



## **AnchorFree Transparency Report**

November 29, 2017

AnchorFree is committed to providing users with a private and secure web browsing environment. We are also committed to transparency regarding what information we share with governments and law enforcement agencies regarding our users' use of our services.

AnchorFree is regularly contacted by law enforcement in the United States and in other countries regarding our services. In the vast majority of these cases, we receive requests to identify a particular user based on an IP address that is registered to AnchorFree. We also receive requests regarding what kind of information we store regarding our users.

Because we do not collect information that allows us to trace Internet usage on Hotspot Shield back to individual users, we do not and cannot provide information to governments about what websites our users visit when using our services. Additionally, we cannot identify an individual user based on a public-facing IP address that law enforcement agencies provide to us. To date, AnchorFree has never provided the identity or other personal information regarding our users to the government. We cannot do so based on public-facing IP addresses regardless of the type of process the government uses—whether a search warrant, a subpoena, a court order, or other request. (See “Definitions” below regarding types of lawful processes a government might issue.)

AnchorFree has no desire to allow its products to be used for criminal purposes. In some instances, at the request of law enforcement, AnchorFree has blocked access to certain domains. AnchorFree strives to be a good corporate citizen, while ensuring the privacy, security, and freedom of our users.

For further transparency, AnchorFree is committed to releasing an annual report regarding the types of requests for information we receive from government agencies as well as the geographic location of those requests. For this inaugural report, we are releasing data from 2016 as well as from the first ten months of 2017. Going forward, we will release the data on an annual basis for the prior calendar year.

**Total User Data Requests in 2017 (as of Oct 31, 2017) – 81**

**Amount of User Data Produced in 2017 – NONE**

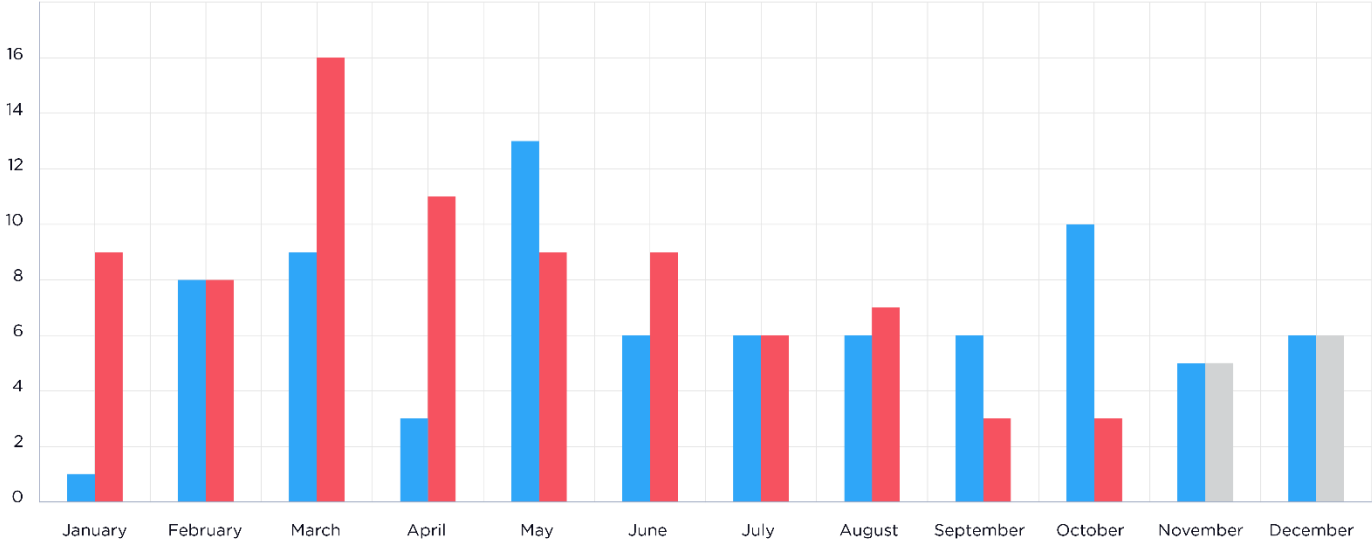
**Total User Data Requests in 2016 – 79**

