

# 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.

# Overview

## 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.

## 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.

## 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

1. Cloudflare has never turned over our encryption or authentication keys or our customers' encryption or authentication keys to anyone.
2. Cloudflare has never installed any law enforcement software or equipment anywhere on our network.
3. Cloudflare has never provided any law enforcement organization a feed of our customers' content transiting our network.
4. Cloudflare has never modified customer content at the request of law enforcement or another third party.
5. Cloudflare has never modified the intended destination of DNS responses at the request of law enforcement or another third party.
6. 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 the Data

The data presented below covers the period from July 1, 2022, to December 31, 2022. A request received in December 2022, but not processed until January 2023 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 number of domains affected and the total number of accounts affected refer only to requests which have been answered.

## Background on Requests for User Data

Cloudflare receives requests for different kinds of data on its users from U.S. 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.

We also recognize that a government’s request for data might be inconsistent with another government’s regulatory regime for protecting the personal data of its citizens. Cloudflare believes that government requests for the personal data of a person that conflict with the privacy laws of that person’s country of residence should be legally challenged.

This report does not include information about government requests for data that may be received by Cloudflare’s partners.

## 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 a subpoena or a foreign government equivalent of a subpoena before providing this type of information to either foreign or domestic government authorities 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 provide users' personal information. The U.S. government can also issue National Security Letters (NSLs), which are similar to subpoenas, for subscriber and limited 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, particularly when they are indefinite in nature. 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 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.

Cloudflare believes that government access to data must be consistent with the

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.

### **Emergency Requests**

Cloudflare receives emergency requests for data from time to time from law enforcement and governments. Cloudflare will respond on a voluntary basis if we have a good faith belief that there is an emergency involving the danger of death or serious physical injury.

### **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. The court orders that Cloudflare receives typically include a temporary non-disclosure requirement.

### **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 as 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 does not store customer content -- like email or other types of customer-generated material -- for websites using Cloudflare's pass-through security and performance services.

Cloudflare does have a number of products that involve storage services, such as our R2, Workers, Stream, and Pages products. As those services involve customer content under the Electronic Communications Privacy Act, we would insist on a search warrant before providing information to any law enforcement request for customer content stored in our storage services, consistent with the principles laid out in [U.S. v. Warshak](#). Any such warrants for stored content will be reported separately in our Transparency Report.

### **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, we have not had customer content to provide in response to those warrants when they seek content related to Cloudflare's pass-through security and performance services.

### **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. As noted above, Cloudflare does not have access to the type of traditional customer content generally sought by FISA court orders. Because the public reporting of all national security process is highly regulated, if Cloudflare were to receive such an order, it 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 the WHOIS records 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. Consistent with legal requirements like those in the EU's Digital Services Act (DSA), Cloudflare has different terms of service and a different process for responding to legal requests or abuse complaints about content stored on our network, as opposed to content transiting or being temporarily cached on the network, reflecting the distinct legal requirements and expectations for definitively hosted content. If Cloudflare receives a valid takedown request content that is stored on the Cloudflare network, Cloudflare will disable access to the content, as appropriate. This report includes details on the requests we receive to disable access to content stored on our network, described as "hosted content."

### 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 receive a DMCA complaint regarding the limited amount of content that we host, we will notify the user of the alleged infringement, allow for the user to provide a counter notice contesting the infringement allegation, and remove content consistent with the DMCA.

### Termination of Hosting Services Due to Technical Abuse

When Cloudflare determines that a domain for which we provide hosting services, such as Pages, is engaged in technical abuse, we may terminate hosting services for that domain. This may include domains engaged in phishing or the dissemination of malware.

### Requests for Content Blocking

Cloudflare also may receive written requests from law enforcement, government agencies, or foreign courts 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 evaluate 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”. In those cases, we strive to be transparent about the basis for the blocking, typically with a block page that includes a link to the underlying legal order. We will attempt to clarify and narrow overbroad requests when possible.

### Requests for Content Blocking through DNS resolver

Cloudflare has received a small number of legal requests related to blocking or filtering content through the 1.1.1.1 Public DNS Resolver. Because such a block would apply globally to all users of the resolver, regardless of where they are located, it would affect end users outside of the blocking government’s jurisdiction. We therefore evaluate any government requests or court orders to block content through a globally available public recursive resolver as requests or orders to block content globally.

Given the broad extraterritorial effect, as well as the different global approaches to DNS-based blocking, Cloudflare has pursued legal remedies before complying with requests to block access to domains or content through the 1.1.1.1 Public DNS Resolver or identified alternate mechanisms to comply with relevant court orders. To date, Cloudflare has not blocked content through the 1.1.1.1 Public DNS Resolver.

### IPFS / Ethereum Gateways

Cloudflare offers a number of gateways to enable users to access content stored on new distributed web technologies. Specifically, Cloudflare’s IPFS and Ethereum Gateways provide access to content on the InterPlanetary File System (IPFS), which is a peer-to-peer file system, and the Ethereum network, which is a distributed virtual computing network that stores and enforces smart contracts. Cloudflare does not host content on IPFS or the Ethereum network, and cannot remove it from storage. Indeed, because of the nature of distributed systems, content is generally stored on many nodes at the same time.

Although Cloudflare does not have the ability to remove content on IPFS or Ethereum, Cloudflare may disable access through Cloudflare-operated gateways to certain content on IPFS and the Ethereum network in response to abuse reports, including reports of copyright, technical, sanctions compliance, and other abuse. This action does not prevent access to that content through other gateways, which Cloudflare does not control.

