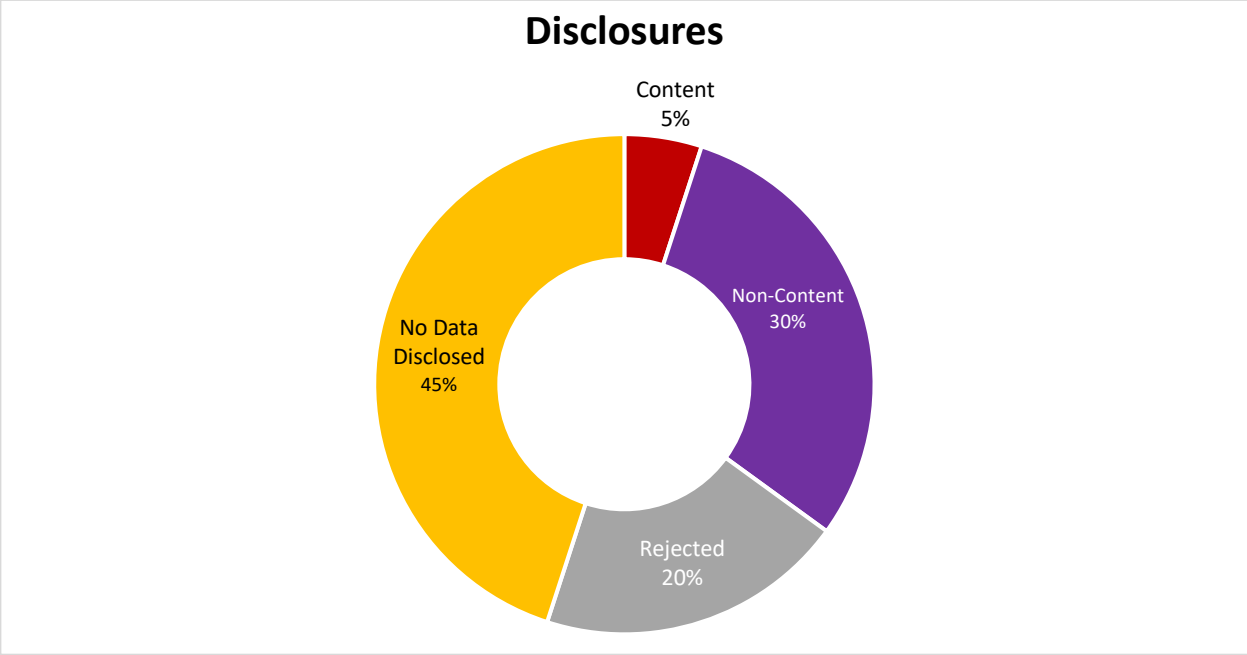
RACKSPACE TECHNOLOGY LAW ENFORCEMENT REQUESTS

This annual report provides additional information on the volume and types of law enforcement requests that Rackspace Technology processed between January 1, 2021 through December 31, 2021.