**Amount of User Data Produced in 2016 – NONE**

**Monthly Breakdown of Requests in 2016 and 2017**

# Total Requests By Month

2016 2017 N/A



Total requests by month	2017	2016
January	9	1
February	8	8
March	16	9
April	11	3
May	9	13
June	9	6
July	6	6
August	7	6
September	3	6
October	3	10
November	N/A	5
December	N/A	6
<b>TOTAL</b>	<b>81</b>	<b>79</b>

## 2017 Requests from Governments (January 1 – October 31, 2017)

### Requests by country

Country	Number of Requests	Amount of User Data Released
U.S.	62	NONE
Canada	1	NONE
Brazil	1	NONE
France	7	NONE
Germany	3	NONE
India	2	NONE
U.K.	2	NONE
Switzerland	1	NONE
Czech Republic	1	NONE
Spain	1	NONE
<b>Total</b>	<b>81</b>	<b>NONE</b>

### Requests by Type

Type of Process	Number received	Percentage of User Data Released
Search Warrant	4	NONE
Court Order	1	NONE
Subpoena	38	NONE
Other*	38	NONE

## 2016 Requests from Governments

### Requests by country

Country	Number of Requests	Amount of User Data Released
Austria	1	NONE
Canada	3	NONE
France	6	NONE
Germany	2	NONE
India	2	NONE
Netherlands	1	NONE
Switzerland	1	NONE
U.K.	4	NONE
U.S.	59	NONE
<b>Total</b>	<b>79</b>	<b>NONE</b>

## Requests by Type

Type of Process	Number received	Percentage of User Data Released
Search Warrant	6	NONE
Court Order	2	NONE
Subpoena	29	NONE
Other*	42	NONE

\* Other requests include, but are not limited to, email inquiries, requisitions, requests forms, demands, official letters and other types of process.

## Definitions

Under United States federal law – the Electronic Communications Protection Act (ECPA) – the government cannot force AnchorFree to provide data on its users without serving AnchorFree with legal process. Foreign governments also have to seek U.S. legal process to obtain information from AnchorFree about its users, which they can do using Mutual Legal Assistance Treaties (MLATs) those countries may have with the United States.

ECPA permits the government to use three separate types of legal process to obtain information about our users. **Subpoena.** A subpoena is a form of legal process that a government agency, which has been granted authority to issue subpoenas, can use to request limited types of information about AnchorFree’s customers. AnchorFree most commonly receives grand jury subpoenas, although there are other types of subpoenas. Under the statute, a governmental entity may seek a customer’s name, address, the types of services the customer uses and how long the customer has been using a service, telephone number, and means and source of payment for such service. As noted above, because AnchorFree does not associate this information with public facing IP addresses, it has not provided any information about our customers to any government.

**Court Order.** ECPA allows the government to seek more information about a user than the government could get with a subpoena *if* the government seeks a court order for such information. The government, however, cannot seek “contents” of communications using only a court order. Court orders are issued by judges or magistrates. In order to receive such an order, the government must “offer[] specific and articulable facts showing that there are reasonable grounds to believe that. . . the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 USC § 2703(d). As noted above, because AnchorFree does not associate any records with public facing IP addresses, it has not provided any information about our customers to any government.

**Search Warrant.** A search warrant is a process under the United States Constitution that allows the government to seek a wide-range of information, including contents of communications. For AnchorFree, contents of communications would theoretically include the web addresses and contents of pages visited using AnchorFree’s products. A search warrant can only be issued by a judge or magistrate, and the government must provide an oath or affidavit articulating specific facts that demonstrate “probable cause” that the place to be searched (generally, AnchorFree’s servers) would produce evidence of criminal activity or contraband. As noted above, AnchorFree cannot execute search warrants for information about individual users based on a public-facing IP address, and therefore does not produce any information even when served with a search warrant.

**Other.** AnchorFree receives many requests for information from governments that do not fall into the above three categories. For example, we often receive requisitions, requests forms, demands, and official letters from foreign governments. As noted above, these types of processes are not recognized under U.S. law, and the foreign government would have to seek U.S. lawful process using an MLAT in order to lawfully request information from AnchorFree. Nevertheless, we inform these governments that we would not be able to produce data on our users even if they were to seek lawful process using an MLAT. Additionally, AnchorFree often receives other informal types of outreach, such as phone calls and emails, where government officials request either information about a specific user or information about what types of information we could provide about users. With these types of requests, we inform the government that, even if they provided a formal request for data, we cannot produce any information about users based on public-facing IP addresses. We keep records of these informal requests and disclose them as part of our annual transparency report.