EmTech Perspectives

Babst | Calland
Attorneys at Law

Ashleigh H. Krick

FTC Issues Settlement Requiring Zoom to Implement Robust Information Security Program in Response to Years of Deceptive Security Practices

On November 9, 2020, the Federal Trade Commission (FTC) announced a settlement agreement with Zoom Video Communications, Inc. (Zoom) that arose from alleged violations that Zoom engaged in a series of deceptive and unfair practices that undermined user security.

The FTC found that Zoom made several representations across its platform regarding the strength of its privacy and security measures used to protect users' personal information that were untrue and provided users with a false sense of security. Specifically, the FTC found that Zoom made multiple statements regarding "end-to-end" and "AES 256-bit" encryption used to secure videoconference communications. However, Zoom did not provide end-to-end encryption for any Zoom meeting conducted outside of Zoom's "Connecter" product. And, Zoom used a lower level of encryption that did not provide for the same level of security as "AES 256-bit" encryption. The FTC also found that Zoom stored meeting recordings unencrypted and for a longer period than Zoom claimed in its Security Guide. And, Zoom circumvented browser privacy and security safeguards through software updates without notice to users and without establishing replacement safeguards.

> ... Zoom **made several representations across its platform** regarding the strength of its privacy and security measures used to protect users' personal information that were untrue and **provided users with a false sense of security.**

As a result of these alleged privacy and security violations, Zoom has agreed to establish a comprehensive information security program that meets enumerated criteria, including annual reviews of security risks and corresponding safeguards, implementing a vulnerability management program, and deploying safeguards such as multi-factor authentication. Zoom must also obtain an initial and biennial security assessments by a third party for the next 20 years. Zoom is also required to report security breaches to the FTC. As should go without saying, Zoom is prohibited from making misrepresentations about its privacy and security practices. Notably, the settlement agreement did not require Zoom to pay a penalty or provide compensation to affected users; however, there are multiple outstanding lawsuits that may result in compensation to affected users.

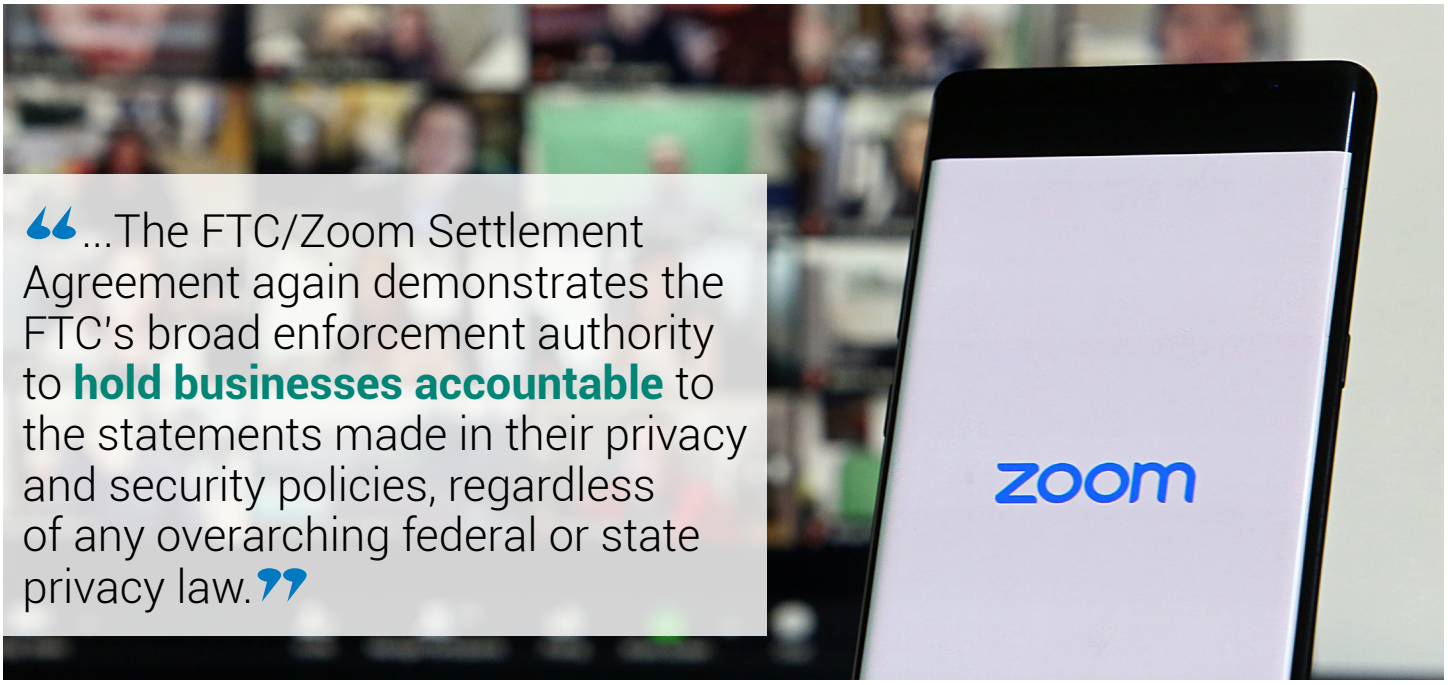
The FTC/Zoom Settlement Agreement again demonstrates the FTC's broad enforcement authority to hold businesses accountable to the statements made in their privacy and security policies, regardless of any overarching federal or state privacy law. As I previously wrote about in the article "FTC Investigation of Twitter for Alleged Privacy Violations Reinforces Need for Strong Privacy Policies and Practices," businesses today, regardless of whether they may be subject to the EU's General Data Protection Regulation or California's Consumer Privacy Act, must be proactive in understanding of how their current privacy and security policies align with their actual practices.

And, businesses should also consider how a change in Administration may affect FTC enforcement and prospects of a federal privacy law. Both Republicans and Democrats have been interested in privacy legislation and we will likely continue to see interest and movement under a Biden administration. And, a Democratic-led FTC could lead to increased enforcement and heightened interest in individual privacy and net neutrality.

When we work with businesses to review their privacy and security practices, we often start with a privacy impact assessment that reviews questions such as:

- What personal information is the business collecting? What is the purpose of that information collection? How is such information being used? Are there retention limitations for this information?
- Has the business conducted a privacy and security risk assessment? What was the outcome of that assessment? How has the business implemented appropriate security measures to address identified risks?
- Has the business identified an individual charged with updating, enforcing, and ensuring compliance with the company's privacy and security policies? Has the business conducted employee training regarding privacy and cybersecurity?

These questions, among others, can help a business determine whether their privacy and security practices align with the statements and guarantees they are making to their customers and service partners.



> ...The FTC/Zoom Settlement Agreement again demonstrates the FTC's broad enforcement authority to **hold businesses accountable** to the statements made in their privacy and security policies, regardless of any overarching federal or state privacy law.

Babst Calland's Emerging Technologies Group has recently created EmTech Law Blog which contains news, articles and legal and regulatory information published by our attorneys in an effort to provide timely legal and business information on issues impacting companies developing or investing in new technologies, new companies, and new ideas.

To subscribe, simply register at EmTech Law Blog and add your e-mail address. Whenever we post information, you'll be notified. We hope that you find our blog posts to be informative and will share them with a colleague or a friend. We look forward to hearing your feedback.

Babst | Calland
Attorneys at Law

Where Trust and Value Meet™

PITTSBURGH, PA I CHARLESTON, WV I HOUSTON, TX I SEWELL, NJ I STATE COLLEGE, PA I WASHINGTON, DC