Our Principled Approach to Government Requests for Data

Cisco believes that law enforcement and national security agencies should go directly to our business and government customers to obtain information or data regarding those entities, their employees, and users.

If a law enforcement or intelligence agency ("government agency", generically) requests customer data from Cisco, we will take the following steps to protect our customer's interests:

- Cisco will notify the customer that its data has been requested (so that the customer may attempt to limit or prevent disclosure), unless applicable law prohibits notification. Where appropriate and in order to protect our customer's legitimate interests, Cisco will, through appropriate legal process or other means, challenge requests that prohibit notification to the customer.
- Cisco will only provide such data if the government agency has appropriate authority under applicable law to require us to provide such data. For example, absent a valid warrant or court order, we will not provide any customer data to the U.S. government.
- Where appropriate, Cisco will seek to narrow (including moving to formally modify by judicial mandate) any government agency request or demand for customer data to only the specific information required to respond.
- Where compliance with a valid government agency request for customer data 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 customer data, Cisco will challenge such request and invoke the mutual assistance mechanisms contained in international law where appropriate.
- Cisco will only make an exception to these commitments in emergency cases where we believe disclosing customer data will prevent imminent death or serious physical harm to an individual. We will notify the customer promptly if such an exception is made, and will include that disclosure in our semiannual transparency report.