# UNITED STATES
# SECURITIES AND EXCHANGE COMMISSION
**WASHINGTON, D.C. 20549**

# FORM 8-K

**CURRENT REPORT**

**Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934**

**Date of Report (Date of earliest event reported): December 18, 2020**

# Zoom Video Communications, Inc.

**(Exact name of Registrant as Specified in Its Charter)**

| **Delaware** | **001-38865** | **61-1648780** |
|---|---|---|
| **(State or Other Jurisdiction of Incorporation)** | **(Commission File Number)** | **(IRS Employer Identification No.)** |

| **55 Almaden Boulevard, 6th Floor San Jose, California** | **95113** |
|---|---|
| **(Address of Principal Executive Offices)** | **(Zip Code)** |

**(888) 799-9666**
**(Registrant's Telephone Number, Including Area Code)**

**Not Applicable**
**(Former Name or Former Address, if Changed Since Last Report)**

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instructions A.2. below):

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

**Securities registered pursuant to Section 12(b) of the Act:**

| Title of each class | Trading Symbol(s) | Name of each exchange on which registered |
|---|---|---|
| Class A Common Stock, $0.001 par value per share | ZM | The Nasdaq Global Select Market |

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☒

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☒

**Item 8.01 Other Events.**

On December 18, 2020, Zoom Video Communications, Inc. (the "Company") issued a blog post regarding the announcement by the United States Department of Justice that a former employee of the Company has been charged with conspiracy to commit interstate harassment and unlawful conspiracy to transfer a means of identification in connection with an alleged scheme to disrupt video meetings commemorating Tiananmen Square. The Company also released its December 18, 2020 transparency report.

Copies of the blog post and transparency report are attached hereto as Exhibits 99.1 and 99.2, respectively.

**Item 9.01 Financial Statements and Exhibits.**

| Exhibit No. | Description |
|---|---|
| 99.1 | Blog post dated December 18, 2020. |
| 99.2 | Transparency report dated December 18, 2020. |

**SIGNATURES**

Pursuant to the requirements of the Securities Exchange Act of 1934, as amended, the Registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

**ZOOM VIDEO COMMUNICATIONS, INC.**

Dated: December 18, 2020

By: /s/ Aparna Bawa
Aparna Bawa
Chief Operating Officer

**Our Perspective on the DOJ Complaint**
**By Zoom**

We would like to start by making three important points:

1. **We support the U.S. Government's commitment to protect American interests from foreign influence.** As the DOJ notes, Zoom has been fully cooperating with them in this matter. We have also been conducting a thorough internal investigation, and we terminated for violating company policies the China-based former employee charged in this matter. We have also placed other employees on administrative leave pending the completion of our investigation.
2. **We are dedicated to the free and open exchange of ideas.** As the DOJ makes clear, every American company, including Zoom and our industry peers, faces challenges when doing business in China. We have taken actions to make our values clear. We issued our Government Requests Guide in July, through which we subject any government request to a careful review, prioritizing the privacy, security, and safety of our users at all times. We have also made tremendous investments in our platform and have implemented robust policies and safeguards.
3. **We will continue to act aggressively to anticipate and combat ever-evolving data security challenges.** We launched our end-to-end encryption feature to free and paid users worldwide. We have significantly enhanced our internal access controls. We have also ceased the sale of direct and online services in China and launched engineering hubs in the United States, India, and Singapore.

**Background**

In September 2019, the Chinese government turned off our service in China without warning. At that time, we were a much smaller company primarily serving businesses. The shutdown caused significant disruption for many of our multinational customers, who could not effectively communicate with their employees and partners in China. They urged us to take immediate action to get the service resumed.

The shutdown put Zoom in an unfamiliar and uncomfortable position. Like many fast-growing companies, we were focused on building the best possible product and delighting our customers. We had not, at that point in our evolution, been forced to focus on societal or policy concerns outside of this relatively narrow frame of vision.

