

Cisco Transparency and Law Enforcement Requests for Customer Data

Cisco is committed to publishing data regarding requests or demands for customer data that we receive from law enforcement and national security agencies around the world. We publish this data twice yearly (covering a reporting period of either January-to-June or July-to-December). Cisco reports these numbers with a six-month delay.

The table below lists the number of requests Cisco has received from United States federal, state or local law enforcement during the stated time period. A table with requests from International agencies follows. National Security Requests and Clarifying Lawful Overseas Use of Data (CLOUD) Act orders are listed in separate tables later in this document.

NOTE: If a single request includes both customer and non-customer data, Cisco reports these as two individual requests. Further, the numbers listed in the columns titled *No Data Disclosed* include requests for which Cisco was unable to identify responsive data as well as requests for which Cisco determined the accompanying legal process to be insufficient.

July 1–December 31, 2017	Total Requests	No Data Disclosed	Data Disclosed
Customer Data	4	4	0
Non-Customer Data	41	39	2
Emergencies	0	0	0

Government Data Requests – International		Data Disclosed	Data Disclosed
Customer Data	0	0	0
Non-Customer Data	1	1	0
Emergencies	0	0	0

Customer Data is all data (including text, audio, video or image files) that is provided to Cisco in connection with your use of our products or services. Customer Data does not include Administrative Data, Payment Data, Support Data or Telemetry Data, as defined in the [Data Definitions](#) document. Requests that do not fall into the Customer Data category are listed as “Non- Customer Data.”

Cisco carefully reviews each request we receive. [Cisco's Principled Approach to Government Requests for Data](#) outlines how Cisco protects customers while assisting law enforcement under the appropriate legal conditions. [The Trust Center](#) is the best source of information on how Cisco is Trustworthy, Transparent and Accountable to our customers.

Emergency Requests

Law enforcement may request information from Cisco that is needed to help resolve serious emergencies. Cisco is authorized by federal law to provide the requested information in such emergencies and we have an established process to respond to emergency requests, in accordance with the law.

National Security Requests

Cisco may receive requests for data from national security organizations. This includes Foreign Intelligence Surveillance Act (FISA) court orders, warrants and directives, and FBI National Security Letters (NSLs). The table below lists the number of National Security Requests Cisco has received during the applicable period.

July 1-December 31, 2017	Total Requests	No Data Disclosed	Data Disclosed
Customer Data	0	0	0

The CLOUD Act is a U.S. federal law enacted in 2018 that modernized data privacy and government surveillance laws to reflect industry cloud computing practices. Primarily the CLOUD Act amends the Stored Communications Act (SCA) of 1986 to allow federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil. Additionally, the CLOUD Act enables law enforcement from non-US countries to, with agreement of the US Government, go directly to US companies to request data.

NOTE: In the next report Cisco, will share data about CLOUD Act requests. This data will be an aggregate of both U.S. Federal requests as well as non-U.S. country law enforcement requests. Requests noted here will also be reflected in other categories of this report as we treat our CLOUD Act reporting as an additional point of clarity for the larger categories in this report. Further, the numbers listed in the columns titled No Data Disclosed include requests for which Cisco was unable to identify responsive data as well as requests for which Cisco determined the accompanying legal process to be insufficient. Cisco will report these numbers with a six-month delay. (Below is sample and intentionally left blank)

CLOUD Act Requests

<Reporting Period>	Total Requests	No Data Disclosed	Data Disclosed
Customer Data			
Non-Customer Data			
Emergencies			