CLOUDFLARE

Transparency Report

An essential part of earning and maintaining the trust of our customers is being transparent about the requests we receive from law enforcement and other governmental entities. To this end, Cloudflare publishes semi-annual updates to our Transparency Report on the requests we have received to disclose information about our customers.

Respect Privacy

It is Cloudflare's overriding privacy principle that any personal information you provide to us is just that: personal and private. We will not sell, rent, or give away any of your personal information without your consent. Our respect for our customers' privacy applies with equal force to commercial requests and to government or law enforcement requests.

Require Due Process

Any law enforcement requests that we receive must strictly adhere to the due process of law and be subject to judicial oversight. It is not Cloudflare's intent to make law enforcement's job any harder, or easier.

Provide Notice

It is our policy to notify our customers of a subpoena or other legal process requesting their customer or billing information before disclosure of information, whether that legal process comes from the government or private parties involved in civil litigation, unless legally prohibited.

Some things we have never done

- **Cloudflare has never turned over our encryption or authentication keys or our customers' encryption or authentication keys to anyone.**
- **Cloudflare has never installed any law enforcement software or equipment anywhere on our network.**
- **Cloudflare has never terminated a customer or taken down content due to political pressure.***
- **Cloudflare has never provided any law enforcement organization a feed of our customers' content transiting our network.**
- **Cloudflare has never modified customer content at the request of law enforcement or another third party.**
- **Cloudflare has never modified the intended destination of DNS responses at the request of law enforcement or another third party.**
- **Cloudflare has never weakened, compromised, or subverted any of its encryption at the request of law enforcement or another third party.**

If Cloudflare were asked to do any of the above, we would exhaust all legal remedies, in order to protect our customers from what we believe are illegal or unconstitutional requests.

Background on Requests for User Data

Cloudflare receives requests for different kinds of data on its users from US and foreign governments, courts and those involved in civil litigation. To provide additional transparency about the type of information Cloudflare might provide, we have broken down the types of requests we receive, as well as the legal process we require before providing particular types of information. We review every request for legal sufficiency before responding with data.

Requests for basic subscriber data

The most frequent requests Cloudflare receives are requests for information that might be used to identify a Cloudflare customer. This basic subscriber data would include the information our customers provide at the time they sign up for our service, like name, email address, physical address, phone number; the means or source of payment of service; and non-content information about a customer's account, such as data about login times and IP addresses used to login to the account. Unless there is an emergency, Cloudflare requires valid legal process such as subpoena or a foreign government equivalent of a subpoena before providing this type of information to either foreign or domestic law enforcement or civil litigants.

U.S. Government

Under the Electronic Communications Privacy Act (ECPA), the U.S. government can compel disclosure of subscriber information with a subpoena, a type of legal process that does not require prior judicial review. Although Cloudflare typically requires a subpoena before providing subscriber information, consistent with ECPA, Cloudflare may disclose information without delay to law enforcement if the request involves imminent danger of death or serious injury to any person. Cloudflare will evaluate emergency disclosure requests on a case-by-case basis as we receive them. For emergency disclosure requests, we request that law enforcement obtain legal process when time permits.

Beyond subpoenas issued under ECPA, some U.S. government agencies may issue administrative subpoenas for subscriber data. Cloudflare has received a number of such subpoenas from the Securities and Exchange Commission (SEC).

National security process

The U.S. government can also issue a variety of different types of national security requests for data. Under the Foreign Intelligence Surveillance Act (FISA), the U.S. government may apply for court orders from the FISA Court to, among other actions, require U.S. companies to hand over users' personal information. The U.S. government can also issue National Security Letters (NSLs), which are similar to subpoenas, for subscriber and non-content data. Both FISA court orders and NSLs typically come with a non-disclosure obligation.

Cloudflare has long had concerns about these types of non-disclosure obligations. In 2013, after receiving such an NSL, Cloudflare objected to an administratively imposed gag which prohibited Cloudflare from disclosing information about this NSL to anyone other than our attorneys and a limited number of our staff, under threat of criminal liability. Cloudflare provided no customer information subject to NSL-12-358696; but the NSL's nondisclosure provisions remained in effect for nearly four years, until December 2016, after which Cloudflare disclosed receipt of the NSL, along with a redacted copy of the NSL.

