DigitalOcean is committed to providing cloud services for everyone to build, grow, and expand their ideas. We believe that fostering a community based on a foundation of trust is a core value of our services. We take our responsibility of being trusted data stewards very seriously.

Like many cloud computing companies, DigitalOcean occasionally receives requests from law enforcement regarding one of the numerous servers hosted on our platform. Because we have data centers and customers around the world, these requests come from various different governments. DigitalOcean's policy is to comply with the valid legal process that we receive from these governments when it applies to us. However, we stand with our customers and prioritize the privacy and confidentiality of their identities and data.

This means we check the validity of legal requests and push back when needed to protect the rights of our customers. We also inform users about requests for their data unless we are legally prevented from doing so. Even when we do feel that disclosing information is the required outcome, we are careful to limit disclosure to protect the rights of our customers as much as possible.

Finally, we publish this report on an annual basis so that customers better understand the landscape that we face in complying with these requests, as well as underscore our commitment to being responsible providers of the Internet to our global community.

This report is for any government or law enforcement request for customer data received between January 1, 2019 through December 31, 2019. We will continue to publish these reports annually.

During this period, we received a total of 558 requests for customer data from U.S. law enforcement agencies. This is a decrease from the 563 requests we processed in 2018, and marks the first decrease in requests from law enforcement since we published our first report in 2014.

We specifically want to call attention to the increase in requests from non-U.S. governments. Although DigitalOcean is a U.S. company, we have data centers in several other countries. In 2019, we began receiving more legal demands in countries where we have data center assets and have taken steps to create new processes for servicing requests. Because of this and our ever-growing business, we expect to continue to see an increase in the number of international requests.

2019 - US	Request Still in Process	No Data Found	No Information Provided	Only NCD Disclosed	Content Disclosed	Total
Subpoena	4	23	127	243	N/A	397
Court Order	0	1	0	11	1	13

Search Warrant	4	2	10	24	10	50
PRTT	0	6	3	19	N/A	28
Wiretap	1	0	0	N/A	0	1
Imminent Harm	0	1	24	44	0	69
NSL/FISA	0-249	0-249	0-249	0-249	0-249	
					Total	558
2019 - US	Complied	Did Not Comply	Total			
Preservation	103	14	117			

2019 - International	Request Still in Process	No Data Found	No Information Provided	Only NCD Disclosed	Content Disclosed	Total
Subpoena	0	0	195	3	N/A	198
Court Order	1	0	0	3	9	13
PRTT	1	0	0	1	N/A	2
Wiretap	0	0	0	N/A	0	0
Imminent Harm	0	1	4	6	0	11
					Total	224
2019 - International	Complied	Did Not Comply	Total			
Preservation	8	1	9			

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.
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 or instructed use of MLAT 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, government attorney-issued subpoenas, and case agent issued subpoenas.
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 network activity and, in some jurisdictions, information stored in a user's Droplet.
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.
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.
Preservation	A request to copy and securely store subscriber and/or content data in anticipation of future legal process. Preservation requests are not demands for the production of user information, and we do not provide

user information in response to preservation requests.