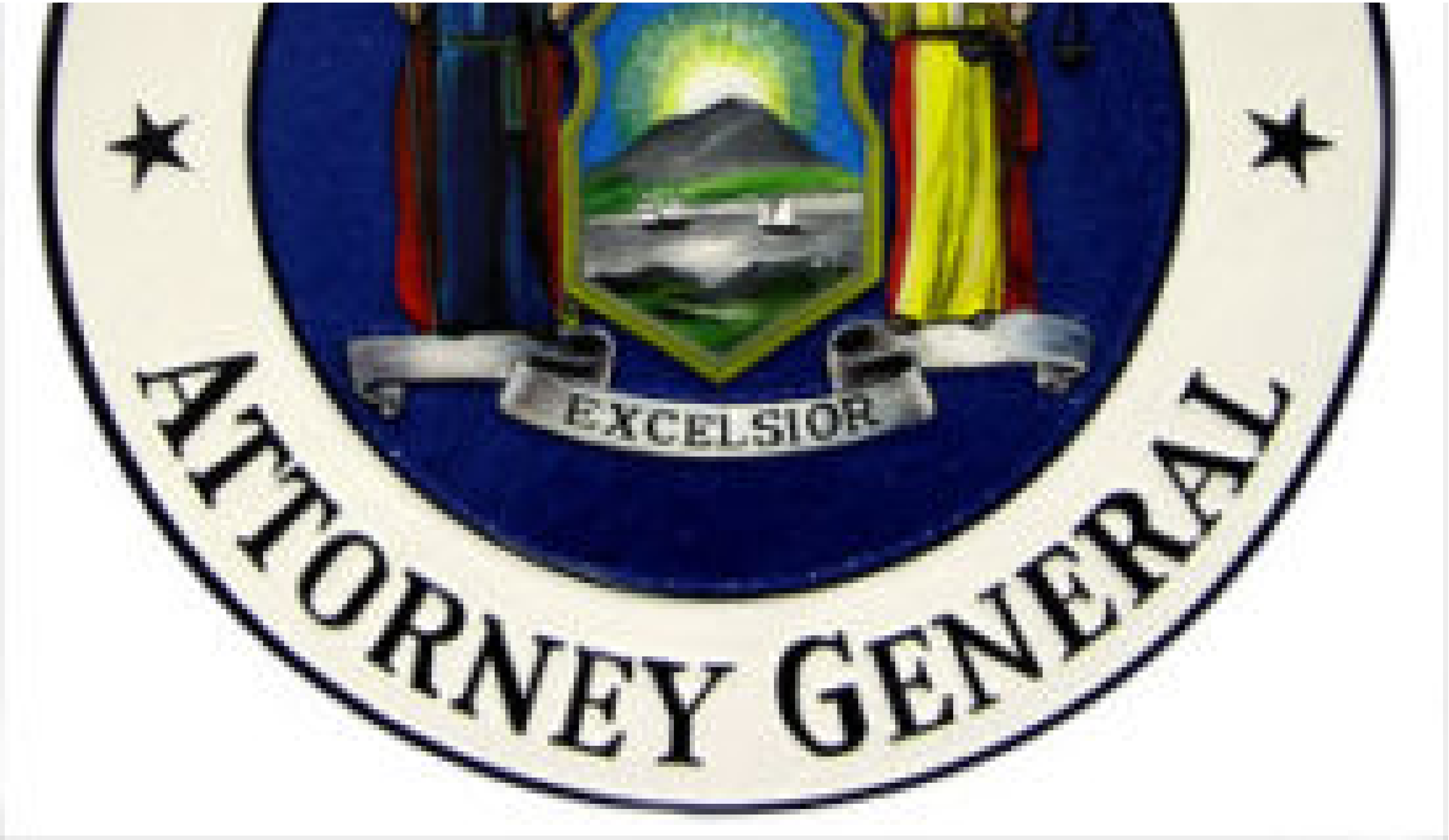
Frankfurt Kurnit Klein+Selz PC

Focus on the Data

Unique Insights and Practical Guidance on Privacy and Data Security Issues Worldwide

# Zoom Reaches Agreement with New York Attorney General to Resolve Privacy and Security Issues

By Elliott Siebers on May 13, 2020



Previously, my colleague Tanya Forsheit wrote a cautionary tale, "**A Big Zooming Mess**," about the Zoom video conferencing service whose rise in popularity also brought increased scrutiny of its privacy and data security practices. That scrutiny came not just from media outlets and consumers, but also from government agencies such as the New York Attorney General and New York City Department of Education. The entire FKKS Privacy and Data Security team even had a round-table discussion (over WebEx) to unpack all the issues (recording available **here**). Now, both the New York Attorney General and the New York City Department of Education announced that they reached coordinated but independent agreements with Zoom to address various privacy and security issues, and paving the way for NYC DOE educators to resume using Zoom for virtual classroom instruction. This post looks at the terms of the NY AG agreement and discusses some of its key takeaways.