Governments outside the United States

Cloudflare responds to requests from governments outside the United States for all types of information, including subscriber data, that are issued through a U.S. court by way of diplomatic process like a mutual legal assistance treaty (MLAT) request. The information produced to governments outside the United States in response to these requests is the same as would be produced to the U.S. government in response to a similar U.S. court order.

Cloudflare evaluates on a case-by-case basis requests for subscriber information from governments outside the United States that do not come through the U.S. court system. Cloudflare may, in our discretion, provide subscriber data to in response to a local equivalent of a subpoena, provided that the request complies with local law, and is consistent with international norms and Cloudflare policies.

In March 2018, the United States passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which permits the U.S. government to enter into Executive Agreements with other governments to allow direct law enforcement access for both governments to data stored in the other country to investigate and prosecute certain crimes. The law permits countries that enter into such Agreements with the United States to seek content data from U.S. companies directly, using that country's legal process, rather than requiring the country's law enforcement agencies to work with U.S. law enforcement to get U.S. legal process such as a court order.

Given the difficult questions of national sovereignty, privacy, and conflict of laws that are raised by cross-border access to data, Cloudflare supports modernizing the rules and international frameworks regarding law enforcement access to data, as long as the new rules provide sufficient procedural safeguards to protect privacy. As these Executive Agreements move forward, we will have more opportunity to assess whether they provide adequate "protections for privacy and civil liberties" as required by the CLOUD Act.

Cloudflare believes that government access to data must be consistent with principles of rule of law and due process, including prior independent judicial review of requests for content; that users are entitled to notice when the government accesses their data; and that companies must have procedural mechanisms to raise legal challenges to access requests. Whether inside or outside the United States, we will fight law enforcement requests that we believe are overbroad, illegal, or wrongly issued, or that unnecessarily restrict our ability to be transparent with our users.

Civil process

Cloudflare responds to legal process requesting subscriber data from civil litigants, such as subpoenas issued pursuant to the Digital Millennium Copyright Act (DMCA) seeking information on users alleged to be infringing copyright.

Requests for other non-content data

Beyond requests for the types of subscriber data described above, Cloudflare sometimes receives court orders for transactional data related to a customer's account or a customer's website, such as logs of the IP addresses visiting a customer's website or the dates and times a customer may have contacted support. Because Cloudflare retains such data for only a limited period of time, Cloudflare rarely has responsive data to provide to such requests.

Court Orders

Court orders are requests for data issued by a judge or magistrate. With a court order, Cloudflare may provide both the basic subscriber information that might be provided in response to a subpoena and other non-content information.

Pen Register Trap and Trace

Cloudflare periodically receives pen register/trap and trace orders, issued by a court, seeking real-time disclosure of non-content information, such the IP addresses of visitors to an account or website. We provide limited forward looking data in response to those requests.

Requests for content data

Cloudflare is not a hosting provider or an email service provider and does not have customer content -- like email or other types of customer-generated material -- in the traditional sense. In the rare instances where law enforcement has sought content such as abuse complaints or support communications, Cloudflare has insisted on a search warrant for those electronic communications, consistent with the principles laid out in U.S. v. Warshak. To date, we have received no such warrants.

Search warrants

Search warrants require judicial review, a finding of probable cause, inclusion of a location to be searched, and a detail of items requested. Although we have received a number of search warrants, as noted above, we have not had customer content to provide in response to those warrants.

Wiretap

A wiretap order is a court order that requires a company to turn over the content of communications in real time. Law enforcement must comply with very detailed legal requirements to obtain such an order. Cloudflare has never received such a wiretap order.

National security process

The U.S. government may apply for court orders from the FISA Court to require U.S. companies to turn over the content of users' communications to the government. Because the public reporting of all national security process is highly regulated, Cloudflare's receipt of such an order would be reported as part of a combined number of NSLs and content and non-content FISA orders, in a band of 250, beginning with 0-250.

Background on Requests for Content Removal or Blocking

Cloudflare runs a global network that provides security and performance enhancements for Internet-facing websites and applications around the world. Because Cloudflare's infrastructure sits between our customers' websites and Internet users in order to protect those websites from direct attack and serve requests to and from those servers, Cloudflare's nameservers may appear in WHOIS data and Cloudflare's IP addresses may appear in the DNS records for websites using our service.

