CLOUDFLARE

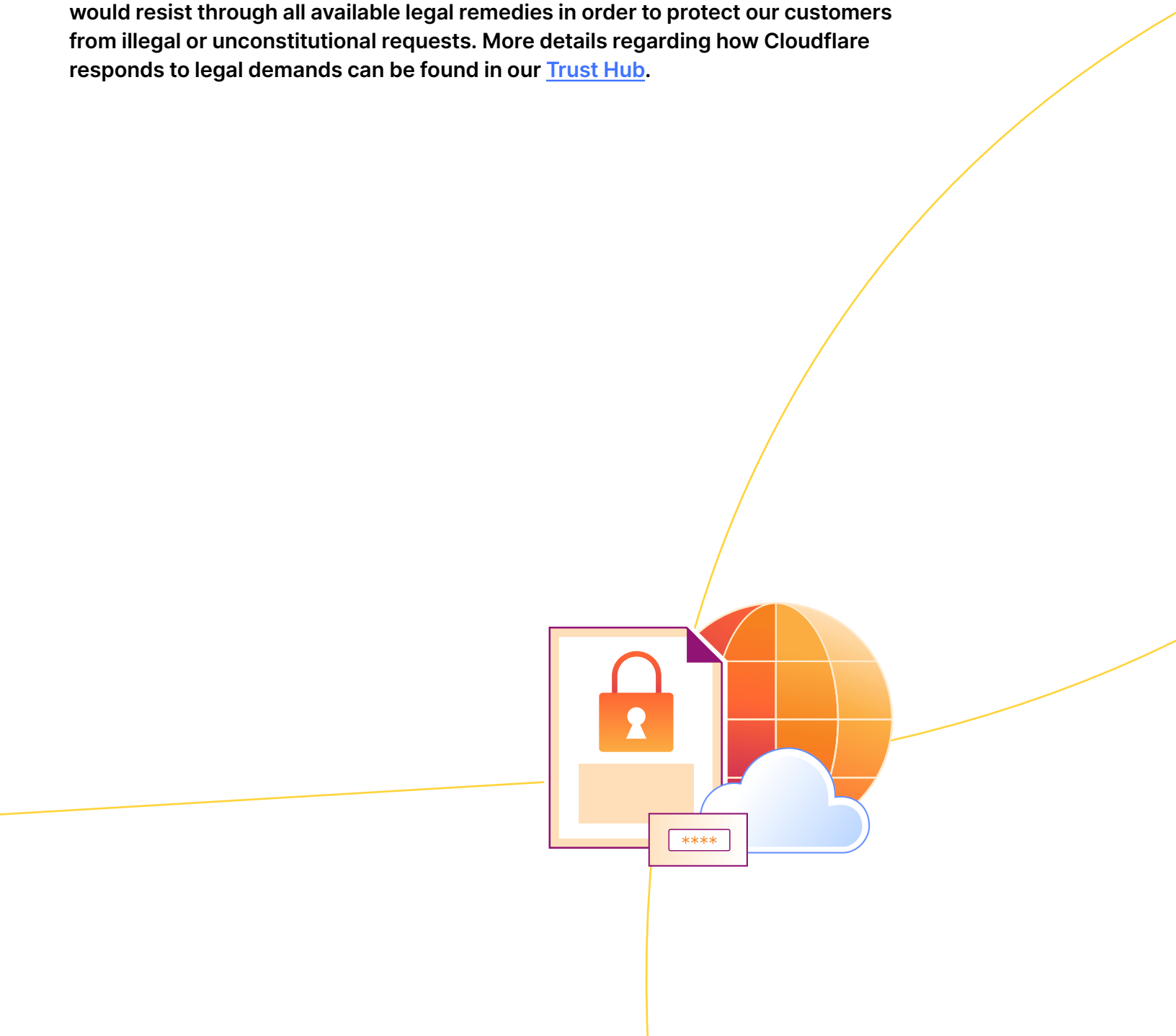
H2 2025 – Legal requests for information

Cloudflare Transparency Report

Legal requests for information

An essential part of learning and maintaining the trust of our customers is being transparent about the legal requests for customer information that we receive from government entities and private parties. To this end, and consistent with the transparency reporting obligations under the European Union's (EU) Digital Services Act, Cloudflare publishes semi-annual updates to our Transparency Report on the requests we have received to disclose information about our customers.