With the caveat that Zoom is neither admitting nor denying any of the allegations, many of the issues that caused the NY AG to open an investigation appear to have been addressed, including Zoom's disclosures regarding the Facebook SDK, its representations regarding encryption, and issues arising from "Zoombombing" and children's use of the platform. The AG declined to commence a "statutory proceeding," recognizing the unusual circumstances of the pandemic as well as the role that Zoom's services have played in connecting people despite social distancing measures. The form of the agreement, a letter, as well as the absence of any civil penalty, suggests that the interest of the Attorney General here was to address quickly any privacy or security issues. That being said, Zoom isn't entirely out of the woods, as the agreement is voidable in the sole discretion of the NY AG if it comes to light that Zoom made any inaccurate or misleading statements in the course of the inquiry.

So what is Zoom actually agreeing to do? In substance, the agreement has Zoom committing to: general compliance obligations, a comprehensive information security program, additional security measures, privacy and privacy controls, protection of users from abuse, and audit and testing. The general compliance obligations require Zoom to comply with New York General Business Law §§ 349 and 350, the Children's Online Privacy Protection Act (COPPA), and New York Education laws and regulations.
As a part of the security measures, Zoom has essentially agreed to the requirements of the SHIELD Act amendments to New York's General Business Law §899-bb, which became effective in late March. Accordingly, Zoom will continue to designate a "head of information security," who will be responsible for overseeing the implementation of a comprehensive information security program and report to the CEO and Board of Directors periodically. The information security program will require organizational changes, including a security team that reports to the head of information security, a risk assessment identifying "material internal and external risks to the security, confidentiality, and integrity of personal information," and controls designed to mitigate those risks.

Beyond those obligations that Zoom might otherwise incur under the SHIELD Act, the company has also agreed to encrypt personal information it stores in the cloud, as well as data transmitted over the Zoom app. Recall that Zoom publicly admitted that, despite representations that it used end-to-end encryption, its actual method of encryption was not what most people would consider end-to-end. Despite the apparent misrepresentation, the encryption obligations of the agreement don't explicitly commit Zoom to implementing end-to-end encryption. However, Zoom is committing to updating and upgrading its security and encryption as industry standards evolve, so its encryption practices may (have to) change over time. Zoom has also agreed to produce a SOC 2 report to the NY AG, and to continue to conduct pen tests of its systems, including "at least one annual white box penetration test."

As to the Privacy and Privacy Controls provisions, much of the agreement seems aimed at addressing how Zoom is used among educational institutions, with Zoom committing to provide educational materials for consumers, K-12 students, and universities or other institutions, instructing those users how to enable Zoom's privacy-enabling features. Zoom is obligated to maintain or implement some of the controls, including default password-protected meetings, limiting meetings to users with a specific email domain, and allowing hosts to limit participants. These controls are geared toward preventing Zoombombing incidents and therefore specifically tailored to Zoom.

Zoom voluntarily disabled the Facebook SDK prior to the agreement, and the agreement doesn't specifically address the SDK going forward (beyond the general obligation that Zoom not misrepresent its practices).

Though Zoom's lack of a bug bounty program did not appear to be an issue leading up to the investigation, this agreement requires Zoom to implement one in order to facilitate "external monitoring" of the Zoom platform. To that end, Zoom has also agreed to create a portal for users, consumer advocates, and watchdog groups to submit complaints involving privacy and data security and to review any complaints "within a reasonable time after receipt." It's common for technology companies to implement bug bounty programs, but no U.S. law actually requires it.

Several other attorneys general announced investigations into Zoom and the company may yet face further consequences. We will continue to monitor those developments.

Focus on the Data

Klein+Selz

Copyright © 2021, Frankfurt Kurnit Klein & Selz PC. All Rights Reserved.