As the point of contact listed on relevant records, Cloudflare receives requests to remove content from our network from copyright holders alleging infringement or from governments taking the position that the content is unlawful. As Cloudflare cannot remove material from the Internet that is hosted by others, we generally forward requests for removal of content to the website hosting provider, who has access to the website content and the ability to address the underlying concern.

A small but growing number of Cloudflare's products include storage. For content that is stored definitively on the Cloudflare network, as opposed to transiting or being temporarily cached on the network, we review the complaint carefully to determine whether additional action needs to be taken.

Requests for content removal due to copyright

Cloudflare carefully reviews requests that we receive for content removal under the Digital Millennium Copyright Act (DMCA). If we are storing the content in question and we receive a valid takedown request that meets DMCA requirements, we will notify the user of the complaint and take steps to disable access to that content, consistent with the DMCA.

Government requests for content blocking

Cloudflare also may receive written requests from law enforcement and government agencies to block access to content based on the local law of the jurisdiction. Because of the significant potential impact on freedom of expression, Cloudflare will evaluates each content blocking request on a case-by-case basis, analyzing the factual basis and legal authority for the request.

If we determine that the order is valid and requires Cloudflare action, we may limit blocking of access to the content to those areas where it violates local law, a practice known as "geo-blocking". We will attempt to clarify and narrow overbroad requests when possible.

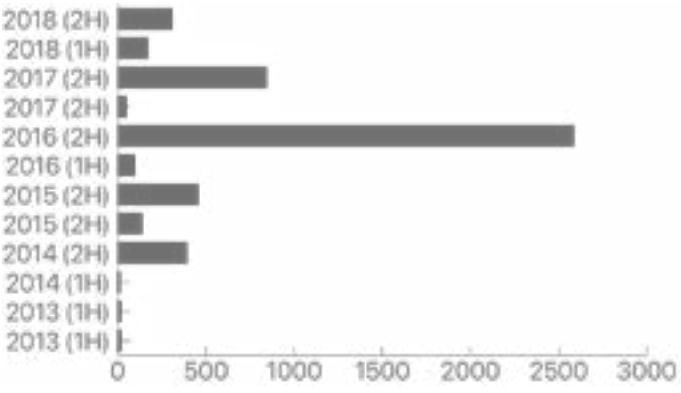
The data

The data presented below is updated through December 31, 2018. A request received in December 2018, but not processed until January 2019 will show as both "Requests received" and "Requests in process." Also, requests for which we are waiting for a response from law enforcement before moving forward may also be reflected in "Requests in process." The "Total # of domains affected" and the "Total number of accounts affected" refer only to requests which have been answered.

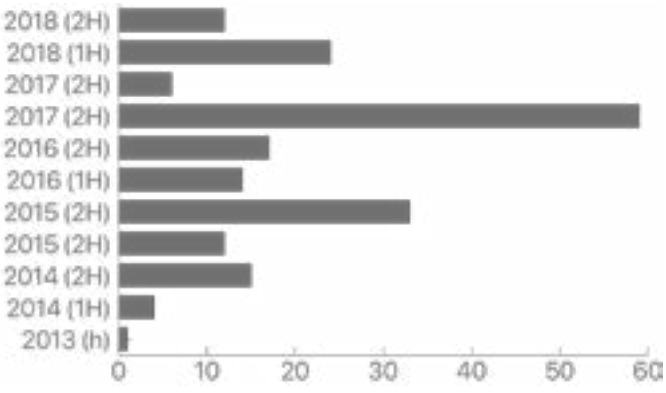
U.S. Government Criminal Subpoenas

This category includes U.S. legal process in connection with a criminal investigation that does not have prior judicial review, including but not limited to grand jury subpoenas, U.S. government attorney issued subpoenas, and case agent issued summonses.