As we worked to resolve the shutdown, China requested that Zoom confirm it would comply with Chinese law, including designating an in-house contact for law enforcement requests and transferring China-based user data housed in the United States to a data center in China. With the goal of restoring our service, Zoom personnel, including our CEO, met in China with government authorities in October 2019. We outlined steps we could take to address the Chinese government's reasons for shutting down our service. This is the "rectification plan" that the DOJ cited in its complaint. The plan included measures to comply with real ID and data localization requirements applicable in China, in a manner that is capable of audit and verification, as well as establishing a legal entity in China to meet China's local legal and regulatory requirements. The plan also references measures that we did not carry out, such as working with a local Chinese partner to develop technology that would analyze the content of meetings hosted in China to

identify and report illegal activity and shut down meetings that violate Chinese law. The plan also contains information about actions Zoom previously took to adhere to Chinese law, including shutting down certain types of political, religious, and sexually explicit meetings. The goal of the rectification plan was to get our service restored, and the Chinese government ultimately unblocked Zoom on November 17, 2019.

In October 2019, Zoom appointed the now-former employee to serve as the government contact in China. This former employee's job included responding to the Chinese government's requests for account terminations, meeting terminations, and user data. While the DOJ did not share with us its factual allegations in advance of the public release of the complaint, we learned during the course of our investigation that this former employee violated Zoom's policies by, among other things, attempting to circumvent certain internal access controls. We have terminated this individual's employment. We have also placed other employees on administrative leave pending the completion of our investigation.

During the time this individual was employed by Zoom, he took actions resulting in the termination of several meetings in remembrance of Tiananmen Square and meetings involving religious and/or political activities, some of which were hosted by non-China-based users. We terminated the host accounts associated with certain of these meetings.* We learned during our investigation that this former employee also shared or directed the sharing of a limited amount of individual user data with Chinese authorities. At this stage in our investigation, and with the exception of user data for fewer than ten individual users, we do not believe this former employee or any other Zoom employee provided the Chinese government with user data of non-China-based users. The former employee also potentially shared meeting information for a Tiananmen Square remembrance. There is no indication that any enterprise data was shared with the Chinese government.

While the complaint alleges that the former employee obtained Zoom account and user IDs associated with the Xinjiang region of China, our investigation shows that this data was anonymized, and at this time we do not have reason to believe that it was shared with the Chinese government.

**DOJ and SEC Investigations**

In June 2020, Zoom received a grand jury subpoena from the Department of Justice's U.S. Attorney's Office for the Eastern District of New York (EDNY). This subpoena requested information regarding our interactions with foreign governments and foreign political parties, including the Chinese government. In addition, it requested information regarding storage of and access to user data, the development and implementation of Zoom's privacy policies, and the actions Zoom took relating to the Tiananmen commemorations on Zoom. Zoom has since received additional subpoenas from EDNY seeking related information.

In July 2020, we received subpoenas from the Department of Justice's U.S. Attorney's Office for the Northern District of California (NDCA) and the U.S. Securities and Exchange Commission. Both subpoenas seek documents and information relating to various security and privacy matters, including Zoom's encryption, and Zoom's statements relating thereto, as well as calculation of usage metrics and related disclosures. In addition, the NDCA subpoena seeks information relating to any contacts between Zoom employees and representatives of the Chinese government, and any attempted or successful influence by any foreign government in Zoom's policies, procedures, practices, and actions as they relate to users in the United States.

We are fully cooperating with all of these investigations and have been conducting our own thorough internal investigation.

**What We've Done**

We are committed to rigorously examining how we navigate a complex and contentious global environment. We have dedicated ourselves to helping the world during the pandemic, and we are honored to have helped individuals, schools, hospitals, governments, and businesses around the world stay connected during this difficult time. We also serve the U.S. Government through our Zoom for Government platform, which is 100% deployed in continental U.S. data centers and managed by U.S.-based, U.S. persons only.

Facilitating the free and open exchange of ideas is one of our key missions. Over the last several months, we have reaffirmed our commitments to this mission and to maintaining the highest standards of trust and security. We have worked hard to develop robust tools and policies to help uphold those commitments. For example:

- **End-to-end encryption:** We launched our end-to-end encryption feature to free and paid users worldwide;
- **Geo-fenced data routing:** We implemented strict geo-fencing procedures around our mainland China data center. No meeting content will ever be routed through our mainland China data center (one of 19 co-located data centers routing traffic) unless the meeting includes a participant from China. Our paid customers have the ability to choose the specific data centers through which their data is routed;
- **Internal access controls:** We significantly enhanced our internal access controls. Among other things, we have restricted China-based employees' access to Zoom's global production network;
- **Government Requests Guide:** We implemented a Government Requests Guide, which provides that Zoom will subject any government request to a careful and thoughtful review, prioritizing the privacy, security, and safety of our users at all times. Zoom's handling of requests from any government must now receive approval by Zoom's U.S. legal department; and
- **Employee training:** We've conducted robust training for employees focused on data protection and compliance.

