# Cisco Transparency and Law Enforcement Demands for Customer Data

## Reporting Period: July 1st -Dec 31st, 2020

Cisco is committed to being transparent about government demands for customer data received from government and law enforcement agencies globally. We publish transparency reports twice yearly covering a reporting period of either January to June or July to December. Each report is published six months following the end of the reporting period.

The following tables list the total number of demands for customer data received from government and law enforcement agencies by type of customer data demanded. This includes the number of demands that were rejected, the number of demands that did not result in disclosure, and the number of demands that resulted in disclosure.

### Government Data Demands – United States (exclusive of National Security Demands, which are reported below)

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 5 | 4 | 1 | 0 |
| Non-Content Data | 26 | 15 | 5 | 6 |
| Emergencies | 0 | 0 | 0 | 0 |

### United States National Security Demands

Cisco may receive demands for data from U.S. national security organizations. This includes Foreign Intelligence Surveillance Act (FISA) warrants, orders, directives, or National Security Letters (NSLs). The table below lists the number of U.S. National Security demands Cisco has received during the applicable period, subject to the limitations prescribed by the USA Freedom Act of 2015. For example, in a period where Cisco receives such a demand, the law would limit Cisco's ability to report the exact number of orders received and specifies that these demands be reported within a broader band of numbers, and with a six-month delay.

| July 1st - December 31st, 2020 | Totals |
|---|---|
| National security orders, directives, or national security letters received | 0 |
| Number of accounts affected under all national security orders, directives, or national security letters | 0 |

## International

### Government Data Demands –Germany

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 0 | 0 | 0 | 0 |
| Non-Content Data | 8 | 0 | 0 | 8 |
| Emergencies | 0 | 0 | 0 | 0 |

### Government Data Demands –India

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 0 | 0 | 0 | 0 |
| Non-Content Data | 7 | 1 | 6 | 0 |
| Emergencies | 0 | 0 | 0 | 0 |

### Government Data Demands –Russia

| Data Type Demanded | Total Demands | No Data Found | Total Rejected | Total Disclosed |
|---|---|---|---|---|
| Content Data | 0 | 0 | 0 | 0 |
| Non-Content Data | 1 | 0 | 1 | 0 |
| Emergencies | 0 | 0 | 0 | 0 |

### Percent Disclosed

| July 1st - December 31st, 2020 | Totals | % Disclosed |
|---|---|---|
| Demands Received | 47 | 29.8% |

### Preservation Requests

A preservation request asks that data be saved for a specified period of time in anticipation of a legal process (i.e. search warrant, court order, etc.) to ensure data is not tampered, destroyed, or lost until the legal process can be concluded. This time frame is specified in the preservation request and may result in data being stored longer than its standard retention period.

| July 1st - December 31st, 2020 | Totals |
|---|---|
| Preservation Requests Received from the United States | 3 |
| Preservation Requests Received from outside of the United States | 0 |

# Frequently Asked Questions

**Q. How does Cisco respond to Government Data Demands?**

Cisco will assess and respond to government and law enforcement demands for customer data in accordance with Cisco's Terms of Service, privacy policies, and applicable law. We carefully review each demand we receive to ensure we are protecting the privacy of our customers while meeting our legal obligations. For more detail on how we respond to demands for customer data, please see our Principled Approach to Government Demands for Data. The Trust Center is the best source of information on how Cisco is Trustworthy, Transparent, and Accountable to our customers.

**Q. What is the difference between content and non-content data?**

Cisco categorizes data into three categories: Systems Information, Personal Data, and Customer Content. These definitions are outlined in the Data Management page of Cisco's Trust Center, as well as in the Data Briefs hosted on the Cisco Trust Portal. U.S. law places a higher burden on government requests for content data than non-content data. Content data aligns to Cisco's "Customer Content" (formerly "Customer Data") classification, and includes text, audio, video, or image files our customers create in connection with the use of Cisco products or services. Non-content data generally aligns to Cisco's "Systems Information" and "Personal Data" classifications, and includes basic subscriber information such as name, address, phone number, IP address and email address, payment data such as credit card information, and telemetry data generated in connection with customer's use such as URLs, net flow data, and information relating to the existence of cookies.

