



STATE OF NEW YORK  
OFFICE OF THE ATTORNEY GENERAL

LETITIA JAMES  
ATTORNEY GENERAL

DIVISION OF ECONOMIC JUSTICE  
BUREAU OF INTERNET  
AND TECHNOLOGY

May 7, 2020

**VIA EMAIL**

Travis LeBlanc  
Cooley LLP  
1299 Pennsylvania Avenue, NW Suite 700  
Washington, DC 20004-2400

Re: Letter Agreement between Zoom and the NYAG

Dear Travis:

This letter confirms the understanding between Zoom Video Communications, Inc. (“Zoom”) and the New York State Attorney General’s office (“NYAG”) regarding Zoom’s privacy and data security practices, as well as its acceptable use policy.

**Background**

Zoom offers software-based communication services, allowing users to participate in video conferences on desktop computers, laptops and mobile devices. Zoom is a Delaware corporation, with its principal place of business at 55 Almaden Boulevard, San Jose, California.

Zoom provides its services through a client-side software application (“Zoom’s app” or “the Zoom app”) that is downloaded and installed onto a user’s computer, or mobile device. The app connects to Zoom’s servers and then to the Zoom app on other users’ devices. By creating a Zoom account, a user can create and host a videoconference and invite others to attend by providing them with a hyperlink or conference identifier.

Founded in 2011, Zoom has traditionally marketed and sold its software and services to businesses and other enterprise clients, who typically have dedicated information technology staff to help users within their organizations use Zoom’s software and services.

Beginning in late 2019, a novel coronavirus, designated COVID-19, emerged and began to spread across the globe. Within a matter of months, the virus became a global pandemic, and by March 2020, governments in New York and across the United States, began instituting social

distancing policies to limit contagion. These policies required, among other things, limits on travel and socializing in person and the closure of primary and secondary schools. As a result, Zoom experienced a massive surge in demand for its services, as consumers began using it to socialize remotely with friends, families, and colleagues, and as teachers began using the platform to conduct classes remotely with students. In response, Zoom offered its services for free (or at vastly reduced costs) to schools and others.

By March 2020, Zoom was hosting approximately 200 million daily meeting participants on its platform, compared to the approximately 10 million daily meeting participants in January 2020, an increase of 2,000% in three months.

As Zoom's platform was increasingly used by consumers and students to voluntarily communicate and share personal information, a number of media reports raised concerns relating to use of the platform.

For example, a number of people reported that their Zoom conferences had been interrupted by uninvited participants seeking to disrupt the conference. Dubbed "Zoombombing," some of these disruptions evidenced an intent to harass participants on the basis of their race, gender, religion, or their membership in another historically marginalized class.

There were a number of privacy and data security concerns reported in the media, as well. For example, there were reports that Zoom failed to use AES 256 bit encryption and end-to-end encryption as it had publicly represented. Additionally, some media outlets picked up a report that Zoom had been inadvertently issuing encryption keys either by or through data centers in China for some calls taking place purely between individuals in the United States.

Zoom used Facebook's SDK for iOS to enable users to login via Facebook on Zoom's iOS mobile app. Zoom was unaware that Facebook collected technical device information<sup>1</sup> related to its users' phones when they opened the Zoom iOS mobile app. However, Zoom informed users in its privacy policy that it may use third-party tools that collect information. Facebook's collection included users who were not using the Facebook Login feature and users without a Facebook account.<sup>2</sup> Zoom felt that Facebook's collection was "unnecessary for [Zoom] to provide [the] services,"<sup>3</sup> so Zoom removed the Facebook SDK two days after learning about the issue.

Similarly, Zoom users who subscribed to the LinkedIn Sales Navigator feature were able to view links to the publicly available LinkedIn profiles of other meeting participants.<sup>4</sup> This functionality worked even for users attempting to stay anonymous by adopting pseudonyms, disclosing their real names despite Zoom's guidance indicating that users could control how their

---

<sup>1</sup> Data sent included the device's mobile OS type and version, time zone, model and carrier, screen size, processor cores, and disk space. <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/>

<sup>2</sup> [https://www.vice.com/en\\_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account](https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account)

<sup>3</sup> <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/>

<sup>4</sup> <https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html>

name appeared.<sup>5</sup> Zoom has publicly acknowledged “unnecessary data disclosure by the [LinkedIn] feature.”

