Our Principled Approach to Government Demands for Data

At Cisco, we believe our customers own their data and have the right to control it. We are committed to protecting the privacy, integrity, and confidentiality of customer data in our possession. We believe governments, including law enforcement and national security agencies, should go directly to our customers to gain access to their data, including data about their employees and their users. We never create backdoors in our solutions to allow governments access to data, the solutions Cisco provides, or anything else.

When a government demands data directly from Cisco, we take the following steps to protect our customer interests:

- We will seek to redirect the government to the relevant customer before providing any data in Cisco's possession
- Cisco will provide data in response to a demand only if the requesting government has presented Cisco with a legally valid warrant, a court order, or a subpoena that requires us to provide the data. Where demands are not accompanied by valid legal process, Cisco will challenge or reject the request.
- Cisco will carefully review every government demand to ensure legal validity, and we will narrowly interpret demands to produce the least data necessary to comply. Cisco will challenge any government demand that raises human rights concerns. Cisco's actions will be guided by our Global Human Rights Policy.
- Cisco will notify the customer that its data has been requested prior to producing any data to government, so that the customer may attempt to limit or prevent disclosure, unless applicable law prohibits disclosure.
- Where demands that prohibit notification to the customer are excessive in duration (over one year in length), are overly broad in scope, or are unnecessary in nature, Cisco will challenge the demand to protect our customer's legitimate interests.
- Cisco will only make an exception to our customer notification commitments in emergency circumstances where disclosure will prevent imminent death or serious physical harm to an individual. Where not prohibited by applicable law, we will subsequently notify the customer if such an exception has been made. Emergency demands will be included in our Semiannual Transparency Report.
- Where compliance with a valid government demand would put Cisco in potential breach of applicable data protection and/or privacy related laws in another country that has jurisdiction or authority over the data, we will challenge the demand and invoke mutual legal assistance mechanisms, where appropriate.