We have made numerous other well-documented security enhancements, and our work is never done. We have U.S.-based security engineering and source compliance teams that conduct periodic reviews of source code. We are also establishing an Insider Threat Program that ensures that Zoom has necessary information on its current and prospective employees to assess insider threat risk and systems to flag warning signs of suspicious behavior of current and prospective employees.

At Zoom, we exist to serve our users. We remain committed to fulfilling the expectations of the millions of people that trust and rely on our platform.

**We have updated our June 11 blog post regarding the meetings in remembrance of Tiananmen Square to reflect information we have recently learned*.

**Safe Harbor for Forward-Looking Statements**

Certain statements contained in this post constitute “forward-looking statements” within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended, and are based on our current beliefs, understanding and expectations regarding the governmental and internal investigations described in this post and the underlying events that are the subject of those investigations. These investigations are ongoing, and we do not know when they will be completed, which facts we will ultimately discover as a result of the investigations, or what actions the government may or may not take.

Forward-looking statements are only predictions and are subject to additional future events, risks, and uncertainties, many of which are beyond our control or are currently unknown to us. These risks and uncertainties include but are not limited to additional facts that we may learn as a result of our ongoing investigation or from evidence presented to us by the U.S. Government, actions taken by the U.S. Government enforcement and regulatory agencies with respect to the events described in this blog, actions taken by the Chinese government that may impact our business operations, including our ability to operate in China, and the potential impact that any of these events, risks, and uncertainties may have on our employees. With respect to the continued safety and security of our platform, we face additional events, risks, and uncertainties, including the risk of our security measures being compromised in the future, any actual or perceived failure to comply with evolving privacy, data protection and information security laws, regulations, standards, policies, and contractual obligations, delays or outages in services from our co-located data centers, and failures in internet infrastructure or interference with broadband access, which could cause current or potential users to believe that our platform is unreliable. Additional risks and uncertainties that could cause actual outcomes and results to differ materially from those contemplated by the forward-looking statements are included under the caption “Risk Factors” and elsewhere in our most recent filings with the Securities and Exchange Commission, including our quarterly report on Form 10-Q for the quarter ended October 31, 2020.

Forward-looking statements speak only as of the date they are made, and we do not undertake to update these statements other than as required by law and specifically disclaim any duty to do so.

# Transparency Report Overview

Released: December 18, 2020

We are pleased to offer our first transparency report, which we intend to publish semiannually beginning in 2021. This report is designed to offer insight into how Zoom Video Communications, Inc. (Zoom) responds to requests for user data from law enforcement agencies and government authorities. Zoom believes that transparency is critical to building trust and fostering the free and open exchange of ideas.

As detailed in our Privacy Statement, Zoom is committed to protecting user privacy and only produces user data to governments in response to valid and lawful requests in accordance with our Government Requests Guide and relevant legal policies.

This report covers government requests that we processed between May 1, 2020 and December 12, 2020. Until spring 2020, when our user base expanded significantly as a result of the Covid-19 pandemic, Zoom had no set approach to these law enforcement requests. Like many smaller technology companies without a significant consumer user base, we received requests via multiple avenues, handled each one in a high-touch, intensive way, and didn't preserve categorizing information about them. As our usage soared following the beginning of the pandemic that approach became untenable. After a period of ramping up and resourcing, we developed a more streamlined approach to handle the volume. Our first improvements included hiring experienced legal staff to evaluate and process requests efficiently, publishing our Government Requests Guide to enable law enforcement agencies and government authorities to submit more tailored requests, and categorizing the data associated with each request in our case management system. We've also standardized our policies, centralized how we track requests, and established internal guidelines and quality controls processes. All of these improvements were made with an eye towards transparency reporting.