Domain affected



Accounts affected



Year	Requests received	Requests answered	Requests in process	Total # of domains affected	Total # of accounts affected
2018 (2H)	19	7	0	309	12
2018 (1H)	23	14	0	172	24
2017 (2H)	22	13	2	846	6
2017 (1H)	21	8	1	51	59
2016 (2H)	9	6	0	2586	17
2016 (1H)	12	11	0	96	14
2015 (2H)	26	22	0	458	33
2015 (1H)	12	10	0	139	12
2014 (2H)	12	11	1	393	15
2013	18	1	0	17	1

U.S. administrative subpoenas

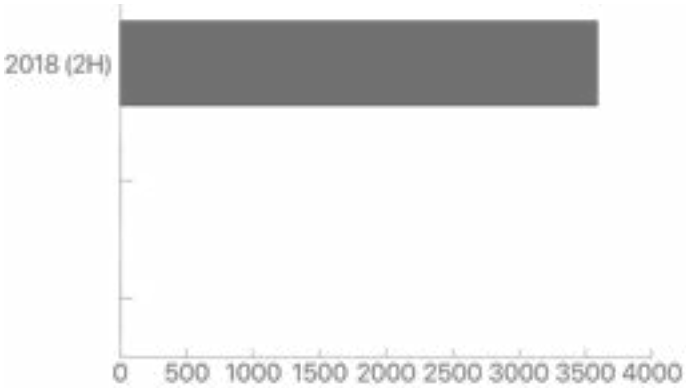
Administrative subpoenas are legal process issued directly by a U.S. government agency without judicial oversight like those issued by the Securities and Exchange Commission and the Federal Trade Commission.

Year	Requests received	Requests answered	Requests in process	Total # of domains affected	Total # of accounts affected
2018 (2H)	N/A	0	0	0	0

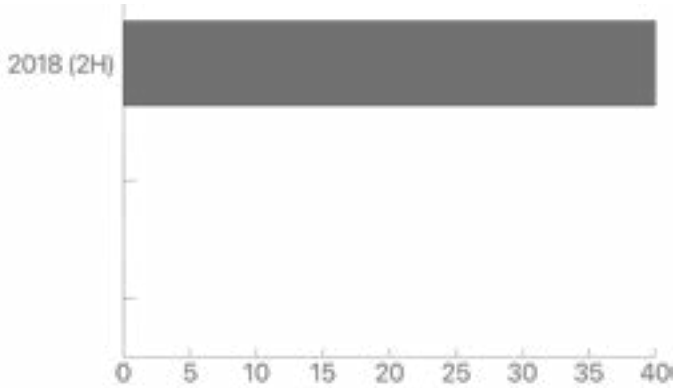
Civil Subpoenas

This category includes subpoenas for subscriber information received from civil litigants, such as subpoenas issued pursuant to the Digital Millennium Copyright Act (DMCA).

Domain affected



Accounts affected

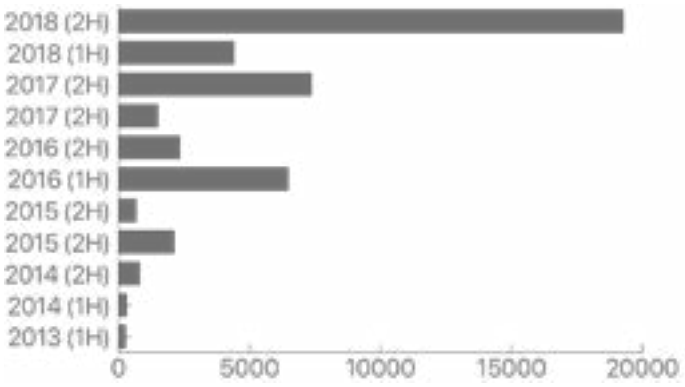


Year	Requests received	Requests answered	Requests in process	Total # of domains affected	Total # of accounts affected
2018 (2H)	21	21	0	3,588	40

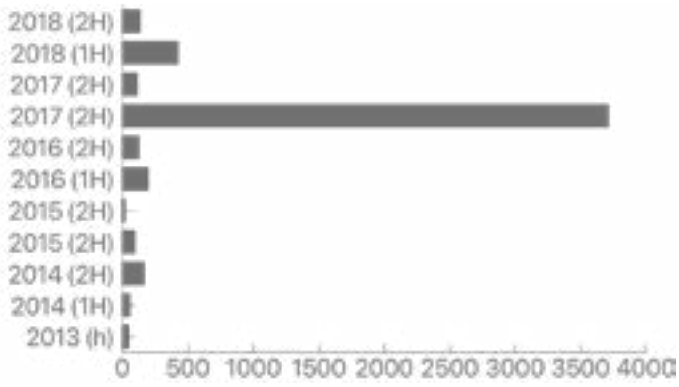
Court orders

This category includes any order issued by a judge or magistrate, including but not limited to 18 U.S.C. § 2703(d), 18 U.S.C. § 2705(b), and MLAT orders. Orders which may fall under a more specific category such as search warrants or pen register / trap and trace orders will be reported under the more specific category and not counted here.