### Requests for Uniform Domain-Name Dispute Resolutions



As an ICANN-accredited domain registrar, Cloudflare follows ICANN's Uniform Domain-Name Dispute Resolution Policy (UDRP) for trademark-based domain name disputes. Consistent with the policy, Cloudflare will, upon receipt of a valid UDRP verification request from an ICANN approved dispute board: (1) Lock the disputed domain name(s) to prevent modification to the registrant and registrar information for the duration of the dispute, and (2) Unmask or provide the underlying WHOIS information to the dispute board.

Upon receipt of a valid notice of decision from an ICANN approved dispute board, and based on the decision, Cloudflare will, as appropriate, unlock the domain to allow the Respondent to manage the domain, transfer the domain to the Complainant at a predetermined time to allow the Respondent to initiate legal dispute with their local legal system that is within the jurisdiction of the Registrar, or delete the domain.

## Child Safety

Cloudflare has viewed responding to incidents of child sexual abuse material (CSAM) online as a priority since the company's earliest days. When it comes to CSAM, our position is simple: We don't tolerate it. We abhor it. It's a crime, and we do what we can to support the processes to identify and remove that content.

Cloudflare is committed to providing tools to helping website operators to keep their sites free from child sexual abuse material (CSAM). To do that, we created our CSAM Scanning Tool and made it generally available for free in the second half of 2021 to all customers, regardless of plan level. Once enabled, the CSAM Scanning Tool identifies potential CSAM material on a website using fuzzy hashing technology, takes steps to block that content from being accessed, helps ensure the customer reports the content to the National Center for Missing and Exploited Children (NCMEC), and notifies the customer so that they can take appropriate additional steps. Under the scanning tool's original configuration in place in the first half of 2021, Cloudflare submitted reports to NCMEC from the tool on our customers' behalf. Incorporating input from NCMEC, we subsequently updated the tool to allow our customers to submit the reports themselves to enable more direct follow up.

Cloudflare also prioritizes responding to reports of CSAM. Although we are not in a position to remove content from the Internet that we do not host, we do everything we can to assist in getting that content taken offline. Abuse reports filed under the CSAM category are treated as the highest priority for our Trust & Safety team and moved to the front of the abuse response queue. Whenever we receive such a report, generally within minutes regardless of time of day or day of the week, we forward the report to NCMEC, as well as to the hosting provider and/or website operator, along with some additional information to help them locate the content quickly. We also respond to the reporter with additional details so that they can follow up as necessary.

# The Data

The data presented below is updated through December 31, 2022. A request received in December 2022, but not processed until January 2023 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. Requests for User Data

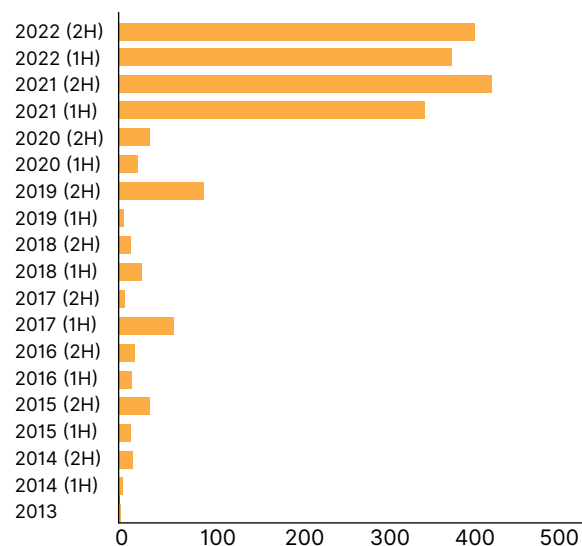
### U.S. Government Criminal Subpoenas

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.

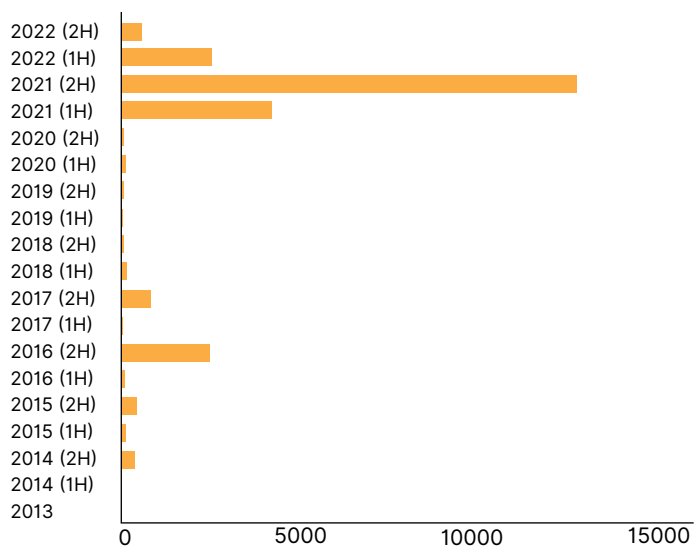
Year	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	246	192	18	385	592
2022 (1H)	224	168	28	360	2662*
2021 (2H)	163	122	8	404	13339*
2021 (1H)	183	152	0	332	4402
2020 (2H)	33	11	0	33	73
2020 (1H)	22	7	0	20	125
2019(2H)	11	7	0	92	78
2019(1H)	20	8	0	5	53
2018 (2H)	21	10	0	12	72
2018 (1H)	23	14	0	24	172
2017 (2H)	22	13	2	6	846
2017 (1H)	21	8	1	59	51
2016 (2H)	9	6	0	17	2586
2016 (1H)	12	11	0	14	96
2015 (2H)	26	22	0	33	458
2015 (1H)	12	10	0	12	139
2014 (2H)	12	11	1	15	393
2014 (1H)	11	4	0	4	12
2013	18	1	0	1	17

\* A single request sought information related to a large number of domains.

