Government Requests for Cloud Customer Data
Government requests for cloud customer data

Google Cloud helps businesses and consumers be more productive. Our users benefit from the 15+ years Google has spent designing, building, and operating a highly secure infrastructure: security and trust is at the center of every decision we make. That being said, customer and user data is stored with Google and our customers and users want to know how we respond to requests from governments for access to their data. Like other technology and communication companies, Google receives requests from governments and courts around the world for such data, and this includes Google Cloud.

Google understands that this is important, and is committed to maintaining trust with both our users and customers by being transparent about how we respond to such requests. As such, in 2010, Google was the first cloud provider to publish regular transparency reports on government requests that set forth the number of government inquiries for information about users, as well as requests for Google to remove content from publication. While greater transparency helps in public policy discussions about the appropriate scope and authority of government requests, more importantly it provides a critical datapoint for use by customers in conducting a meaningful risk assessment of cloud services and their providers.

The purposes of this Whitepaper is to describe Google’s practices around government requests for data. Please note that this Whitepaper should not be considered as legal advice. If you are seeking legal advice, please consult your attorney. Google's practices are covered by the customer agreement, applicable privacy policies, and legal requirements.
What is a government data request?

Like other technology and communications companies, Google may receive requests for data from third parties, such as U.S. and foreign government agencies. The requests can be for information about the use of our services, such as the last time a user logged in, or for information about the content that is stored with Google, such as a request for a user’s email messages.

Most governments have created legal means to request data. In the U.S., the Electronic Communications Privacy Act (ECPA) regulates how a U.S. government agency can compel companies like Google to disclose information about users. ECPA sets forth the type of legal process the U.S. government must use to compel the production of different types of data, ranging from a subpoena for basic subscriber information, to a search warrant for the content of communications. ECPA places more restrictions on the U.S. government’s ability to obtain data from service providers than the laws of most other countries. More information about ECPA can be found in the legal process section of our transparency report.

As with most other countries, the U.S. also has legislation regulating the collection of data for national security investigations. With a national security letter (“NSL”), the FBI can request “the name, address, length of service, and local and long distance toll billing records” of a subscriber. That’s it. To get any other type of data, the government must seek a court order pursuant to the Foreign Intelligence Surveillance Act (“FISA”). More information on NSLs and FISA orders can be found in the FAQ section of our transparency report.

The interpretations of these laws may be quite complex — Google has a team of lawyers and trained personnel dedicated to reviewing government requests.
How Google responds to government data requests

The customer is primarily responsible for responding to law enforcement requests relating to the customer’s data; however, if Google does receive a government data request regarding a customer account, each request is reviewed using these guidelines:

➊ **Respect for the privacy and security of data you store with Google.** When we receive a request, our team reviews it to make sure it satisfies legal requirements and Google's policies. Generally speaking, for us to produce any data, the request must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law. If we believe a request is overly broad, we'll seek to narrow it. Google has a trained team dedicated to these efforts.

➋ **Customer notification.** Except in emergency situations involving a threat to life, it is our policy to notify the customer before any information is disclosed unless such notification is prohibited by law. We will provide delayed notice to users after a legal prohibition is lifted, such as when a statutory or court ordered disclosure prohibition period has expired. This notification typically goes to the G Suite and Google Cloud customers’ point of contact.

➌ **Consideration of customer objections.** Google will, to the extent allowed by law and by the terms of the request, comply with a customer's reasonable requests regarding its efforts to oppose a request, such as the customer filing an objection to the disclosure with the relevant court and providing a copy of the objection to Google.

For US government legal requests, if Google notifies the customer of the request and the customer subsequently files an objection to disclosure with the court and provides a copy of the objection to Google, Google will not provide the data in response to the request if the objection is resolved in favor of the customer. Other jurisdictions may have different procedures and are handled on a case-by-case basis.