Types of Information Requests Received by Rackspace

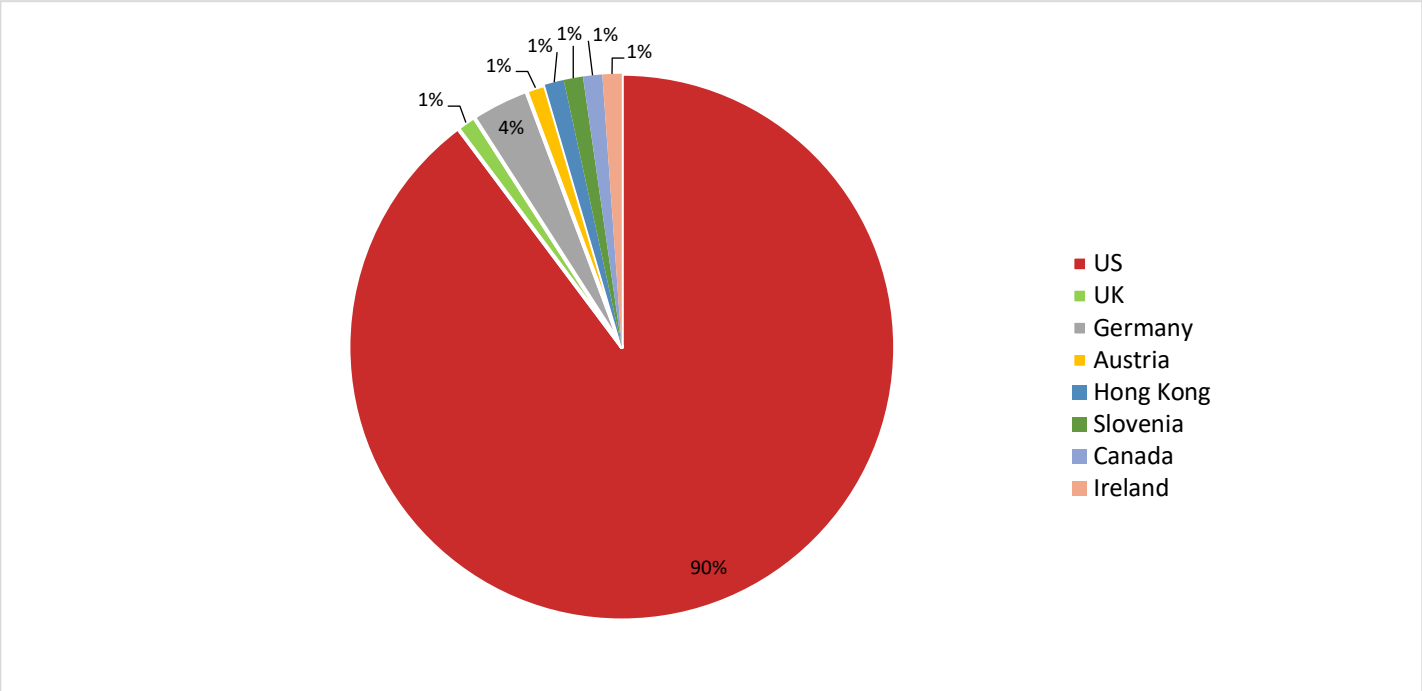
- *Non-content* – Non-content information means subscriber information such as name, address, phone number, length of service and billing information. We require a valid legal demand, such as a subpoena or court order, before we will consider disclosing non-content data to law enforcement.

- *Content* – Content information means the data and/or files that a customer transfers for processing, storage, or hosting in connection with the Rackspace Technology services and any computational results. Rackspace Technology requires a warrant (or its local equivalent) before it will consider disclosing content to law enforcement.