#### Accounts affected



#### Domains affected



## 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	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	3	2	0	2	2
2022 (1H)	7	3	1	2	2
2021 (2H)	3	3	0	7	24
2021 (1H)	0	0	0	0	0
2020 (2H)	1	0	0	0	0
2020 (1H)	2	2	0	10	7
2019 (2H)	1	1	0	1	1
2019 (1H)	0	0	0	0	0
2018 (2H)	N/A	0	0	0	0

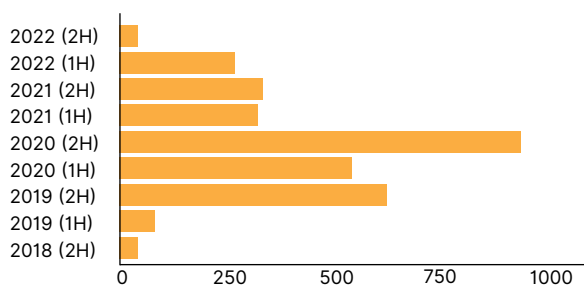
## Civil Subpoenas

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

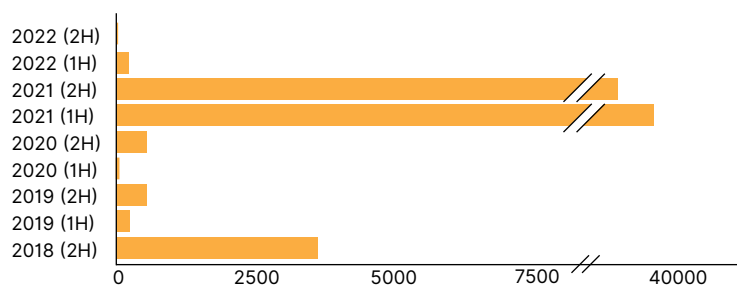
Year	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	20	20	0	40	57
2022 (1H)	35	34	1	272*	203
2021 (2H)	56	53	4	336	33025*
2021 (1H)	45	45	0	325	35382
2020 (2H)	47	42	0	952	517
2020 (1H)	31	30	0	548	79
2019 (2H)	51	51	0	629	461
2019 (1H)	28	27	0	80	209
2018 (2H)	21	21	0	40	3588

\* A single request sought information related to a large number of accounts.

### Accounts affected



### Domains affected

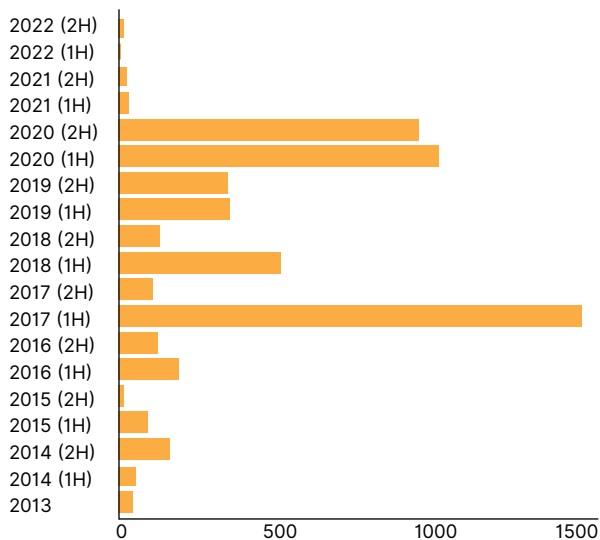


## Court Orders

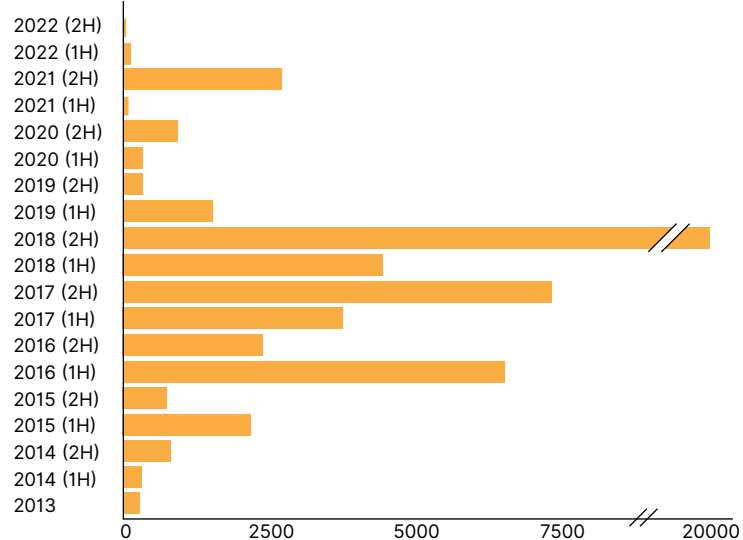
This category includes any order issued by a judge or magistrate, including but not limited to 18 U.S.C. § 2703(d), 18 U.S.C. § 2705(b), and MLAT orders. Orders which may fall under a more specific category such as search warrants or pen register / trap and trace orders will be reported under the more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

Year	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	19	13	0	14	19
2022 (1H)	11	7	4	7	95
2021 (2H)	14	12	0	26	2600
2021 (1H)	18	17	0	35	40
2020 (2H)	136	109	0	973	873
2020 (1H)	148	118	0	1038	328
2019 (2H)	92	76	0	353	325
2019 (1H)	132	108	0	363	1446
2018 (2H)	57	45	1	134	19222
2018 (1H)	95	83	0	526	4400
2017 (2H)	79	64	1	113	7354
2017 (1H)	75	56	4	1498	3711
2016 (2H)	60	55	0	126	2338
2016 (1H)	47	43	0	196	6465
2015 (2H)	14	14	0	18	668
2015 (1H)	50	49	0	96	2120
2014 (2H)	24	23	5	167	802
2014 (1H)	22	21	1	57	290
2013	28	27	0	47	266