Because many of the procedures that Zoom now uses to confirm the receipt of government requests were implemented on or about July 1, 2020, our ability to accurately identify government requests has significantly improved since that date. This means that we cannot guarantee that our May and June 2020 records are fully accurate. Nevertheless, the Report discloses the requests we processed from May 1, 2020 through December 12, 2020 of which we are currently aware, and, while we now have additional processes in place for handling and tracking these types of requests, it remains possible that we received additional requests during this period that were not properly tracked or otherwise identified by us in the preparation of this report.

Two further notes about this transparency report: In May and June of this year, there were meetings in remembrance of Tiananmen Square. Zoom received several requests from Chinese government authorities in the days of and leading up to these meetings, some of which resulted in our termination of specific meetings. Those requests are reflected in this report.

As described in our blog post published on December 18, 2020, we terminated a China-based employee who was responsible for responding to Chinese government requests because this individual violated Zoom's policies by, among other things, attempting to circumvent certain internal access controls, including those required to manage government requests as described in this report.

The United States DOJ has charged this former employee with conspiracy to commit interstate harassment and unlawful conspiracy to transfer a means of identification in connection with an alleged scheme to disrupt video meetings commemorating Tiananmen Square. We are cooperating with the DOJ in these investigations, which are ongoing, and we do not know when they will be completed. As a result, the outcome of these investigations will be informed by the discovery of additional facts that are an inherent part of any ongoing investigation. The discovery of additional facts from our own investigation or from evidence presented by the DOJ or the SEC could impact the information that is contained in this report. We will not update this transparency report for this reporting period other than as required by law.

## Definitions

We use a number of terms in this report that have specific legal meanings in this context. Wherever you don't see a particular kind of request or outcome noted in the charts or graphs, that means that there weren't any of that type. Notably, we did not disclose any content in this reporting period, nor did we receive any national security requests.

- ***Subpoena*** (U.S. only) - a request made by an entity with investigative powers, such as a grand jury. Need not be signed by a judge, cannot demand content.
- ***Search Warrant*** (U.S. only) - a request for a search, signed by a judge, in which a prosecutor alleges that there is "probable cause" to believe that a crime has taken place, or is about to. May demand content or non-content.
- ***Order*** (U.S. only) - any other type of order issued by a court. Cannot demand content.
- ***Other -*** Any other kind of request or resolution. For example, if a law enforcement officer writes seeking user data but without a subpoena, search warrant, or court order, or where the data owner gives written authorization to disclose their data to law enforcement.
- ***Preservation Request*** (U.S. or international) - a request to preserve user information for a period of time, usually 90 or 180 days. We do not disclose information in response to preservation requests.
- ***Emergency Request*** - (U.S. or international)- a request for user data without standard legal process, on the grounds that there is a danger of death or serious physical injury to a person.
- ***MLAT Request*** (International only) **-** a request made by a foreign country through the U.S. Department of Justice pursuant to a Mutual Legal Assistance Treaty. Can demand content.

- ***CLOUD Act*** (U.K. only, for now)- a request made pursuant to the CLOUD Act. Can demand content.
- ***Withhold Access Request*** - a governmental request to restrict an individual's access to any aspect of Zoom's product, or to prevent or terminate a particular meeting.
- ***Rejected -*** includes rejections for invalid service or other legal reasons, instances where there was no responsive data, or where the law enforcement agency did not provide enough information for us to locate data.
- ***Non-content*** - non-content refers to metadata, or information about content. Non-content can include things like the dates and times of meetings, the IP address of a user, or information about their platform. When we report disclosing "non-content" that means we disclosed non-content only.
- ***Content*** - can include video content, chat logs or transcripts; essentially, any media that depicts what a person spoke, wrote or did. When we report disclosing "content," that means we disclosed both content and non-content.
- ***General information*** means we provided general information about the law enforcement request process, but not content or non-content.

A note about Withhold Access Requests: Zoom does business in more than 80 countries and counting. Many countries, including the U.S., have laws that may restrict one of its residents from participating in or hosting particular Zoom meetings or webinars. If Zoom receives a legally valid and appropriately scoped request from a legitimate government agency demanding that Zoom restrict one of its residents from using Zoom, Zoom will carefully review it. In no event will Zoom will restrict the access of users who are outside the requesting country and/or the jurisdiction of the requesting government agency or who are otherwise not subject to applicable local law.