Domain affected



Accounts affected

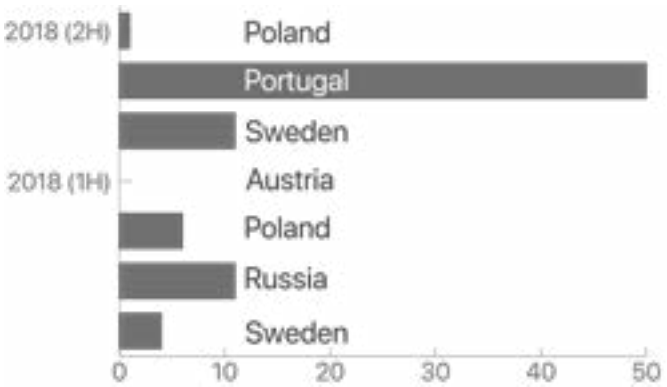


Year	Requests received	Requests answered	Requests in process	Total # of domains affected	Total # of accounts affected
2018 (2H)	55	44	1	19265	134
2018 (1H)	95	83	0	4400	425
2017 (2H)	79	64	1	7354	113
2017 (1H)	74	56	4	1498	3711
2016 (2H)	60	55	0	2338	126
2016 (1H)	47	46	0	6465	196
2015 (2H)	14	14	0	668	18
2015 (1H)	50	49	0	2120	96
2014 (2H)	24	23	5	802	167
2014 (1H)	22	21	1	290	57
2013	28	27	0	266	47

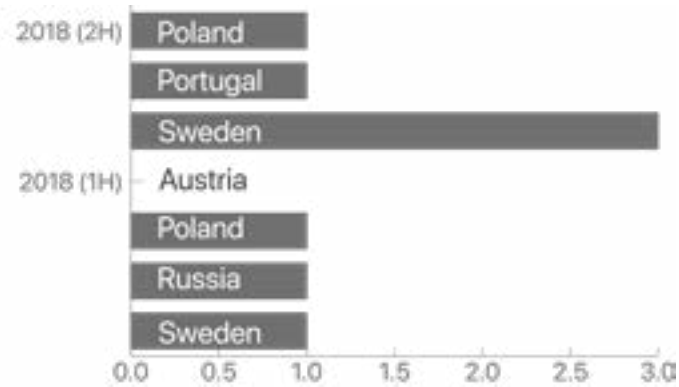
Mutual Legal Assistance Treaty

Our reporting on U.S. court orders above includes orders requested by foreign governments through the MLAT process. To provide additional granularity on MLAT requests, we have also identified those court orders clearly identified to be requested from a foreign government through the MLAT process.

Domain affected



Accounts affected

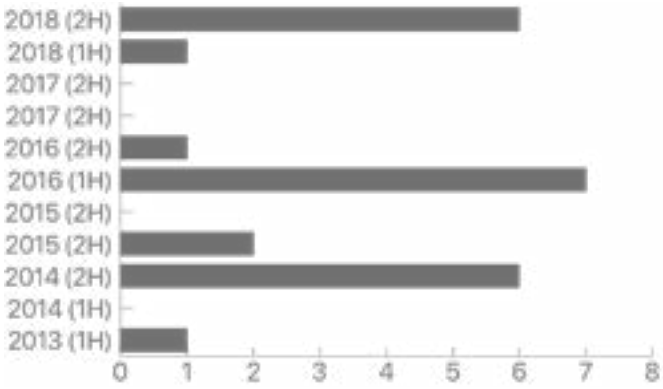


Year	Country	Requests received	Requests in process	Total # of domains affected	Total # of accounts affected
2018 (2H)	Poland	2	0	1	1
	Portugal	2	0	50	1
	Sweden	5	0	11	3
2018 (1H)	Austria	1	0	0	0
	Poland	2	0	6	1
	Russia	1	0	11	1
	Sweden	2	0	4	1