➍ **The CLOUD Act.** The CLOUD Act clarifies the US government’s authority to obtain user data in criminal investigations where it has jurisdiction. The CLOUD Act looks at the nationality or residency of the customer rather than at the location of the data. It creates a new mechanism for cloud providers to object to U.S. government requests seeking the disclosure of stored communications of foreign customers when there is a material risk that the disclosure would violate the laws of a qualifying foreign government. To be considered as qualifying, a government must meet strict criteria and enter into an executive agreement with the U.S.
Examples of the data request process*

**Example 1:** Customer receives legal process (e.g., a court order) from a government entity. Here are the steps that a customer may choose to take in responding to the request:

1. Customer reviews legal process to determine that it satisfies legal requirements.
2. If legal process is valid, customer retrieves the information and provides it to the requesting party.

- **Yes** Customer obtains the information and provides it to the requesting entity.
- **No** Customer refuses to provide the information to the requesting party.
Example 2: Google receives legal process (e.g., a court order) from a police department in the U.S. for subscriber information concerning a G Suite or Google Cloud Platform customer. Here are the steps that Google would typically take in responding to this request:

1. Google is served legal process for customer data.

2. Is process valid under U.S. law?
   - Yes: Google notifies customer on government access request.
   - No: Google refuses to provide the information to the requesting party.

3. Customer objects in court/forum & provides copy to Google?
   - Yes: Google refuses to provide the information to the requesting party.
   - No: Google may provide the information to the requesting entity.

Google reviews legal process to determine that it satisfies legal requirements.

Unless prohibited by law, or in exceptional circumstances, Google notifies the customer of its receipt of the request.

If the customer files a timely objection with a court or other appropriate forum, and provides Google with a copy of the filing, Google will not produce the information to the police if the objection is approved by the court or appropriate forum.
Example 3: Google receives legal process (e.g., a court order) for disclosure of information about a Google Cloud customer from a government entity located outside the U.S. Here are the steps that Google would typically take in responding to this request:

1. Google will evaluate the demand to ensure that it satisfies legal requirements under the laws of the requesting government’s jurisdiction and is not contrary to U.S. law.

2. In some circumstances, if the demand is valid under the non-US law and isn’t contrary to U.S. law, Google may disclose some identifying information, such as recent login IP addresses and account registration details.

3. If the request seeks content of communications, Google will typically direct the requesting authority to pursue the data directly from the customer, or through diplomatic arrangements with the U.S.

4. The CLOUD Act allows Google, in certain circumstances, to disclose stored communications directly to qualifying foreign governments. As of the publication date of this Whitepaper, this disclosure mechanism has not been used in practice because no government has yet entered into an appropriate executive agreement with the U.S.

*Note that the examples in this section are for illustrative purposes only. Legal process may be complex and is assessed on a case-by-case basis. Resulting actions by Google, the customer, and the requesting party - in addition to variances in applicable law or the type data requested - may affect the outcome of a given scenario.*
Summary

Because Google takes the security and privacy of our customers very seriously, we take industry-leading measures to provide transparency and visibility into Google’s handling of government data requests. We were the first major cloud computing provider to disclose information about the number of these requests publicly. Google is also working with stakeholders to update U.S. and other relevant laws to provide additional privacy protections to new and emerging technologies. In this regard, we are proud of our leadership role in establishing the Digital Due Process coalition to increase online privacy protections. For more detail, please see this blog post.

Google is continually working to increase the transparency of our activities in these areas. We are proud of our track record and history of defending the privacy of our customers. With the rapid pace of innovation on the Internet and in cloud computing, Google (along with many of our colleagues in industry and academia) recognizes that legally-sound policies and a strong understanding of international governance are a prerequisite to offering cloud computing services. This is why we have discussions with governments and privacy groups about the importance of privacy and security in cloud computing.

For more information on how we protect your business’s data, please visit Google’s Business and Data Page. For more information on the security and privacy of data in Google Cloud, please visit: Google Cloud’s Trust and Security Page.
Appendix: URLs

Page 2:

1 Transparency reports:
   http://www.google.com/transparencyreport/

Page 3:

2 Legal process section of our transparency report:
   https://www.google.com/transparencyreport/userdatarequests/legalprocess/

   3 FAQ section of our transparency report:
   https://www.google.com/transparencyreport/userdatarequests/faq/

Page 8:

4 Number of transparency requests:
   http://www.google.com/transparencyreport/

6 Please see this blog post:

6 Google's Business and Data Page:
   https://privacy.google.com/businesses/

7 Google Cloud's Trust and Security Page:
   https://cloud.google.com/security/