We list in our Transparency Center some things that Cloudflare has never done and would resist through all available legal remedies in order to protect our customers from illegal or unconstitutional requests. More details regarding how Cloudflare responds to legal demands can be found in our Trust Hub.



Content

Our guiding principles

Require due process

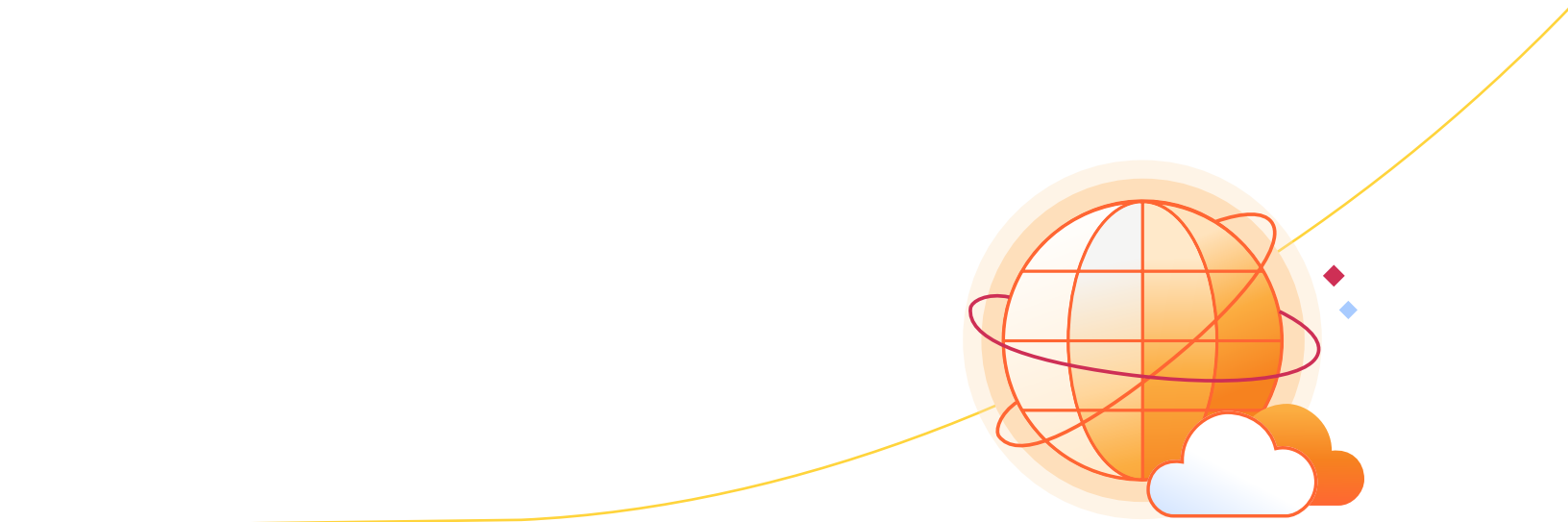
Before producing customer data, we require that all law enforcement, government, or third-party requests we receive adhere to the due process of law and are subject to appropriate judicial oversight.

Respect privacy

It is Cloudflare's overriding privacy principle that any personal information provided to us by our customers is just that: personal and private. Our respect for our customers' privacy applies with equal force to requests from law enforcement, government, or private third parties.

Provide notice

Unless legally prohibited, it is our policy to notify our customers of any legal request where we may produce their information, whether it comes from law enforcement, government, or private third parties.



Background on requests for customer information

Cloudflare receives requests for different kinds of data on its users from governments, courts, and private parties around the world. To provide transparency about the information Cloudflare might provide in response to these requests, 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, and we take steps to ensure the request is consistent with the human rights principles in Cloudflare's Human Rights Policy. 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.

The data

As a company headquartered in the United States, Cloudflare follows U.S. law, in particular the Electronic Communications Privacy Act (ECPA), in determining what constitutes valid legal process. In particular, U.S. law differentiates between requests for "basic subscriber information" that can be used to identify a subscriber, other "non-content data" about a subscriber or their website, and "content data" including email or other types of customer-generated material.

