Law Enforcement Requests Report

Law enforcement requests

Twice a year we publish the number of legal demands for customer data that we receive from law enforcement agencies around the world. While this report only covers law enforcement requests, Microsoft follows the same principles for responding to government requests for all customer data.

Requests for customer data

Government requests for customer data must comply with applicable laws. A subpoena or its local equivalent is required to request non-content data, and a warrant, court order, or its local equivalent, is required for content data.

Requests by country/region

Apply filters >

2019 (Jan-Jun) - Global

Requests

Country/Region

Asia-Pacific

- **Australia** ×
- Bangladesh
- China
- French Polynesia
- French Southern Territories
- Hong Kong
- India
- Israel
- Japan
- Malaysia
- New Zealand
- Pakistan
- Qatar
- Singapore
- South Korea
- Taiwan
- Thailand

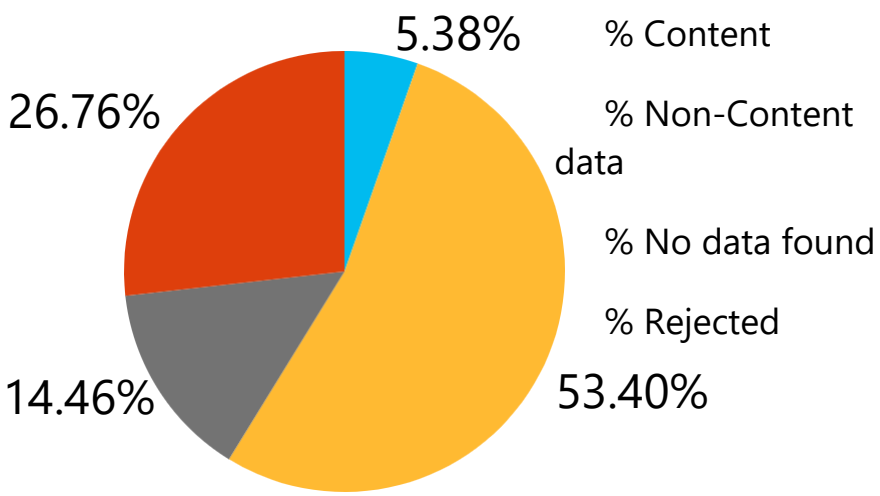
Total number of requests

24,175

Accounts/users specified in request

43,727

Disclosures



Europe

Middle East and Africa

North America

South America

Time

Period

2019 (Jan-Jun)

2018 (Jul-Dec)

2018 (Jan-Jun)

2017 (Jul-Dec)

2017 (Jan-Jun)

2016 (Jul-Dec)

2016 (Jan-Jun)

2015 (Jul-Dec)

2015 (Jan-Jun)

2014 (Jul-Dec)

2014 (Jan-Jun)

2013 (Jul-Dec)

2013 (Jan-Jun)

Apply filters >

Download report

2019 (Jan-Jun)

Download XLSX >

FAQs

The below are frequently asked questions concerning requests we receive from law enforcement agencies around the world. Additional information and FAQs related to Microsoft policies and procedures for responding to government requests for data can be found in the **Data Law blog**.

Expand all | Collapse all

What are “content” and “non-content” data?

Non-content data include basic subscriber information, such as email address, name, state, country, ZIP code, and IP address at time of registration. Other non-content data may include IP connection history, an Xbox gamertag, and credit card or other billing information. We require a valid legal demand, such as a subpoena or court order, before we will consider disclosing non-content data to law enforcement.

Content is what our customers create, communicate, and store on or through our services, such as the words in an email exchanged between friends or business colleagues or the photographs and documents stored on OneDrive or other cloud offerings such as Office 365 and Azure. We require a warrant (or its local equivalent) before we will consider disclosing content to law enforcement.

What is the process for disclosing customer information in response to government legal demands?

Microsoft requires an official, signed document issued pursuant to local law and rules. Specifically, we require a subpoena or equivalent before disclosing non-content, and only disclose content to law enforcement in response to a warrant (or its local equivalent). Microsoft's compliance team reviews government demands for customer data to ensure the requests are valid, rejects those that are not valid, and only provides the data specified in the legal order.

Where does Microsoft stand on CALEA?

The U.S. law, Communications Assistance for Law Enforcement Act, does not currently apply to many Microsoft services, including Skype, because they are not considered telecommunications services.

Does Microsoft ever challenge a law enforcement request?

As our report shows, every year we reject a number of law enforcement requests. Challenges to government requests can take many forms. In many of these cases, we simply inform the requesting government that we are unable to disclose the requested information and explain our reason for rejecting the request. We also, where it is appropriate, challenge requests in court.

If a request was rejected, can you assure your customer that their information was never disclosed?

Not necessarily. While no customer information is provided to governments in response to a rejected request, it is possible that the government later submitted a valid request for the same information.

Does Microsoft have a program to disclose information in response to imminent emergencies?

Yes, consistent with industry practice and as permitted by law, we do, in limited circumstances, disclose information to criminal law enforcement agencies where we believe the disclosure is necessary to prevent an emergency involving danger of death or serious physical injury to a person. Microsoft considers emergency requests from law enforcement agencies around the world. Those requests must be in writing on official letterhead, and signed by a law enforcement authority. The request must contain a summary of the emergency, along with an explanation of how the information sought will assist law enforcement in addressing the emergency. Each request is carefully evaluated by Microsoft's compliance team before any data is disclosed, and the disclosure is limited to the data that we believe would enable law enforcement to address the emergency. Some of the most common emergency requests involve suicide threats and kidnappings. A summary of the emergency requests received is included in the downloadable version of this report.