### Accounts affected



### Domains affected

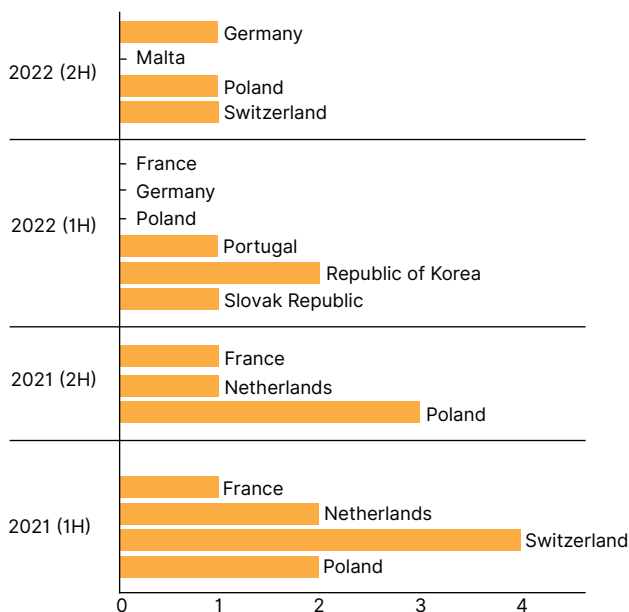


## Mutual Legal Assistance Treaty

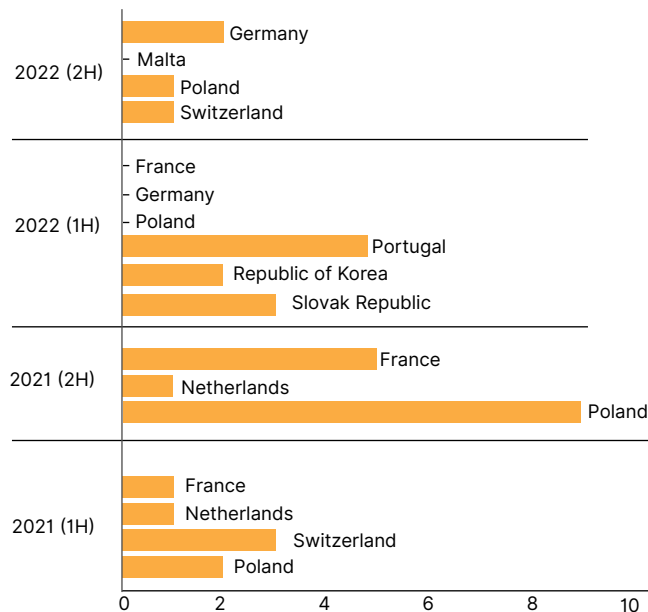
Our reporting on U.S. court orders above includes orders requested by foreign governments through the MLAT process. To provide additional granularity on MLAT requests, we have also identified those court orders clearly identified to be requested from a foreign government through the MLAT process.

Year	Country	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	Germany	1	1	0	1	2
	Malta	1	0	0	0	0
	Poland	1	1	0	1	1
	Switzerland	1	1	0	1	1
2022 (1H)	France	1	1	0	0	0
	Germany	1	0	0	0	0
	Poland	1	0	0	0	0
	Portugal	1	1	0	1	4
	Republic of Korea	1	1	0	2	2
	Slovak Republic	1	1	0	1	3
2021 (2H)	France	1	1	0	1	5
	Netherlands	1	1	0	1	1
	Poland	2	2	0	3	9
2021 (1H)	France	1	1	0	1	1
	Netherlands	1	1	0	2	1
	Switzerland	2	2	0	4	3
	Poland	2	2	0	2	2

### Accounts affected



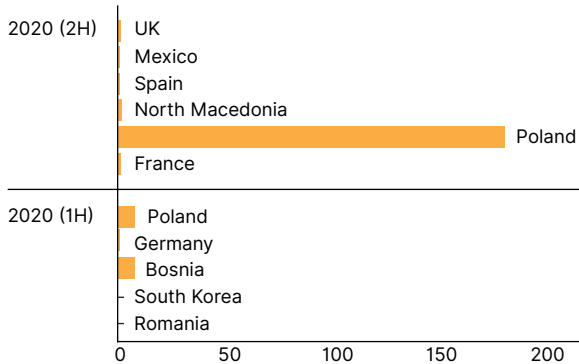
### Domains affected



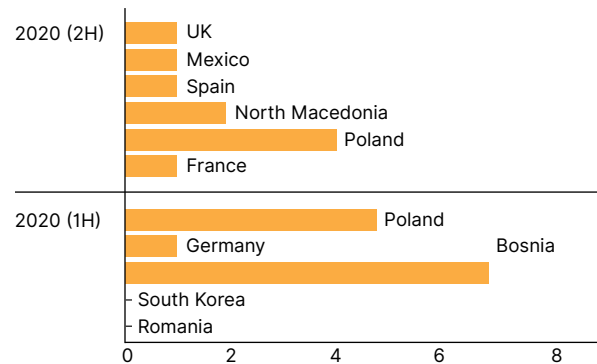
Continued on next page

Year	Country	Received	Answered	In process	Accounts affected	Domains affected
2020 (2H)	UK	1	1	0	2	1
	Mexico	1	1	0	1	1
	Spain	1	1	0	1	1
	North Macedonia	2	2	0	4	2
	Poland	3	2	0	186	4
	France	1	1	0	3	1
2020 (1H)	Poland	3	3	0	14	5
	Germany	1	1	0	1	1
	Bosnia	1	1	0	14	7
	South Korea	1	0	0	0	0
	Romania	1	0	0	0	0