Requests for basic subscriber information

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 log in to the account.

Unless there is an emergency disclosure request (as contemplated by 18 U.S.C. § 2702), 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 criminal subpoenas

The U.S. government can compel disclosure of subscriber information in connection with a criminal investigation using legal process with judicial oversight, including, but not limited to, grand jury subpoenas, U.S. government attorney-issued subpoenas, and case agent issued summonses. This category includes federal requests issued in the course of the investigations of certain crimes under 18 U.S.C. § 3486, which may be accompanied by court-issued non-disclosure orders.

Year	Received	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H2 2025	336	54%	65%	565	5,193
H1 2025	354	61%	62%	431	1,063

U.S. government administrative subpoenas and civil investigative demands

In addition, the U.S. government can require disclosure of certain basic subscriber information using legal process issued directly by a U.S. federal or state government agency without judicial oversight, such as administrative subpoenas and civil investigative demands. Examples include subpoenas issued by the Securities and Exchange Commission and the Federal Trade Commission, as well as state-issued equivalents.

Year	Received	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H2 2025	4	75%	0%	45	78
H1 2025	10	40%	0%	10	10

U.S. private third-party civil subpoenas

Private third parties can seek subscriber information in the United States using civil subpoenas. This category includes subpoenas issued pursuant to the Digital Millennium Copyright Act (DMCA) regarding users or websites alleged to be infringing copyright.

Year	Received	% where some data was produced	Accounts affected	Domains affected
H2 2025	56	71%	342	404
H1 2025	45	71%	2,013	1,840

Non-U.S. demands from private party requests

Countries outside the United States may have legal regimes that enable civil litigants to seek customer information. Although Cloudflare has generally required civil litigants outside of the United States to direct legal requests for customer information through U.S. courts, we have produced basic subscriber information in response to these non-U.S. legal orders in limited circumstances. Cloudflare evaluates its legal obligations with respect to these demands based on its presence in the country, as well as whether the applicable request satisfies due process, transparency requirements, and consistency with internationally recognized standards. The table below details the non-U.S. court orders seeking customer information to which Cloudflare has responded.

Year	Country	Received	% where user data was produced	% accompanying non-disclosure order	Accounts affected
H2 2025	Japan	41	29%	0%	16
H1 2025	Japan	20	40%	0%	16

WHOIS data disclosures

As an ICANN-accredited domain registrar, Cloudflare follows ICANN's WHOIS data disclosure requirements by providing WHOIS records for Cloudflare's Registrar customers in response to requests from legitimate access seekers.

Year	Received	% where some data was produced	Domains affected
H2 2025	13	100%	13
H1 2025	20	100%	20

Requests for other non-content data

Beyond requests solely 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 a customer's account activities or the IP addresses visiting a customer's website, as well as basic subscriber data. The court orders that Cloudflare receives typically include a temporary non-disclosure requirement. Because Cloudflare retains such transactional data for only a limited period of time, Cloudflare rarely has responsive data to provide to such requests.

U.S. criminal court orders

This category includes any order issued by a judge, including, but not limited to, 18 U.S.C. § 2703(d). 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	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H2 2025	70	76%	90%	184	2,374
H1 2025	46	70%	85%	140	189

Requests from non-U.S. law enforcement and government agencies

Cloudflare typically directs non-U.S. governments to route their requests to the U.S. government pursuant to a Mutual Legal Assistance Treaty (MLAT). Our reporting on the U.S. legal process above includes requests issued by the United States on behalf of a non-U.S. government pursuant to MLAT. To provide additional granularity, the table below shows those legal demands from a foreign government that were issued through the MLAT process.

MLAT requests

Year	Country	Received	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H2 2025	Peru	2	69%	93%	1	1
	Poland	6			1	1
	North Macedonia	2			1	1
	Republic of Korea	4			6	6
	Romania	1			1	2
	Malta	1			1	1
	Spain	1			2	2
	Ireland	2			2	2
	Switzerland	2			1	3
	Belgium	1			0	0
	Paraguay	1			0	0
	Bulgaria	1			1	1
	Slovakia	1			0	0
	Sweden	1			0	0
	Austria	3			3	2
Total requests		**29**				

Additional context

In H2 2025, we received a number of U.S.-issued MLAT requests on behalf of a foreign country containing identifiers that were not using Cloudflare services, or targeting invalid identifiers such as IP addresses or end-users that accessed websites using Cloudflare services. We thus had no data to produce in response to those requests, contributing to the decrease in “percentage where some data was produced” in the table above.