We comply with Withhold Access Requests selectively, as we balance our commitment to promoting the free and open exchange of ideas against our legal obligations.

## U.S. Requests Overview

U.S. requests to Zoom can come in the form of search warrants, subpoenas (grand jury, trial and administrative), court orders, preservation requests, emergency requests and national security requests. The vast majority of global requests are from U.S. State and Local and Federal law enforcement with 803 coming from the U.S. and 424 coming from all other areas combined. Civil litigation requests are not reflected in this report.

Here is a summary of the U.S. requests we've processed for user-related data, as defined in our Government Requests Guide:

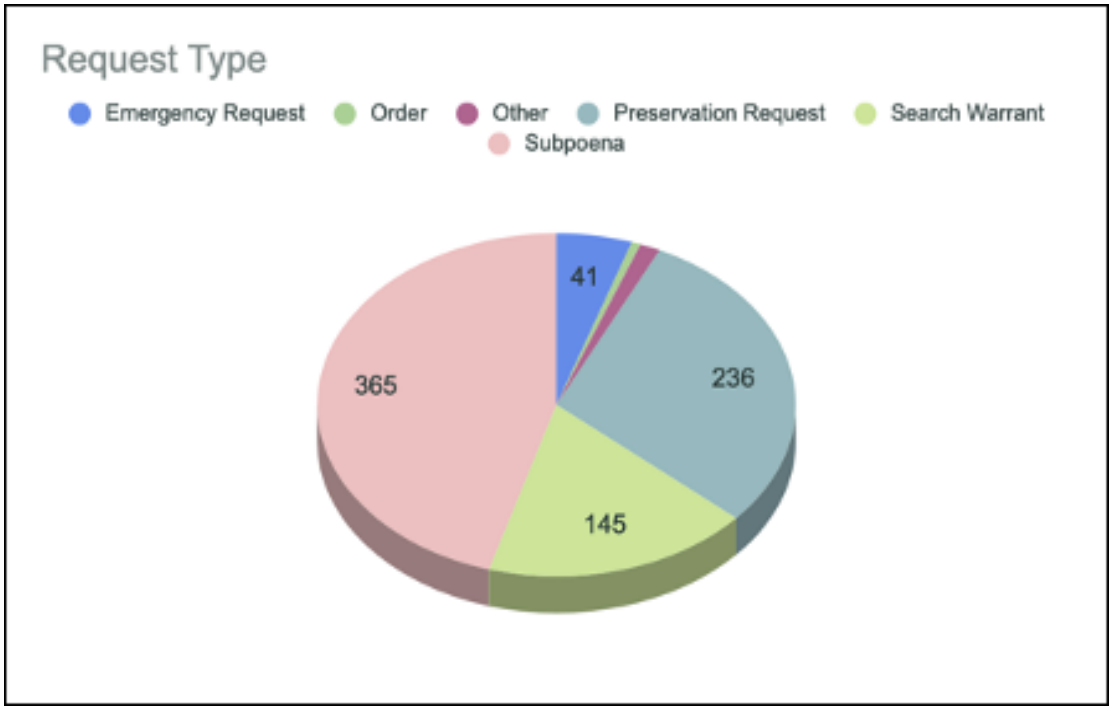
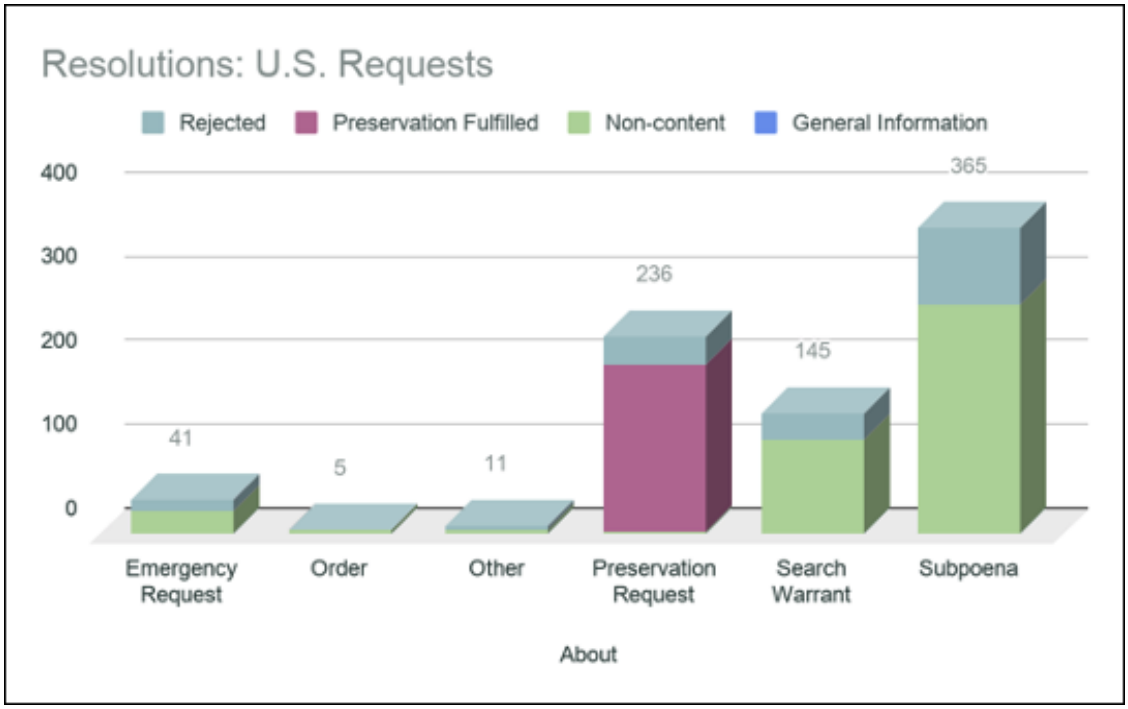