### Accounts affected

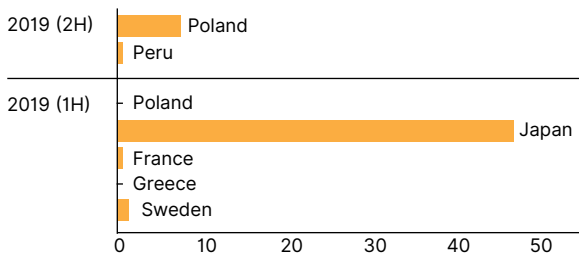


### Domains affected

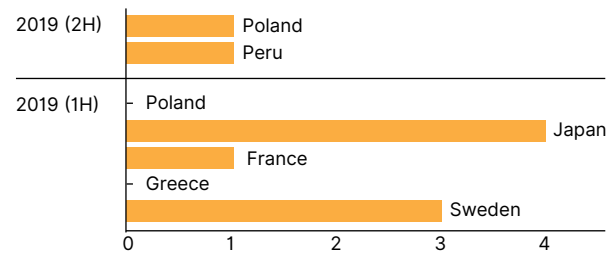


Year	Country	Received	Answered	In process	Accounts affected	Domains affected
2019 (2H)	Poland	1	1	0	7	1
	Peru	1	1	0	1	1
2019 (1H)	Poland	2	0	0	0	0
	Japan	2	2	0	47	4
	France	1	1	0	1	1
	Greece	1	0	0	0	0
	Sweden	1	1	0	2	3

### Accounts affected



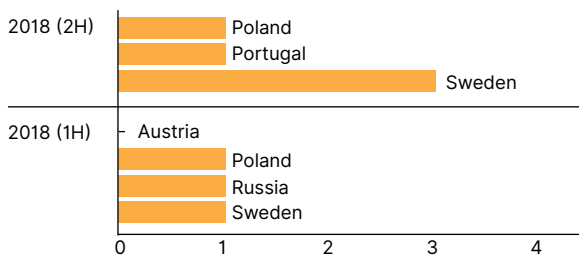
### Domains affected



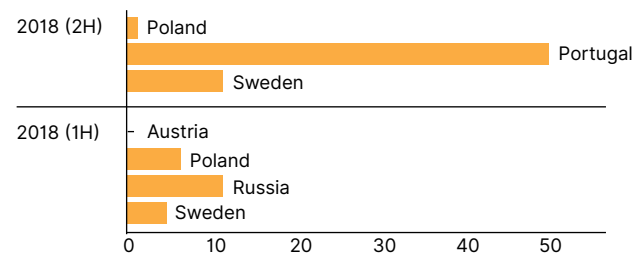
Continued on next page

Year	Country	Received	Answered	In process	Accounts affected	Domains affected
2018 (2H)	Poland	2	1	0	1	1
	Portugal	2	1	0	1	50
	Sweden	5	3	0	3	11
2018 (1H)	Austria	1	0	0	0	0
	Poland	2	1	0	1	6
	Russia	1	1	0	1	11
	Sweden	2	1	0	1	4

### Accounts affected



### Domains affected





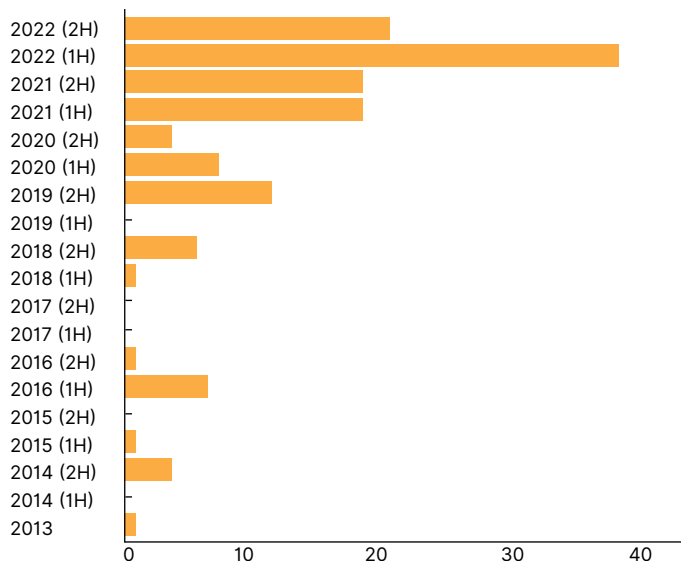
## Pen Register/Trap and Trace (PRTT) Orders

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.

