Cisco Law Enforcement Guidelines for Government Data Demands

Last modified 9 December 2020

Purpose

Cisco created this document to provide guidance to government and law enforcement ("Government") regarding how and when Cisco will process Government demands for customer data in Cisco's possession ("Government Data Demands"). Cisco customers seeking to understand how Cisco protects data from unlawful Government access should review Cisco's Principled Approach to Government Demands for Data.

Position Statement

Cisco recognizes and appreciates Government efforts to thwart bad actors and deter criminal activity. While Cisco respects these efforts, it is also committed to ensuring that access to its solutions and services is free from unlawful intrusion. Therefore, Cisco requires Government to strictly adhere to applicable laws governing how and when Government may access data (e.g., obtaining a warrant, subpoena, court order, or local equivalent). Importantly, Cisco believes Government should first seek to obtain data from Cisco's customers or subscribers before demanding data from Cisco.

Frequently Asked Questions

1. Does Cisco require Government to produce a warrant, subpoena, court order, or local equivalents before sharing data with Government?

Yes, Cisco requires strict adherence to laws requiring Government to follow specific process when demanding data. For example, for US Government Data Demands, Cisco requires strict adherence to the Electronic Communications Privacy Act ("ECPA"), including the Stored Communications Act, Title II of ECPA and other applicable laws. The below table summarizes process Cisco typically will accept for US Government Data Demands for data stored on Cisco systems.

Data Category	Sufficient Process			
	Warrant	Grand Jury Subpoena or Other Court Order	Administrative Subpoena or Civil Investigative Demand	Customer Consent
Content Data	Yes	No	No	Yes
Non-Content Data	Yes	Yes	Yes[1]	Yes

2. What process does Cisco require before providing data to Governments?

Cisco must comply with US Law when responding to Governments seeking data. In some instances, this may require foreign governments to leverage Mutual Legal Assistance Treaty or other avenues authorized by law.

3. Will Cisco provide data to Governments in emergency situations?

Cisco may in its sole discretion disclose data to Government if Cisco, in good faith, believes an emergency is imminent or actively occurring, with evidence of imminent death or serious bodily harm, as permitted by applicable law.

4. How does Cisco work to prevent child exploitation on the Internet?

Cisco discloses Content and Non-Content Data to the National Center of Missing and Exploited Children after obtaining actual knowledge of any facts or circumstances that involve alleged, apparent, or imminent violations of child sexual abuse or exploitation.

5. How does Cisco comply with US Government preservation orders?

Upon receiving a valid preservation order from US Government, Cisco will retain data for 90 days pending the issuance of appropriate process, or as otherwise specified in the preservation order. After 90 days or the time period specified, Cisco will no longer preserve data unless a legally valid extension is provided by Government before the end of the prior preservation period.

[1]With a subpoena for Non-Content Data, Government is entitled by law to obtain only the following information related to the applicable subscriber or customer: (1) name, (2) address, (3) local and long distance telephone connection records, or records of session times and durations, (4) length of service (including start date) and types of services utilized, (5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (6) means and source of payment for such service (including credit card or bank account number).

6. How does Cisco comply with Non-US Government preservation orders?

Cisco evaluates each preservation order to ensure Cisco's compliance with applicable law. Governments seeking to preserve data should send preservation orders via the Cisco government data request intake process.

7. Where should Government send Government Data Demands?

Government should submit legal demands via the Cisco government data request intake process. If Government is unable to provide details via the intake process, please email your contact information to governmentdatademands@cisco.com and a Cisco team member will respond.

8. What information does Cisco need in order to determine whether data is in its possession?

Government Data Demands should contain as much specificity as possible to enable Cisco to more efficiently identify whether Cisco maintains the data requested. For example, if Government is interested in data pertaining to a customer's use of a particular Cisco product or service, Government should list the specific Cisco product or service utilized by the customer.

9. Will Cisco notify its customers or subscribers when Cisco receives a Government Data Demand?

Cisco will provide notification in conformance with its Principled Approach to Government Data Demands.

10. How long will Cisco take to deliver data to Government?

Processing times vary significantly based on the nature of the Government Data Demand. Cisco will aim to comply with orders requiring compliance within a specified time or will otherwise work with Government to ensure compliance in a timely manner.