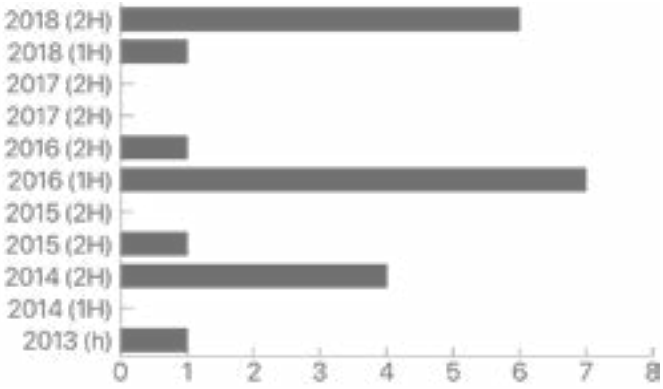
Pen register/Trap and trace (PRTT) orders

This category includes only pen register/trap and trace orders issued by the court for real-time disclosure of non-content information, including IP address information.

Domain affected



Accounts affected



Year	Requests received	Requests answered	Requests in process	Total # of domains affected	Total # of accounts affected
2018 (2H)	1	1	0	6	6
2018 (1H)	1	1	0	1	1
2017 (2H)	0	0	0	0	0
2017 (1H)	0	0	0	0	0
2016 (2H)	1	1	0	1	1
2016 (1H)	2	2	0	7	7
2015 (2H)	0	0	0	0	0
2015 (1H)	1	1	0	2	1
2014 (2H)	1	1	0	6	4
2014 (1H)	0	0	0	0	0
2013	1	1	0	1	1

National security process

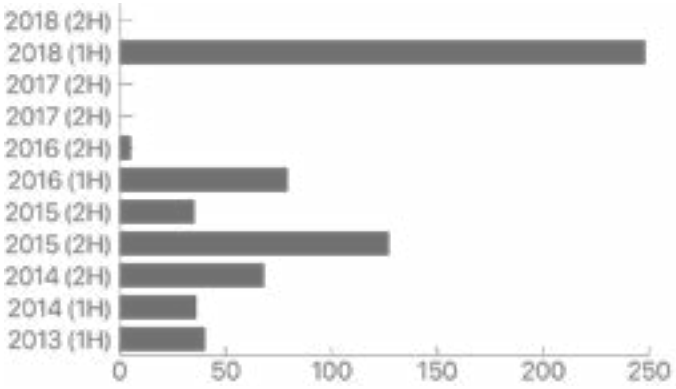
What we can say about either FISA court orders or NSL that we receive is highly regulated, and depends on exactly how we report the information. Current guidelines on reporting, codified as part of the USA FREEDOM Act, allow companies to disclose the combined number of NSLs and both content and non-content FISA orders as a single number in bands of 250, starting with 0-249

Year	Requests received	Requests answered
2018 (2H)	0-249	0-249
2018 1H)	0-249	0-249
2017 (2H)	0-249	0-249
2017 (1H)	0-249	0-249
2016 (2H)	0-249	0-249
2016 (1H)	0-249	0-249
2015 (2H)	0-249	0-249
2015 (1H)	0-249	0-249
2014 (2H)	0-249	0-249
2014 (1H)	0-249	0-249
2013	0-249	0-249
2012	0-249	0-249

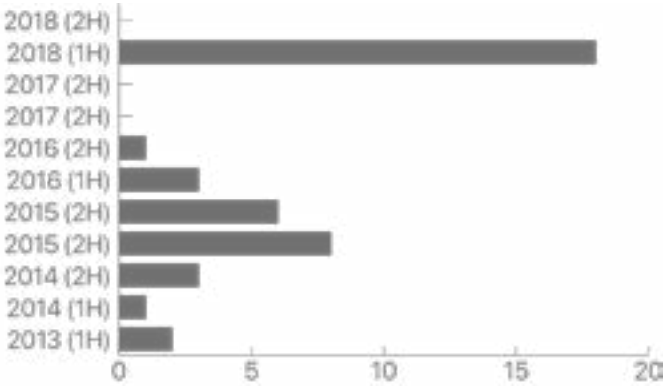
Search warrants

This category includes only search warrants which require judicial review, probable cause, and inclusion of a location to be searched and a detail of items requested.