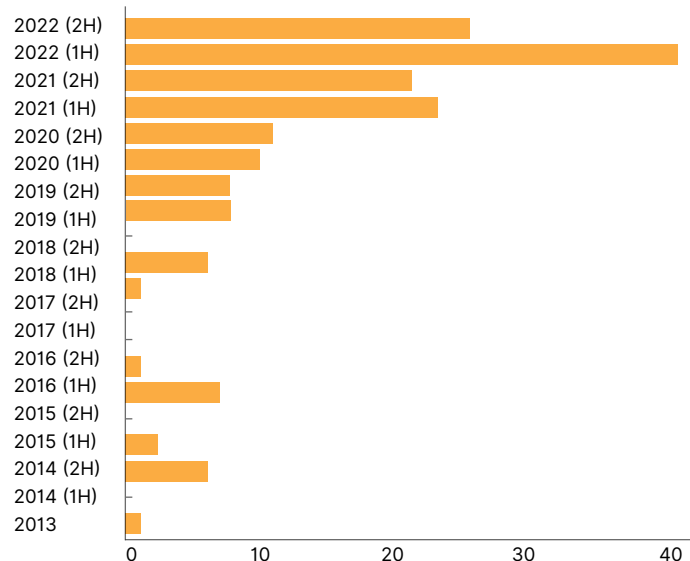
Year	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	21	21	0	21	25
2022 (1H)	39	39	0	39	40
2021 (2H)	16	16	0*	19	21
2021 (1H)	7	7	0	19	23
2020 (2H)	4	4	0	4	11
2020 (1H)	4	4	0	8	10
2019 (2H)	5	5	0	12	8
2019 (1H)	0	0	0	0	0
2018 (2H)	1	1	0	6	6
2018 (1H)	1	1	0	1	1
2017 (2H)	0	0	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	1	2
2014 (2H)	1	1	0	4	6
2014 (1H)	0	0	0	0	0
2013	1	1	0	1	1

\* This number was adjusted in February 2023 to correct a ministerial error.

### Accounts affected



### Domains affected

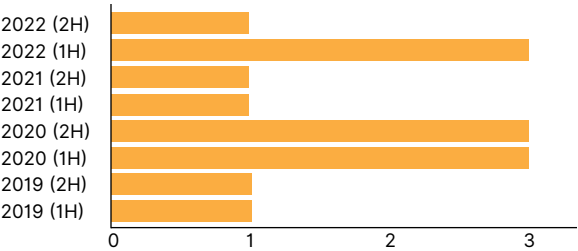


### Emergency Requests

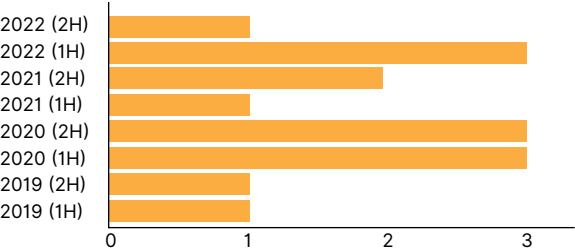
This category includes emergency requests for data.

Year	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	38	31	0	1	1
2022 (1H)	12	11	0	3	3
2021 (2H)	7	5	0	1	2
2021 (1H)	2	2	0	1	1
2020 (2H)	9	6	0	3	3
2020 (1H)	5	3	0	3	3
2019 (2H)	5	1	0	1	1
2019 (1H)	5	5	0	1	1

#### Accounts affected



#### Domains affected



## 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	Received	Answered
2022 (2H)	0-249	0-249
2022 (1H)	0-249	0-249
2021 (2H)	0-249	0-249
2021 (1H)	0-249	0-249
2020 (2H)	0-249	0-249
2020 (1H)	0-249	0-249
2019 (2H)	0-249	0-249
2019 (1H)	0-249	0-249
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

## Search Warrants

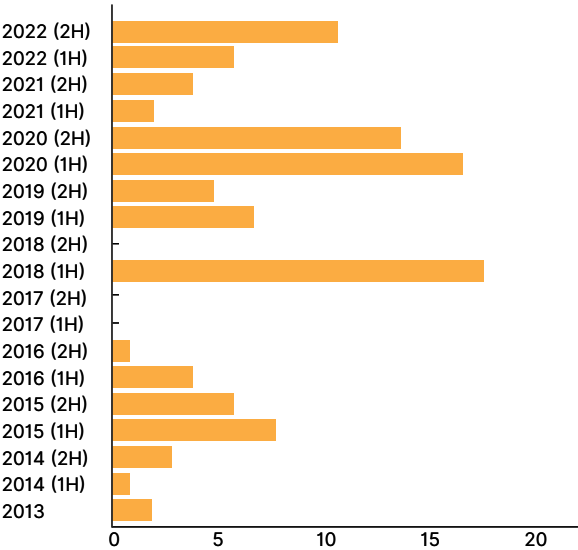
Search warrants which require judicial review, probable cause, and inclusion of a location to be searched and a detail of items requested. Because the information Cloudflare has that might be responsive to a search warrant is dependent on the service at issue, we report search warrants relating to our pass-through services separately from search warrants relating to our storage services.

### Search Warrants Relating to Pass-Through Services

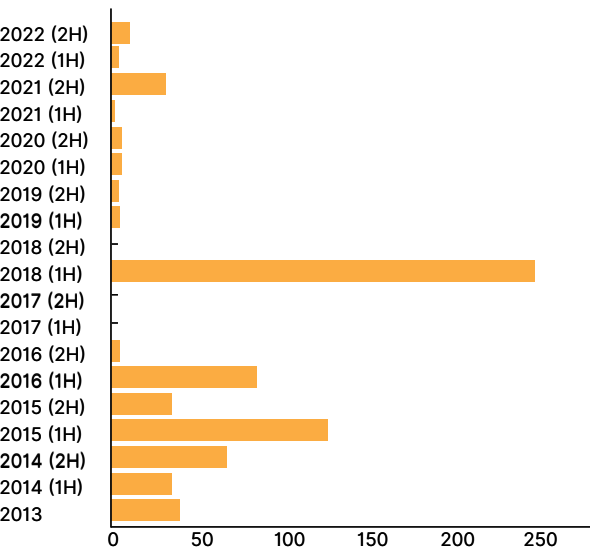
This category includes search warrants for websites using Cloudflare's pass-through security and performance services. In the second half of 2022, Cloudflare processed 8 search warrants relating to our pass-through services. Although we processed the warrants we did not have customer content to provide in response.