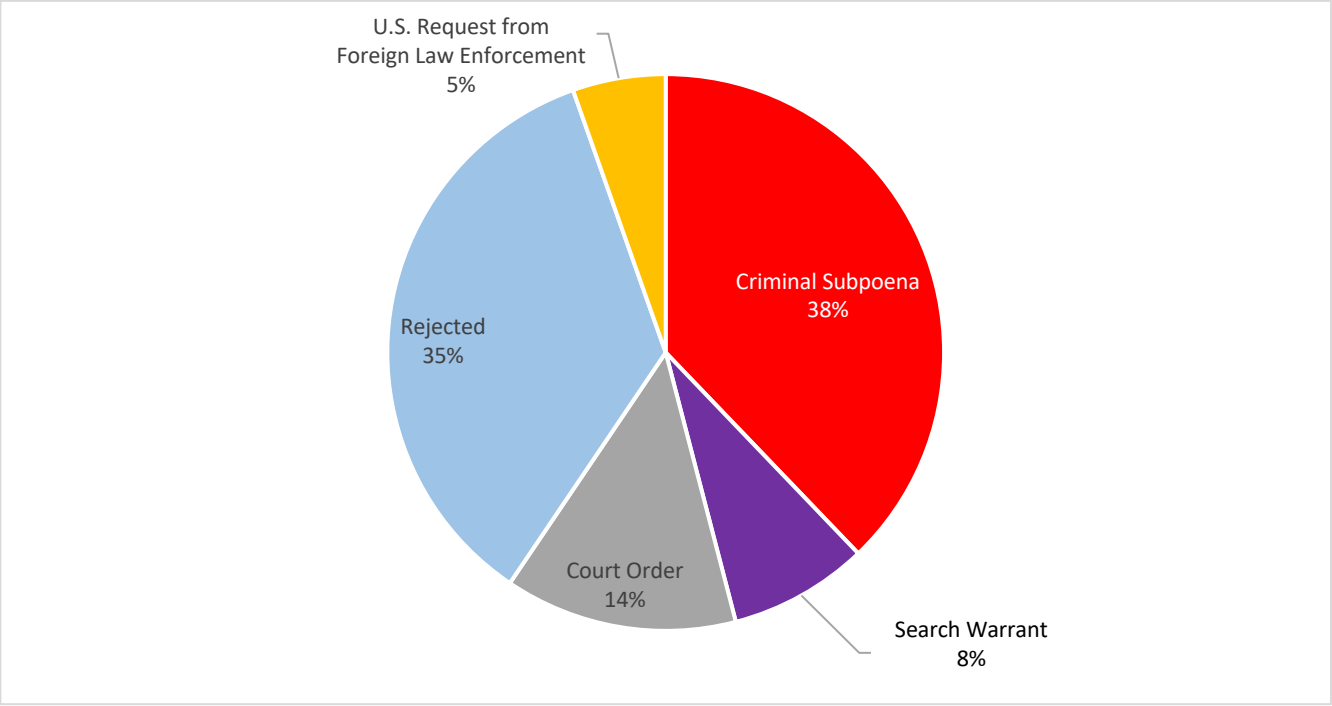


During the applicable reporting period, Rackspace Technology received a total of approximately **88** law enforcement requests.

GLOBAL REQUESTS



TYPES OF REQUESTS RECEIVED IN U.S.



Criminal Subpoenas - Subpoenas are valid and binding legal demands for information or testimony issued by courts, lawyers, law enforcement agencies, or grand juries, usually without any substantive review by a judge or magistrate. We produce *non-content* information only in response to valid and binding subpoenas. We do not produce content information in response to subpoenas.

Search warrants - Search warrants may be issued by local, state, or federal courts upon a showing of probable cause and must specifically identify the place to be searched and the items to be seized. We may produce *non-content* and *content* information in response to valid and binding search warrants.

Court Orders - Court orders refer to valid and binding orders issued by local, state, or federal courts, other than search warrants or court-issued subpoenas. This includes *non-content* information such as access logs.

National Security Requests – National security requests include National Security Letters ("NSLs") and court orders issued under the Foreign Intelligence Surveillance Act ("FISA"). Our responses to these requests depend on the nature of the request. Rackspace is prohibited by law from reporting the exact number of NSLs and FISA orders it receives. Therefore, we report the numbers of such requests only within certain ranges set by the government.

Non-U.S. requests. Non-U.S. requests include legal demands from non-U.S. governments, including legal orders issued pursuant to the Mutual Legal Assistance Treaty process, or the CLOUD Act. Our responses to these requests depend on the nature of the request.

Civil Subpoenas – Rackspace notifies its customer of any civil subpoena, and we object under the Stored Communications Act to any request for customer content.

FAQS

1) **Does the CLOUD Act change how Rackspace Technology responds to requests?**

No. The CLOUD Act amended the Stored Communications Act to clarify that the U.S. government may seek to require service providers located in the U.S. to disclose data that is in their "possession, custody, or control" regardless of whether the data is located within or outside the United States. The CLOUD Act does not change any of the legal and privacy protections that apply to law enforcement requests for data. Rackspace Technology continues to object to overbroad or otherwise inappropriate requests as a matter of course regardless of where the data is located.

2) **During the reporting period, how many U.S. law enforcement requests resulted in disclosure of content data located outside of the U.S.?**

None. Rackspace Technology received no requests during the reporting period by U.S. law enforcement for content data located outside of the U.S.

3) **Does Rackspace Technology provide customer data in response to demands from civil litigation parties?**

Rackspace Technology receives legal demands for customer data from civil litigation parties around the world. Rackspace Technology does not respond to private requests other than those received through a valid legal process. Rackspace Technology 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 Rackspace Technology with a valid subpoena or court order for content or subscriber information or other non-content data. For content requests, Rackspace Technology requires specific lawful consent of the account owner and for all requests, the company provides notice to the account owner unless prohibited by law from doing so. Rackspace Technology requires that any requests be targeted at specific accounts and identifiers. The Rackspace Technology 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 compliance team's responses to civil litigation requests for customer data is included in this report.

4) **Does Rackspace Technology provide governments with direct access to customer data?**

Rackspace Technology believes that its customers should control their own data. Rackspace Technology does not give any government (including law enforcement or other government entities) direct or unfettered access to customer data.