Exhibit 99.2

## U.S. Requests: Responses and Outcomes

From May through December 12, 2020, here is how we've responded to requests from U.S. authorities.

| *About* | *Resolution* General Information | Non-content | Preservation Fulfilled | Rejected | Grand Total |
|---|---|---|---|---|---|
| Emergency Request | 1 | 26 | | 14 | 41 |
| Order | | 5 | | | 5 |
| Other | | 7 | | 6 | 12 |
| Preservation Request | 1 | | 201 | 33 | 236 |
| Search Warrant | 1 | 111 | | 33 | 145 |
| Subpoena | | 274 | | 91 | 365 |
| **Grand Total** | **3** | **422** | **201** | **177** | **803** |



## International Requests

Zoom receives law enforcement requests from around the globe. We screen each international request carefully to ensure that we only respond to ones that are legally valid and appropriately scoped. We do not provide any content internationally without process under MLAT, the CLOUD Act or letters rogatory. Please note some countries or regions may have experienced more rejections prior to July 1, when we published our Government Requests Guide and provided guidance about what is an appropriate request and what types of data we have available.

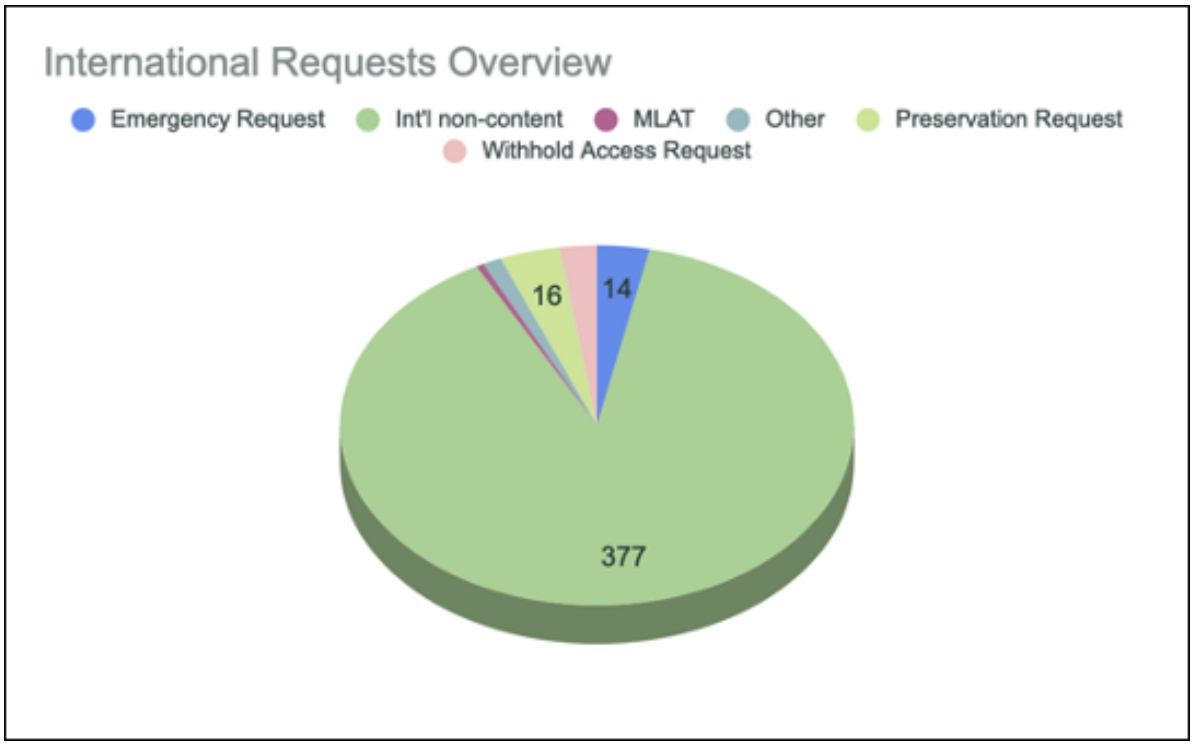
For more information about how we review international requests, please see our Government Requests Guide.