Year	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	18	8	0	11	11
2022 (1H)	9	6	1	6	4
2021 (2H)	10	8	2	4	32
2021 (1H)	8	6	0	2	2
2020 (2H)	9	5	0	14	6
2020 (1H)	6	5	0	17	6
2019 (2H)	3	3	0	5	4
2019 (1H)	5	5	0	7	5
2018 (2H)	1	0	0	0	0
2018 (1H)	4	2	0	18	248
2017 (2H)	1	1	0	0	0
2017 (1H)	1	0	0	0	0
2016 (2H)	1	1	0	1	5
2016 (1H)	4	4	0	4	85
2015 (2H)	5	5	0	6	35
2015 (1H)	3	3	0	8	127
2014 (2H)	2	2	1	3	68
2014 (1H)	1	1	0	1	36
2013	3	2	0	2	40

Accounts affected



Domains affected

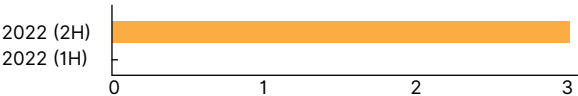


Search Warrants Relating to Stored Content

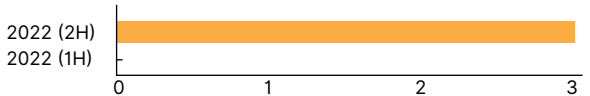
As noted above, a number of Cloudflare products involve storage services that may store customer content. Cloudflare requires a search warrant before providing stored customer content to law enforcement. In the second half of 2022, Cloudflare received one search warrant relating to stored content.

Year	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	1	1	0	3	3
2022 (1H)	0	0	0	0	0

Accounts affected



Domains affected



## Wiretap Orders

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

Year	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	0	0	0	0	0
2022 (1H)	0	0	0	0	0
2021 (2H)	0	0	0	0	0
2021 (1H)	0	0	0	0	0
2020 (2H)	0	0	0	0	0
2020 (1H)	0	0	0	0	0
2019 (2H)	0	0	0	0	0
2019 (1H)	0	0	0	0	0
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

## Non-U.S. Requests for User Data

This category includes requests for user information from governments outside the United States that do not come through the U.S. court system.

### CLOUD Act

On October 3, 2019, the US and UK signed an Executive Agreement under the CLOUD Act, which entered into force on October 3, 2022. Based on the agreement, Cloudflare intends to comply with appropriately scoped and targeted requests for data from UK law enforcement. Information about any legal requests that Cloudflare receives from non-U.S. governments pursuant to the CLOUD Act will be included in future transparency reports. The UK is the only country to have signed a CLOUD Act agreement with the United States that has entered into force as of the date of this transparency report.

## Requests for Content Removal or Blocking

The data presented below is for the period from July 31, 2022 to December 31, 2022. A request received in December 2022, but not processed until January 2023 will show as both “Requests received” and “Requests in process.”

### Requests for Hosted Content Removal Due to Copyright

The Digital Millennium Copyright Act and Digital Services Act contemplate different procedures for hosting services than for other services like caching or transit. As described in more detail above, when Cloudflare receives a copyright abuse report relating to content that we do not host, we forward those requests to the hosting provider storing the content in question. This section addresses only those copyright abuse, DMCA or DSA reports directed towards content actually hosted by Cloudflare.

Only a few Cloudflare products host content. When Cloudflare receives a valid request for removal of copyrighted content for Stream, Pages, Images or R2, we will remove or disable access to that hosted content, and follow the procedures set forth in the DMCA, 17 U.S.C. § 512(g). If we receive a valid counter notice, we restore the removed content or cease disabling access to it as contemplated by the DMCA.

The table below reflects the total number of copyright abuse and DMCA reports received for content hosted by Cloudflare, regardless of whether the report was valid or complete. Because the infringing content may no longer be available online at the time we process the report, there may be no action for Cloudflare to take in response to some reports. In addition, Cloudflare will only remove or disable access to content in response to valid copyright abuse reports that satisfy the requirements of the DMCA. As a result, the number of reports that Cloudflare actions may be smaller than the number of reports received during the reporting period.

Year	Reports Received	Reports Where Cloudflare Took Action on Material	Counter Notices Received
2022 (2H)	972	972	0
2022 (1H)	269	20	2
2021 (2H)	18	2	0
2021 (1H)	7	7	0
2020 (2H)	0	0	0
2020 (1H)	2	2	0
2019 (2H)	1	1	0
2019 (1H)	2	2	0
2018 (2H)	1	1	0

## Actions on Hosted Content to Address Technical Abuse

Cloudflare terminates hosting services to those domains using Pages and other hosted Cloudflare services that we determine are engaged in technical abuse, such as phishing or other malicious activities. This category does not include actions in response to content-based abuse, like DMCA or CSAM-related violations, which are separately reported in the sections above.

Year	Total
2022 (2H)	179
2022 (1H)	186

## U.S. Court Orders

Cloudflare is occasionally subject to third-party orders in the United States directing Cloudflare and other service providers to terminate services to websites due to copyright or other prohibited content. Termination of Cloudflare's pass-through CDN and security services is not an effective means for addressing such content, because termination of services does not remove content from the Internet that we do not host. Other service providers are better positioned to address such websites, and it is normal for issues to be resolved even before Cloudflare takes action. Indeed, many domains that we have been ordered to terminate are no longer using Cloudflare's services by the time Cloudflare assesses whether to take action. Nonetheless, Cloudflare may terminate services in response to valid orders that comply with relevant laws.