Finally, Zoom’s “Company Directory” feature leaked personal information of some users to other users where multiple users signed up for Zoom using the same uncommon email domain.<sup>6</sup> Zoom has acknowledged that it was aware of this issue before it was reported, but had only taken steps to prevent disclosure after an affected user sent a complaint concerning a given email domain.<sup>7</sup>

### **Zoom’s Cooperation with the Investigation**

Since the outset of the NYAG’s investigation, Zoom has cooperated with the NYAG. Zoom also allowed a large number of New York residents and school children to use its service for free. Once data security and privacy concerns were identified, Zoom responded quickly, including devoting its engineering team to remediating reported vulnerabilities and enhancing the platform’s privacy and security features, particularly to address the newly expanded base of individual users. Zoom changed default settings, created features that allow users new ways to increase the protection of their privacy, and removed features that raised privacy concerns. To assist with a broader review of their policies and procedures, Zoom retained outside consultants. Zoom has also launched a number of educational initiatives to teach users how to protect themselves while using the platform. The recently-launched Zoom 5.0 addresses also many outstanding issues, including moving Zoom's encryption to a 256 bit GCM standard.

### **Agreement**

In recognition of the fact that Zoom has acted to quickly to address the issues identified above, has worked cooperatively with the NYAG’s investigation, and has provided valuable services to schools, local governments and health care institutions to help address the unique circumstances of the global pandemic, the NYAG is willing to accept this letter agreement in lieu of commencing a statutory proceeding as follows:

1. Zoom shall comply with Executive Law § 63(12) and GBL §§ 349 and 350, and shall not misrepresent the collection, maintenance and safeguarding of consumers’ personal information and regulation of abusive activity on its platform.
2. Zoom shall comply with the Children’s Online Privacy Protection Act (“COPPA”) Rule, 16 C.F.R. Part 312.
3. Zoom shall comply with New York Education Law § 2-d and implementing regulations, 8 N.Y.C.R.R. Part 121, and related regulations.

---

<sup>5</sup> See *id.*; <https://web.archive.org/web/20200401035315/https://support.zoom.us/hc/en-us/articles/201362193-Joining-a-Meeting>

<sup>6</sup> [https://www.vice.com/en\\_us/article/k7e95m/zoom-leaking-email-addresses-photos](https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos)

<sup>7</sup> *Id.*

## Comprehensive Information Security Program

4. Zoom shall continue to designate a Head of Security, who will report to the Chief Executive Officer quarterly and to the Board of Directors semi-annually.

5. Zoom's Head of Security will continue to implement, and maintain a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, confidentiality, and integrity of personal information that Zoom collects, receives, or processes. Such program will be documented in writing, shall be appropriate to Zoom's size, its complexity, the nature and scope of its activities, and the sensitivity of the data at issue, and have the following administrative, technical, and physical safeguards:

a. Designation of an employee or employees to coordinate and be accountable for the information security program, whom shall report directly to the Head of Security;

b. Identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks;

c. Design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

d. Design and implementation of a security code review process to identify and remediate common security vulnerabilities; and

e. Evaluation and adjustment of the information security program described herein in light of the results of the testing or monitoring required by these terms.

### Additional Data Security Practices

6. Zoom shall employ reasonable encryption and security protocols, including by encrypting all personal information at rest in persistent storage on its cloud servers and by encrypting all personal information in transit except where the user fails to utilize a Zoom app or Zoom software for the transmission. Zoom will update and upgrade its security and encryption as industry standards evolve.

7. Zoom shall develop and maintain reasonable procedures to address credential stuffing attacks, including evaluation of whether a login request is being made by a real person or through automation, and through automatic password resets for affected credentials.

8. Zoom shall adhere to industry standards for preserving user security when bypassing operating system security measures.

9. Zoom shall continue to operate a vulnerability management program to address known vulnerabilities, including those set forth above, and have reasonable safeguards to discover and fix new vulnerabilities.

#### Privacy and Privacy Controls

10. Zoom shall continue to offer – or where not currently offered, shall offer – educational materials (e.g., dedicated web page, instructional videos) about privacy controls for:

- a. consumers;
- b. students (as defined in New York Education Law § 2-d) in kindergarten through twelfth grade, administrators, teachers, and parents; and
- c. universities and other institutions.