**We group international requests into regions:**

- UK (United Kingdom)
- EMEA (Europe, Middle East, and Africa)
- China
- India
- Asia Pacific (including Hong Kong SAR and New Zealand, excluding China and India)
- North America (non U.S.)
- South and Central America
- Australia

Here is an overview of the international requests we've received:

Exhibit 99.2



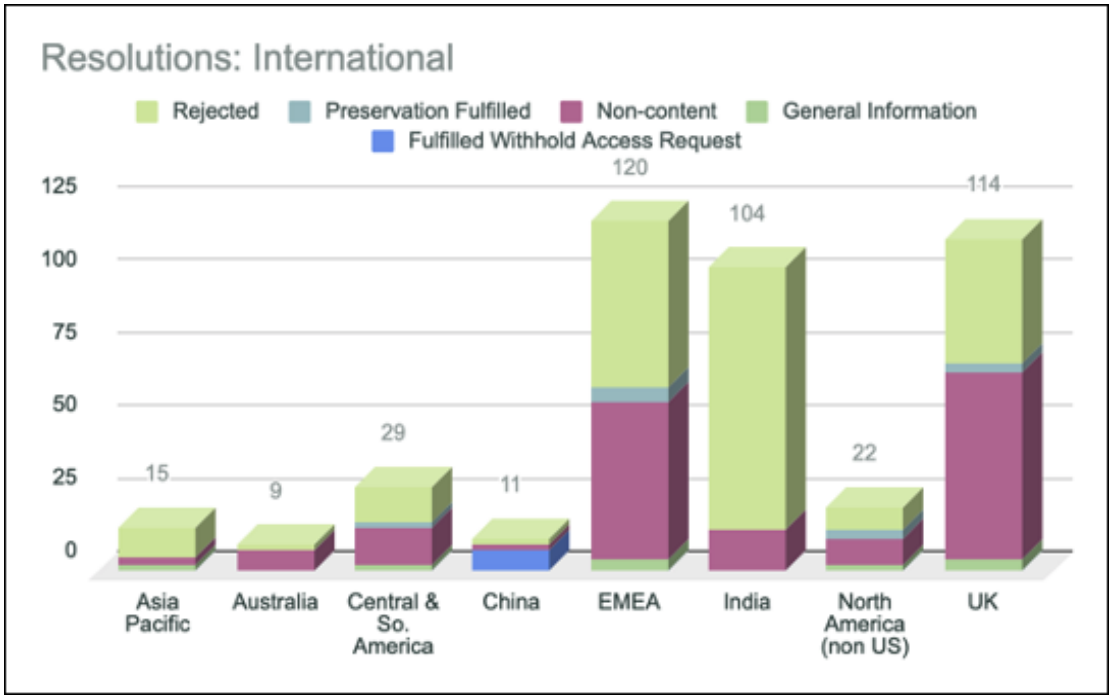

Here is how we responded:

| | *Resolution* | | | | | |
|---|---|---|---|---|---|---|
| *Jurisdiction* | Fulfilled Withhold Access Request | General Information | Non-content | Preservation Fulfilled | Rejected | Grand Total |
| Asia Pacific | | 2 | 3 | | 10 | 15 |
| Australia | | | 7 | | 2 | 9 |
| Central & So. America | | 2 | 13 | 2 | 12 | 29 |
| China | 7 | | 2 | | 2 | 11 |
| EMEA | | 4 | 54 | 5 | 57 | 120 |
| India | | | 14 | | 90 | 104 |
| North America (non US) | | 2 | 9 | 3 | 8 | 22 |
| UK | | 4 | 64 | 3 | 43 | 114 |
| **Grand Total** | **7** | **14** | **166** | **13** | **224** | **424** |

Exhibit 99.2

## International Requests: Responses and Outcomes

From May through December 12, 2020, here's how we responded to international requests:




### Asia Pacific (excludes China, India and Australia)

| *Asia Pacific* | *Resolution* | | | |
|---|---|---|---|---|
| *About* | General Information | Non-content | Rejected | Grand Total |
| Int'l non-content | 2 | 3 | 10 | **15** |

### Australia

| *Australia* | *Resolution* | | |
|---|---|---|---|
| *About* | Non-content | Rejected | Grand Total |
| Int'l non-content | 7 | 2 | **9** |

Exhibit 99.2

## Central and South America

| *Cent. & So. America* | *Resolution* | | | | |
|---|---|---|---|---|---|
| ***About*** | General Information | Non-content | Preservation Fulfilled | Rejected | Grand Total |
| Emergency Request | | 1 | | 1 | **2** |
| Int'l non-content | 2 | 12 | | 10 | **24** |
| Other | | | | 1 | **1** |
| Preservation Request | | | 2 | | **2** |
| **Grand Total** | **2** | **13** | **2** | **12** | **29** |

## China

| *China* | *Resolution* | | | |
|---|---|---|---|---|
| ***About*** | Fulfilled Withhold Access Request | Non-Content | Rejected | Grand Total |
| Int'l non-content | | 2 | 1 | **3** |
| Withhold Access Request | 7 | | 1 | **8** |
| **Grand Total** | **7** | **2** | **2** | **11** |

## EMEA

| *EMEA* | *Resolution* | | | | |
|---|---|---|---|---|---|
| ***About*** | General Information | Non-content | Preservation Fulfilled | Rejected | Grand Total |
| Emergency Request | | | | 2 | 2 |
| Int'l non-content | 4 | 53 | 1 | 52 | 110 |
| MLAT | | 1 | | | 1 |
| Other | | | | 2 | 2 |
| Preservation Request | | | 4 | 1 | 5 |
| **Grand Total** | **4** | **54** | **5** | **57** | **120** |

Exhibit 99.2

## India

| About | Non-content | Rejected | Grand Total |
|---|---|---|---|
| Int'l non-content | 14 | 87 | 101 |
| Other | | 1 | 1 |
| Withhold Access Request | | 2 | 2 |
| **Grand Total** | **14** | **90** | **104** |

## North America (non-U.S.)

| North America | Resolution | | | | |
|---|---|---|---|---|---|
| About | General Information | Non-content | Preservation Fulfilled | Rejected | Grand Total |
| Emergency Request | | 1 | | 1 | 2 |
| Int'l non-content | 2 | 7 | | 5 | 14 |
| Other | | 1 | | | 1 |
| Preservation Request | | | 3 | 2 | 5 |
| **Grand Total** | **2** | **9** | **3** | **8** | **22** |

## UK

| UK | Resolution | | | | |
|---|---|---|---|---|---|
| About | General Information | Non-content | Preservation Fulfilled | Rejected | Grand Total |
| Emergency Request | | 6 | | 2 | 8 |
| Int'l non-content | 4 | 56 | | 41 | 101 |
| MLAT | | 1 | | | 1 |
| Preservation Request | | 1 | 3 | | 4 |
| **Grand Total** | **4** | **64** | **3** | **43** | **114** |

For more information about how Zoom processes Government Requests globally, please see our Government Requests Guide and Government Requests Frequently Asked Questions.