**Q. What is an Emergency Request?**

Law enforcement may demand information from Cisco that is needed to help resolve imminent threats to life or serious physical harm. Where authorized by applicable law, Cisco may provide information in such emergencies, and we have an established process to respond to emergency demands.

**Q. Does Cisco ever challenge government demands for data?**

Demands that are not accompanied by a valid legal process or a valid legal basis are challenged or rejected. Our legal team will seek additional clarification from government and law enforcement officials to narrow the scope of demands that are unclear or overly broad. Cisco believes that governments and law enforcement agencies should go directly to customers for content and non-content data requests in the first instance.

**Q. How has Cisco responded to the CLOUD Act?**

The Clarifying Lawful Overseas Use of Data (or CLOUD Act) is a United States federal law passed in 2018 that allows federal law enforcement to compel, via warrant or subpoena, U.S.-based technology companies to provide requested data regardless of whether the data is stored domestically or abroad. It also authorizes the U.S. government to enter into executive agreements allowing foreign governments to request data directly from American providers. As of this Transparency Report, the United States has entered into one such agreement with the United Kingdom. In the past, Cisco has provided reporting on the CLOUD Act. Through incorporating customer feedback, we are in the process of revamping future

iterations of our Transparency Reports to provide more granularity on the impacts of this legislation. All requests received by Cisco are carefully reviewed and subject to Our Principled Approach to Government Demands for Data, below.

**Q. If Cisco receives a demand for customer information, will Cisco tell the customer about it?**

Cisco's policy is to notify customers before producing content in response to legally valid demands unless such notification to the customer is prohibited by applicable law or emergency circumstances prevent advanced notification. Where appropriate, Cisco will challenge demands that prohibit notification to the customer, through appropriate legal process or other means. For more information, please see Our Principled Approach to Government Demands for Data.

**Q. Why do some new reports show more information than older reports?**

We are constantly working to improve our internal processes and to bring increased transparency to our customers. As a result, we have expanded this report to include country-level information on demands, the number of demands Cisco rejected, the percent of demands where data was disclosed, and the number of preservation requests we have received.

**Q. Why are only certain countries represented on this report?**

Countries that provided a government data demand to Cisco during the current reporting period are illustrated above. If a country isn't included in the tables above, Cisco did not receive any data demands in that jurisdiction during the reporting period.

**Q. Does Cisco ever give governments direct access to content or non-content data, or create back-doors?**

Cisco never gives governments or law enforcement agencies access to content or non-content data without following the appropriate legal process. Consistent with Cisco's Security Vulnerability Policy, our product development practices specifically prohibit any intentional behaviors or product features that are designed to allow unauthorized device or network access, exposure of sensitive device information, or a bypass of security features or restrictions (including, but not limited to, undisclosed device access methods or "backdoors").

**Q. How does Cisco consider Human Rights when responding to Government Demands for Customer Data?**

Cisco's approach to respecting human rights is outlined in our Global Human Rights Policy, which is grounded in the United Nations Guiding Principles on Business & Human Rights. Our Principled Approach to Government Data Demands is designed to minimize disclosure of customer data, uphold and respect human rights, and promote accountability and transparency with our customers and the public.

**Q. How can government agencies send legal demands to Cisco?**

If you are an official representative of a Government or Law Enforcement agency and you are seeking data from Cisco, you may email your legal demand to govt-data-subpoenas@cisco.com. If government and law enforcement agencies have served the legal process by email to govt-data-subpoenas@cisco.com, there is no need to serve a duplicate hardcopy process on Cisco by mail.

**Q. Who should I contact for questions regarding the Transparency Report or Cisco's Principled Approach to Demands for Customer Data?**

Cisco is committed to the transparency of our systems and processes, and accountability to our customer promises. Please direct any questions regarding the Transparency Report or Cisco's Principled Approach to govt-data-requests@cisco.com.