Year	Termination Orders	Number of Domains	Number of Accounts
2022 (2H)	3	11*	4
2022 (1H)	1	1	1
2021 (2H)	2	11	5

*\* All but two of the domains had already stopped using Cloudflare's pass-through CDN and security services prior to Cloudflare taking action. For those domains that had already stopped using Cloudflare's services, the only effect of Cloudflare's action was to prevent those domains from using our services in the future.*



## Non-U.S. Court Orders

In July 2022, an Italian court issued an order directing Cloudflare to block access via Cloudflare's DNS resolver to websites the court concluded were violating copyright law. To the extent that those websites used Cloudflare services, Cloudflare took steps following the issuance of the order to disable access to those websites for users in Italy or from Cloudflare equipment in Italy. Cloudflare took action to geoblock all three domains that were addressed by the court's order and were using our service at the time the orders were issued via Cloudflare's pass-through CDN and security services.

## Voluntary Actions

Consistent with our public commitment in 2019 to report on any voluntary action that we take that could be viewed as termination "due to political pressure," Cloudflare has previously contemporaneously reported on certain efforts it has taken to voluntarily terminate services or block access to sites. To address the obligations of the Digital Services Act to report on "content moderation engaged in at the providers' own initiative," any such actions will now also be reported in our bi-annual transparency reports.

In a small number of well-publicized instances, Cloudflare has taken steps to voluntarily terminate services or block access to sites whose users were intentionally causing harm to others. On September 3, 2022, Cloudflare blocked access to Kiwifarms because of the emergency and immediate threat to human life, as described in more detail in our [blog](#).

## IPFS / Ethereum Gateways

Cloudflare may disable access through Cloudflare-operated gateways to certain content on IPFS and the Ethereum network in response to valid abuse reports, including reports of copyright, technical, sanctions compliance, and other abuse. These actions do not prevent the same content from being available through other gateways.

On August 8, 2022, the U.S. Department of Treasury sanctioned virtual currency mixer Tornado Cash, and included specific digital currency addresses in its [designation](#). Those sanctions raise significant legal questions about the extent to which particular computer software, rather than individuals or entities that use that software, can be subject to sanctions. Nonetheless, to comply with legal requirements, Cloudflare has taken steps to disable access through the Cloudflare-operated Ethereum Gateway to the digital currency addresses identified in the designation.

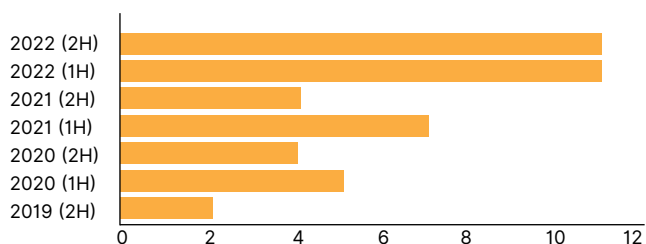
Year	Number of IPFS Actions	Number of Ethereum Actions
2022 (2H)	1142	99
2022 (1H)	1073	0

## UDRP Requests

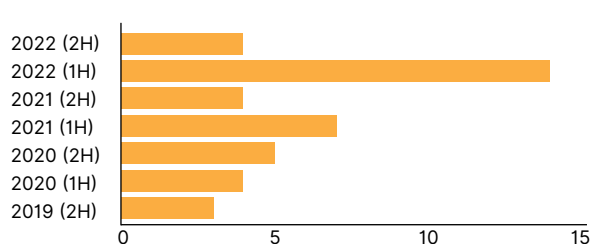
This category includes valid UDRP verification requests Cloudflare received from an ICANN-approved dispute board.

Year	Received	Answered	In process	Accounts affected	Domains affected
2022 (2H)	21	21	1	21	25
2022 (1H)	11	11	1	11	14
2021 (2H)	6	6	0	4	4
2021 (1H)	7	7	0	7	7
2020 (2H)	4	4	0	4	5
2020 (1H)	3	3	0	5	4
2019 (2H)	2	2	0	2	3

### Accounts affected



### Domains affected



## Child Safety

### Reporting to NCMEC

Cloudflare's Trust & Safety team submits reports regarding CSAM to NCMEC in response to reports submitted through our abuse form. For those customers using our CSAM Scanning Tool, we previously submitted reports to NCMEC regarding CSAM Scanning Tool matches on behalf of our customers. However, our CSAM Scanning Tool now enables customers to submit reports of potential CSAM material directly to NCMEC using their own credentials. As a result, the number of Scanning Tool reports submitted to NCMEC has decreased.

In 2021, prior to changes to our CSAM Scanning Tool that now enable our customers to directly submit reports of potential CSAM material to NCMEC, we also submitted reports to NCMEC regarding CSAM Scanning Tool matches on behalf of our customers.

Year	Abuse Form Reports Submitted to NCMEC
2022 (2H)	5640
2022 (1H)	1644
2021 (2H)	1124
2021 (1H)	1119

## Termination of Services

Cloudflare terminates services to domains that fail to take action to remove verified CSAM or are dedicated to the dissemination of CSAM.

Year	Total Number of Accounts Terminated	Total Number of Domains Terminated
2022 (2H)	206	530
2022 (1H)	56	118
2021 (2H)	70	198

## Conclusion

Given the vast amount of information transiting our global network, Cloudflare is mindful of the special and sensitive position we occupy with regard to our customers 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.



© 2023 Cloudflare Inc. All rights reserved.  
The Cloudflare logo is a trademark of Cloudflare. All other  
company and product names may be trademarks of the  
respective companies with which they are associated.

1 888 99 FLARE | [enterprise@cloudflare.com](mailto:enterprise@cloudflare.com) | [Cloudflare.com](https://cloudflare.com)

REV:BDES-4540.2023NOV01