies should consider the additional privacy protections afforded within these highly-regulated industries. Companies will need to assess, for example, whether the data that is transmitted online include the type of information that is governed by the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), or the Gramm-Leach-Bliley Act (GLBA).

6

Protect yourself.

Businesses and individuals can help mitigate the heightened privacy and security risks brought on by COVID-19. Businesses should vet their online service provider's privacy and security policies before requiring or recommending that employees use the service. And they should encourage their employees to utilize existing privacy and security settings, such as meeting passwords, waiting rooms, and similar controls, to protect their meetings and data. For more practical guidance on steps businesses can take to manage cybersecurity risks from a legal compliance standpoint, please see our Cybersecurity Compliance Considerations for COVID-19.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Class Action and Privacy practices:

Eric Bosset	+1 202 662 5606	ebosset@cov.com
Ashley Simonsen	+1 424 332 4782	asimonsen@cov.com
Simon Frankel	+1 415 591 7052	sfrankel@cov.com
Kate Cahoy	+1 650 632 4735	kcahoy@cov.com
Lindsey Tonsager	+1 415 591 7061	ltonsager@cov.com
William Stern	+1 415 591 7069	wstern@cov.com
Libbie Canter	+1 202 662 5228	ecanter@cov.com
Sarah Kwon	+1 415 591 6014	skwon@cov.com