Year	Country	Received	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H1 2025	Sweden	5	96%	96%	4	5
	Netherlands	2			6	7
	Italy	1			61	61
	Greece	1			1	1
	Poland	5			8	13
	South Korea	4			3	22
	Germany	1			2	2
	Slovenia	1			1	1
	Bulgaria	1			1	1
	Switzerland	1			1	1
	Georgia	1			1	1
	Brazil	1			1	1
	Malta	1			1	0
Total requests		**25**				

Pen register trap and trace orders

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

Year	Received	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H2 2025	50	96%	100%	92	107
H1 2025	26	88%	100%	43	45

Additional context
While the table above shows an increase in the number of PRTT orders received, this includes extensions to PRTT orders that relate to the same domains as in the initial order.

Requests for content data

Due to the nature of Cloudflare's services, in the vast majority of requests for content data (like email or other types of customer-generated material), Cloudflare has no data to provide in response. In the rare cases where Cloudflare stores or hosts content data and has responsive data, we require a search warrant consistent with the principles laid out in *U.S. v. Warshak*. Search warrants require judicial review, probable cause, inclusion of a location to be searched, and a detail of items requested.

For more information regarding our approach to requests seeking content, visit our Trust Hub.

Search warrants relating to pass-through services

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

Year	Received	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H2 2025	36	47%	33%	23	25
H1 2025	32	56%	50%	74	88

Search warrants relating to stored content

While the vast majority of legal requests Cloudflare receives relate to services that do not store customer content, a number of Cloudflare's developer products do involve storage services that may store customer content. Cloudflare requires a search warrant before providing stored customer content to law enforcement.

Year	Received	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H2 2025	1	100%	100%	1	2
H1 2025	1	100%	100%	1	1

Wiretap orders

A Title III Wiretap 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.

Year	Received	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H2 2025	0	0	0	0	0
H1 2025	0	0	0	0	0

Other requests for data

Certain other types of legal requests may be used under U.S. law to seek either non-content or content data. Information related to these requests is reported below.

U.S. national security process

The U.S. government has a number of legal mechanisms to obtain content and non-content data from service providers in relation to foreign intelligence investigations. The U.S. government can issue National Security Letters (NSLs), which are similar to subpoenas, for a customer's basic subscriber information such as name, address, and length of service. The Foreign Intelligence Surveillance Act (FISA) provides authorities for the government to request both the content of users' communications and non-content data, with orders or oversight from the Foreign Intelligence Surveillance Court. What we can say about either FISA court orders or NSLs that we receive is highly regulated and depends on exactly how we report the information.

If Cloudflare were to receive an NSL or order, it would be reported as part of a combined number of NSLs and FISA orders in a band of 250, beginning with 0-250, and would be subject to a six-month delay in reporting.

Year	Received (0-249)	Answered (0-249)
H2 2025	0-249	0-249
H1 2025	0-249	0-249

Requests made pursuant to the CLOUD Act

Cloudflare will comply with appropriately scoped and targeted requests from countries that have entered into CLOUD Act agreements with the United States. Cloudflare has no data to report regarding such requests at this time.

Emergency disclosure requests

Cloudflare receives emergency requests for data from law enforcement and government agencies. In accordance with 18 U.S. Code § 2702, Cloudflare will respond on a voluntary basis to an emergency disclosure request if we have a good faith belief that there is an emergency involving the danger of death or serious physical injury and that disclosure of information will help avert the threat. In those cases, we request that law enforcement provide additional information regarding the emergency and obtain legal process when time permits, and we typically disclose only basic subscriber information.

Year	Received	% where some data was produced	% accompanying non-disclosure order	Accounts affected	Domains affected
H2 2025	44	7%	0	6	5
H1 2025	48	0%	0	0	0

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 semi-annual basis.

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-7971.2026FEB26