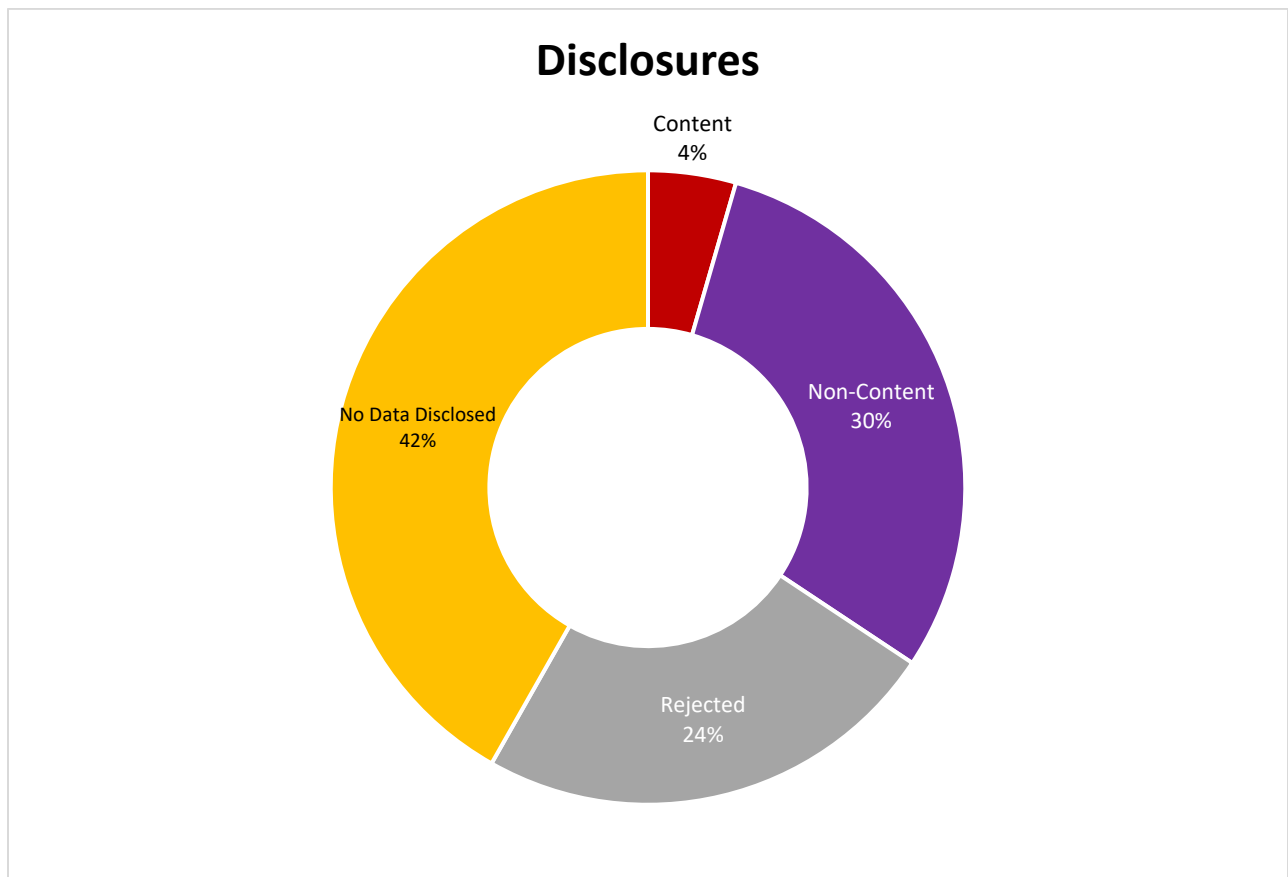


# RACKSPACE TECHNOLOGY LAW ENFORCEMENT REQUESTS

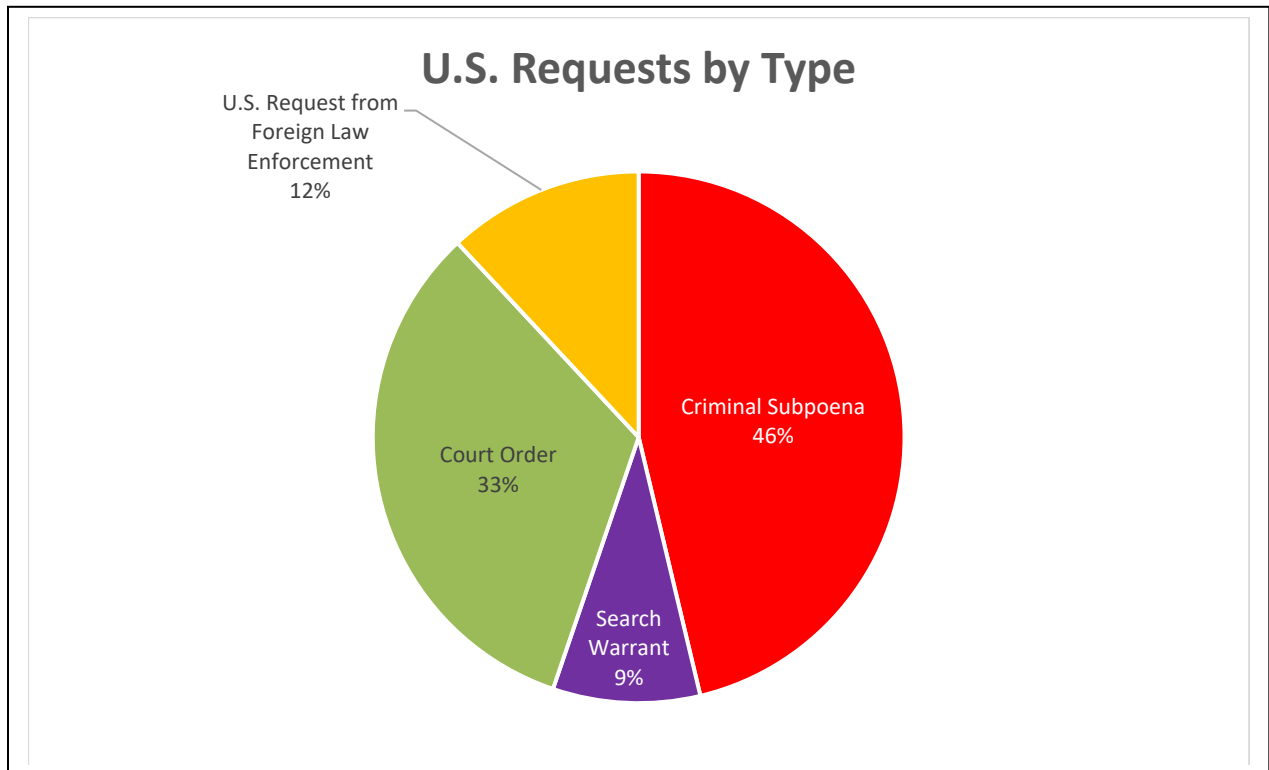
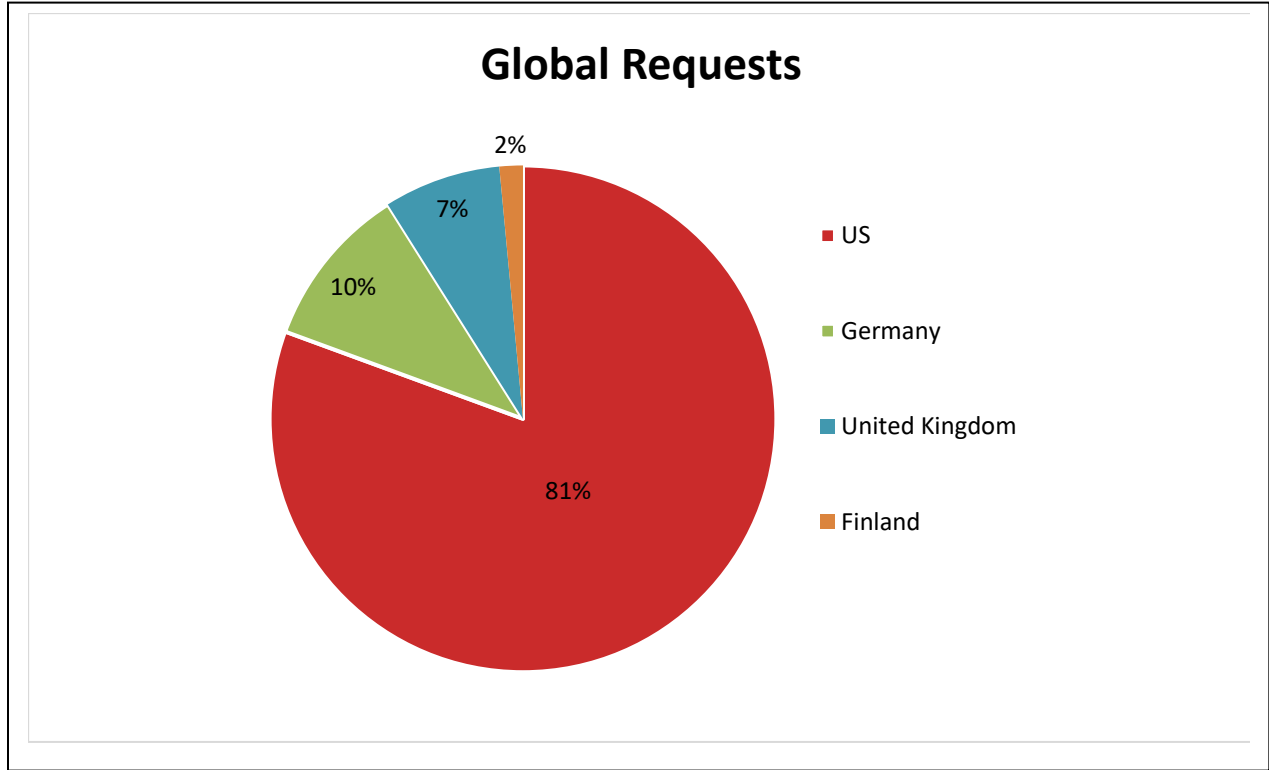
This annual report provides additional information on the volume and types of Law Enforcement Requests that Rackspace Technology processed between January 1, 2023 through December 31, 2023.

## 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 **67** law enforcement requests.



**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. Rackspace Technology produces *non-content* information only in response to valid and binding subpoenas. Rackspace Technology does 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. Rackspace Technology 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”). Rackspace Technology 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. This information is not included in the data presented above.

**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. Rackspace Technology’s responses to these requests depend on the nature of the request.

## **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 law enforcement may compel service providers located in the U.S. to disclose data that is in their “possession, custody, or control” no matter where that data is located. The CLOUD Act does not change the legal and privacy protections that previously applied to law enforcement requests for data. These protections still apply. 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 occasionally receives legal demands for customer data from civil litigation parties. 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. In addition, Rackspace Technology will notify the customer prior to disclosing the requested data unless otherwise prohibited by law.

**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.