2016 Transparency Report

DigitalOcean takes the trust our users place in us very seriously. Our customers expect us to safe-guard their data as if it were our own, and they expect us to communicate openly if we might be compelled to share their data with a third party.

This transparency report highlights instances when DigitalOcean has been required to release customer data in response to lawful government requests. Given our hundreds of thousands of customers, these numbers remain relatively small. Each instance matters, and great care has been taken to ensure we comply with the law, while at the same time protecting user data and responding to requests as narrowly as possible.

The table below summarizes the variety of requests we receive and what data, if any, we disclosed in response. This report is for any request received between January 1, 2016 through December 31, 2016. We will continue publishing these reports annually.

	Request still in process	No Data Found	Rejected / No Information Provided	Only NCD disclosed	Content Disclosed	Total
Subpoena	9	0	55	111	N/A	**175**
ECPA Court Order	0	0	3	18	N/A	**21**
Search Warrant	0	0	0	8	4	**12**
PRTT	0	0	0	5	N/A	**5**
Wiretap	0	0	0	N/A	0	**0**
Imminent Harm	0	0	2	0	0	**2**
International	0	0	25	N/A	N/A	**25**
NSL/FISA	0-249	0-249	0-249	0-249	0-249	
					Total	**240**

Definitions

Request still in process	Request has been received by DigitalOcean but is awaiting further processing or for a response from law enforcement.
No Data Found	The user account information either doesn't exist or has been deleted.
Rejected / No Information Provided	"Rejected / No information provided" could result from: 1) The request was duplicative of a request we already responded to 2) DO objected to the request 3) Law enforcement withdrew the request 4) The request failed to include enough information 5) The request expired
Only NCD disclosed	"Non-content data" such as basic subscriber information, including the information captured at the time of registration such as an alternate email address, name, IP address, login details, billing information, and other transactional information.
Content Disclosed	Data that our users generate, including copies of Droplets, files on backup, or words in emails to customer support.
Subpoena	This category includes any legal process which does not have ex ante judicial review, including but not limited to grand jury subpoenas, US government attorney-issued subpoenas, and case agent issued subpoenas.
ECPA Court Order	Unlike a subpoena, a court order requires judicial review to validate that the requested information is relevant and material to an ongoing criminal investigation. Court Orders can obtain the same information as a subpoena, plus more detail about account usage like the IP address of logins or dates and times of account information changes.
Search Warrant	Search warrants require a still higher threshold before judicial approval. A government agency must demonstrate probable cause and include the location to be searched and detail of items requested. With a search warrant, a law enforcement agency might obtain a copy of a user's droplet.

PRTT	Pen Register and Trap and Trace (PRTT) gather non-content information from packet headers such as connection logs or IP addresses and times.
Wiretap	Wiretap orders seek to gather user information in real-time, hoping to capture future data that does not yet exist. These have the highest threshold of any kind of order, requiring the requesting agency to demonstrate that someone is committing a crime listed in the wiretap act, that the wiretap will collect information about that crime, and that the crime involves the DigitalOcean account that will be tapped.
Imminent Harm	As permitted by US law, we may disclose user information to the government or law enforcement, without a subpoena or warrant if we have a good faith belief that an emergency (danger of death or serious physical injury) requires disclosure of information related to the emergency without delay.
NSL/FISA	What we can say in regard to national security orders is highly regulated. The Department of Justice now allows companies to disclose the number of NSLs and FISA orders as a single number in bands of 250, starting with 0-249.
International	For legal requests from government agencies/law enforcement outside of the United States, we require that the request be served via a United States court or enforcement agency under the procedures of an applicable mutual legal assistance treaty (MLAT). The resultant requests are tallied as court orders or search warrants above. All other requests categorized as "International" in the table above were received directly from foreign goverment or law enforcement officials, and did not go through the MLAT process.
N/A	Not applicable. Specific criteria need to be met in order to provide subscriber or content data to government and law enforcement officials. If the type of request in a given row does not meet the strict requirements necessary to provide the data, it is not applicable. For example, a subpoena will never meet the criteria for disclosing content data. We will therefore never comply with requests asking for this type of information.