NOW + NEXT

PRIVACY AND CLASS ACTION ALERT | NIXON PEABODY LLP

APRIL 6, 2020

Recent privacy class actions against Zoom raise questions about work-from-home technologies as well as CCPA applicability

By Troy K. Lieberman and Marx P. Calderon

Across the country, millions of people are confined to their homes due to the coronavirus pandemic. In the new work-from-home environment, novel and challenging privacy concerns are coming to the forefront. With the use of video conferences exploding, recent class action lawsuits filed against Zoom (one of the most popular video conferencing services) in California federal court for alleged privacy violations highlight these issues. Companies should properly assess services' data privacy and security measures before requiring employees to use such services. Employers could potentially be held liable for a communication services' mishandling of users' personal information.

Zoom class actions

The class actions allege that Zoom failed to properly safeguard the personal information of users of its software application and video conferencing platform. Among other things, the suits allege that Zoom collected and disclosed, without adequate notice or authorization, personal information of its users to third parties, including Facebook.

Zoom allegedly disclosed personal information including the model of a user's device, the time zone and city where a user is connecting from, the phone carrier being used, and a unique identifier for targeted advertisements. The collection and disclosure of this information purportedly was not addressed in Zoom's privacy policy. The class action complaints allege that millions of users were harmed by these failures, as well as Zoom's failure to implement and maintain reasonable security protections and protocols. These purported failures are cited in support of the complaints' causes of action under the California Consumer Privacy Act (CCPA), California Unfair Competition Law, Consumers Legal Remedies Act, negligence, invasion of privacy, and unjust enrichment.

The California Consumer Privacy Act claim

The claims under the CCPA raise novel threshold questions, particularly given that the statute only went into effect on January 1, 2020. As is well known, the CCPA provides California residents with significant privacy rights, including access to their personal information retained or shared by a business, as well as notices from certain businesses regarding their collection, use, and disclosure of

This newsletter is intended as an information source for the clients and friends of Nixon Peabody LLP. The content should not be construed as legal advice, and readers should not act upon information in the publication without professional counsel. This material may be considered advertising under certain rules of professional conduct. Copyright © 2020 Nixon Peabody LLP. All rights reserved.

personal information. Thus far, it has been generally understood that a business's violation of these provisions is only enforceable by the California Attorney General (and such enforcement will not begin until July 1, 2020). The CCPA's very limited private right of action provides California residents recourse when their "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." Cal. Civ. Code § 1798.150(a). It is generally understood, in other words, that this limited private right of action only applies when there has been a data breach (i.e., unauthorized access) which compromises user data.

However, the complaints against Zoom do not allege a data breach; rather they attempt to interpret the CCPA's private right of action (likely in an effort to recover the CCPA's statutory damages) to apply to the "unauthorized disclosure" of personal information (i.e., sharing personal information with a known business partner)—rather than the CCPA's requirement of "unauthorized access *and* . . . disclosure."

Additionally, the CCPA's private right of action provisions do not include the CCPA's otherwise broad definition of "personal information." Instead, those provisions apply only when sensitive personal information—defined under the state's breach notification law (e.g., social security number, payment card information, health information)—is accessed and disclosed. The complaints against Zoom do not focus on this type of sensitive information.

Therefore, Zoom likely has many arguments supporting dismissal of the CCPA claim early in the litigation. The court's handling of these threshold CCPA questions will be interesting and instructive for future CCPA plaintiffs and defendants.

The remaining claims

The complaints against Zoom also assert additional claims, including unfair business practices and negligence, apparently based on the alleged underlying failure to comply with the CCPA. However, the CCPA appears on its face to preclude individuals from using it as a basis for other causes of action: "Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." Cal. Civ. Code § 1798.150(c). The plaintiffs appear to be testing this language, and the court's interpretation of this CCPA provision will similarly prove instructive in future CCPA litigation.

Potential employer liability? What this means for your business:

While not yet an issue in the current Zoom litigation, an obvious question for employers is whether they can, or should, mandate that at-home employees use certain technologies as part of their day-to-day business operations. It does not seem far-fetched to envision a scenario where an employee sues an employer, claiming he or she has been harmed by substandard privacy and security practices of third-party services that the employer required the employee to use.

Plaintiffs firms may be working from home—but they're still working! It is important for businesses to remain vigilant and aware of potential concerns surrounding their new remote workforce. In light of the novel challenges business face with employees working from home, here are some things employers can do to limit their liability and protect their employees:

- Do not require or recommend employees use a communication service that has not been adequately vetted by the employer or its attorneys. If, for example, a service's privacy policy does not appear on its face to comply with notice and transparency requirements (or if an

employer has reason to know affirmative statements in a privacy policy are false), an employer may be liable under negligence or other theories;

- Carefully scrutinize privacy and security measures before recommending any "free" version of a communication service or technology for employees' remote work. Business- or professional-versions, while coming with a cost, often come with additional protections and, at a minimum, are subject to bilateral contract negotiation where representations and warranties likely can be secured;
- Review and follow best practices for using communication services and other technologies to minimize privacy and security concerns. For a list of best practices and other advice, please see our alert, "How to protect your remote workforce from cyberattacks: Tips to consider as working from home becomes the norm."

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Troy Lieberman, 617-345-1281, tlieberman@nixonpeabody.com
- Marx P. Calderon, 617-345-1205, mcalderon@nixonpeabody.com
- Jason Gonzalez, 213-629-6019, jgonzalez@nixonpeabody.com
- Staci Jennifer Riordan, 213-629-6041, sriordan@nixonpeabody.com