Does Microsoft provide customer data in response to demands from civil litigation parties?

Microsoft receives legal demands for customer data from civil litigation parties around the world. Microsoft does not respond to private requests other than those received through a valid legal process. Microsoft adheres to the same principles for all civil proceeding legal requests as it does for government agency requests for user data, requiring nongovernmental civil litigants to follow the applicable laws, rules, and procedures for requesting customer data.

If a nongovernmental party wants customer data, it needs to follow applicable legal process–meaning, it must serve us with a valid subpoena or court order for content or subscriber information or other non-content data. For content requests, we require specific lawful consent of the account owner and for all requests we provide notice to the account owner unless prohibited by law from doing so. We require that any requests be targeted at specific accounts and identifiers. The Microsoft compliance team reviews civil proceeding legal requests for user data to ensure the requests are valid, rejects those that are not valid, and only provides the data specified in the legal order. A summary of the Microsoft team's responses to civil litigation requests for customer data is included in the downloadable version of this report.

Does Microsoft notify customers when civil proceeding litigants request their data and does Microsoft ever challenge nondisclosure obligations?

Yes. Except where prohibited by law, Microsoft will give prior notice to customers whose data is sought by a civil proceeding litigant. Microsoft sometimes receives civil proceeding legal demands that prohibit us from notifying our customer. In some cases, we request permission to notify our customer or even challenge the nondisclosure order. In some cases, Microsoft has persuaded the requesting party that its interests in the underlying litigation will not be prejudiced by Microsoft providing notice.

Does the data include any legal demands that may have been issued pursuant to U.S. national security orders (e.g., FISA Orders and FISA Directives)?

No. This report covers requests from law enforcement agencies—usually local or national police departments investigating a range of criminal activity. The aggregate number of requests we receive under U.S. national security laws, such as the Foreign Intelligence Surveillance Act (FISA), are published **in the U.S. National Security Orders Reports online summary**.

How many Microsoft customers were impacted by law enforcement requests?

Fewer customers are impacted than the number of accounts impacted, but for a variety of reasons, it is difficult to determine an exact number. For example, a single request may seek information about multiple accounts belonging to one user, or the same accounts may also be subject to repeat orders in different time frames and, as a result, be "double counted."

How many enterprise cloud customers are impacted by law enforcement requests?

In the first half of 2019, Microsoft received 74 requests from law enforcement around the world for accounts associated with enterprise cloud customers. In 32 cases, these requests were rejected, withdrawn, no data, or law enforcement was successfully redirected to the customer. In 42 cases, Microsoft was compelled to provide responsive information: 22 of these cases required the disclosure of some customer content and in 20 of the cases we were

compelled to disclose non-content information only. Of the 22 instances that required disclosure of content data, 15 of those requests were associated with U.S. law enforcement.

Does Microsoft disclose additional data as a result of the CLOUD Act?

No. The CLOUD Act amends U.S. law to make clear that law enforcement may compel U.S.-based service providers to disclose data that is in their "possession, custody, or control" regardless of where the data is located. This law, however, does not change any of the legal and privacy protections that previously applied to law enforcement requests for data – and those protections continue to apply. Microsoft adheres to the same principles and customer commitments related to government demands for user data.

In the first half of 2019, Microsoft received 4,860 legal demands for **consumer** data from law enforcement in the United States. Of those, 126 warrants sought content data which was stored outside of the United States.

In the same time frame, Microsoft received 43 legal demands from law enforcement in the United States for **commercial** enterprise customers who purchased more than 50 seats. Of those demands, 1 warrant resulted in disclosure of content data related to a non-US enterprise customer whose data was stored outside of the United States.

What is the difference between a consumer and an enterprise customer?

A consumer service is generally one subscribed to and used by an individual in his or her personal capacity. Some examples include Hotmail/Outlook.com, OneDrive, Xbox Live and Skype. For purposes of this report, "enterprise customer" generally includes those organizations or entities (commercial, government or educational) that purchase more than 50 "seats" for one of our commercial cloud offerings, such as Office 365, Azure, Exchange Online and CRM Online. Those organizations, in turn, may provide services, such as email, to individual employees, students or others.

What should Microsoft customers take away from this data disclosure?

The Microsoft mission is to empower every person and every organization on the planet to achieve more, and all of our technologies are designed to further that mission. We place a premium on respecting and protecting the privacy of our customers, and work to earn their trust every day. At the same time, Microsoft recognizes that law enforcement plays a critically important role in keeping our customers—and our technology—safe and free from abuse or exploitation. We are hopeful that this data disclosure can better inform all sides in the critically important public discussion about how best to strike the balance between the privacy of our customers and the legitimate needs of law enforcement agencies that protect and serve their citizens.

Do you enable third parties to assist governments in conducting voluntary surveillance of your customers?

We are aware of reports that some providers have developed tools that third parties use to voluntarily assist governments in conducting surveillance of that provider's customers. We do not design tools to enable voluntary surveillance of our customers. If we ever provide third parties with access to data about our customers, we expect those third parties to handle that data appropriately, meaning that they should not assist governments in voluntary, widespread surveillance of customers. Instead, these third parties should ensure that they only disclose personal data about customers in compliance with applicable law or in response to valid legal orders.

Does Microsoft provide governments with direct access to customer data?

We believe that you should control your own data. Microsoft does not give any government (including law enforcement, or other government entities) direct or unfettered access to customer data.

Do you give governments access to platform encryption keys?

We do not provide any government with our encryption keys or the ability to break our encryption.