11. Zoom shall continue to offer – or where not currently offered, shall offer – and maintain reasonable user-facing controls for users who create free accounts and K-12 education accounts that may be used to host meetings including students (as defined in New York Education Law § 2-d) in kindergarten through the twelfth grade, to:

- a. Control access to their video conference by requiring by default a password or waiting room before accessing a meeting;
  - b. Control access to private messages in a Zoom chat;
  - c. Control access to email domains in a Zoom directory;
  - d. Enable hosts to control who can share screens;
  - e. Allow hosts to limit participants of a meeting to specific email domains;
- and
- f. Allow hosts to limit participants with accounts, to the extent applicable.

12. Zoom has removed and shall not reinstate the LinkedIn Navigator feature.

#### Protection of Users from Abuse

13. Zoom shall continue to maintain reasonable procedures to enable users to easily report violations of the Zoom Acceptable Use Policy, including allowing meeting hosts to

report a user for engaging in abusive conduct.

14. Zoom shall update the Zoom Acceptable Use Policy specifically to clarify that prohibitions against abusive conduct include hatred against others based on race, religion, ethnicity, national origin, gender, or sexual orientation.

15. Zoom shall continue to implement policies to investigate reported misconduct and violations of the Zoom Acceptable Use Policy and to take appropriate corrective action, including to suspend or ban users who violate the Acceptable Use Policy.

#### Audits and Testing

16. Zoom shall provide a copy of its annual SOC 2 report to the NYAG within thirty days of issuance. If Zoom obtains an outside auditor certification with more stringent requirements than the SOC 2 report, it may provide that report instead.

17. Zoom has implemented and shall continue to maintain a risk-based penetration-testing program reasonably designed to identify, assess and remediate security vulnerabilities, which shall include at least one annual white box penetration test.

#### Miscellaneous

18. Zoom shall continue to offer – or where not currently offered, shall offer – a channel for user complaints about abusive conduct on the platform, and its policies for reviewing complaints and taking corrective action concerning abusers will continue to include meaningful human oversight.

19. Zoom shall facilitate external monitoring of its platform as follows:

a. Zoom shall continue to maintain a bug bounty program for researchers and the public to report vulnerabilities found in Zoom's platform. Zoom shall issue financial awards for discovery and reporting of bugs in amounts that (1) are commensurate with the severity of the vulnerability, the scale of exposure, and sensitivity of the personal information exposed, and (2) are not unreasonably below the market rate for bounties concerning vulnerabilities that are equivalent in severity, scale, and sensitivity of personal information.

b. Zoom shall continue to maintain a portal for users, consumer advocates and watchdog groups to submit complaints involving privacy and data security concerns. Zoom shall review all complaints within a reasonable time after receipt.

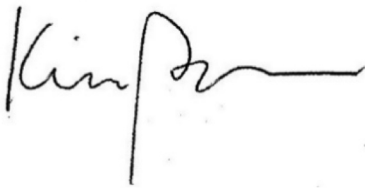
20. Zoom shall continue its practice of defaulting free, K-12 educational accounts, and Pro (or its equivalent tier) provisioned in the United States to data centers located in the United States.

21. Zoom neither admits nor denies the factual and legal allegations in this agreement. The agreement is not intended for use by any third party in any other proceeding and does not create a cause of action for any private party.

22. Based on the assurance and commitments by Zoom, the NYAG is closing its investigation in this matter. The NYAG has agreed to the terms of this agreement based on, among other things, the representations made to the NYAG by Zoom and its counsel and the NYAG's own factual investigation as set forth in background section above. Zoom represents and warrants that neither it nor its counsel has made any material representations to the NYAG that are inaccurate or misleading. If any material representations by Zoom or its counsel are later found to be inaccurate or misleading, this agreement is voidable by the NYAG in its sole discretion. The term of this agreement shall be three years from the date of execution.

23. This agreement shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

Sincerely,



Kim A. Berger | Chief  
Bureau of Internet and Technology  
New York State Office of the Attorney General  
28 Liberty Street, New York, NY 10005  
212-416-8456

AGREED AND ACCEPTED:

Zoom Video Communications, Inc.

/s

---