Domain affected



Accounts affected



Year	Requests received	Requests answered	Requests in process	Total # of domains affected	Total # of accounts affected
2018 (2H)	1	0	0	0	0
2018 (1H)	4	2	0	248	18
2017 (2H)	1	1	0	0	0
2017 (1H)	1	0	0	0	0
2016 (2H)	1	1	0	5	1
2016 (1H)	3	3	0	79	3
2015 (2H)	5	5	0	35	6
2015 (1H)	3	3	0	127	8
2014 (2H)	2	2	1	68	3
2014 (1H)	1	1	0	36	1
2013	3	2	0	40	2

So far in 2018 Cloudflare has pushed back on 2 search warrants, and they were rescinded.

Wiretap orders

This category includes only wiretap orders that were issued by a court.

Year	Requests received	Requests answered	Requests in process	Total # of domains affected	Total # of accounts affected
2018 (2H)	0	0	0	0	0
2018 (1H)	0	0	0	0	0
2017 (2H)	0	0	0	0	0
2017 (1H)	0	0	0	0	0
2016 (2H)	0	0	0	0	0
2016 (1H)	0	0	0	0	0
2015 (2H)	0	0	0	0	0
2015 (1H)	0	0	0	0	0
2014 (2H)	0	0	0	0	0
2014 (1H)	0	0	0	0	0
2013	0	0	0	0	0

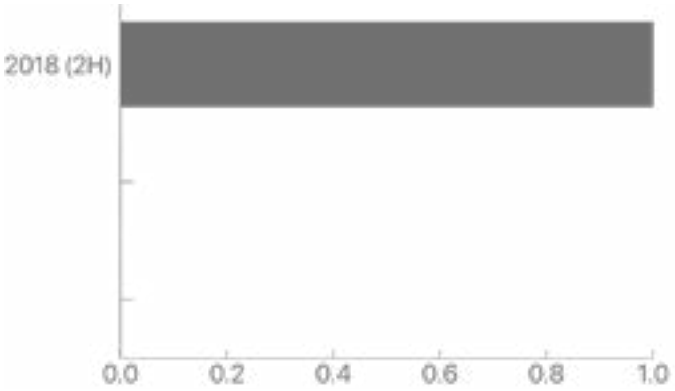
Requests for Content Removal or Blocking

The data presented below is for the period from June 1, 2018 to December 31, 2018. A request received in December 2018, but not processed until January 2019 will show as both "Requests received" and "Requests in process."

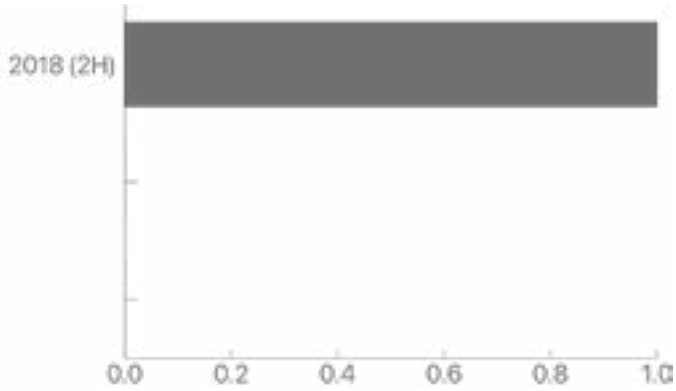
Requests for content removal due to copyright

This report reflects only DMCA takedown requests for content definitively stored on our network, not for cached or transiting content. Cloudflare forwards other requests to the hosting services storing the content in question.

Domain affected



Accounts affected



Year	Requests received	Requests answered	Requests in process	Total # of domains affected	Total # of accounts affected
2018 (2H)	1	1	0	1	1

Conclusion

Given the vast amount of information transiting of our global network, Cloudflare is mindful of the special and sensitive position we occupy with regard to our customers. Cloudflare is extremely mindful of the position and the responsibilities our customers have placed on us through their trust. While there has been a steady increase in the number of law enforcement requests since our first transparency report in 2013, this is due in part to the exponential increase in the number of Cloudflare customer domains during that time period.

We will continue to publish this report on a semiannual basis. Please be advised that we may restate data as we go forward as more complete information becomes available or if we change our classifications.