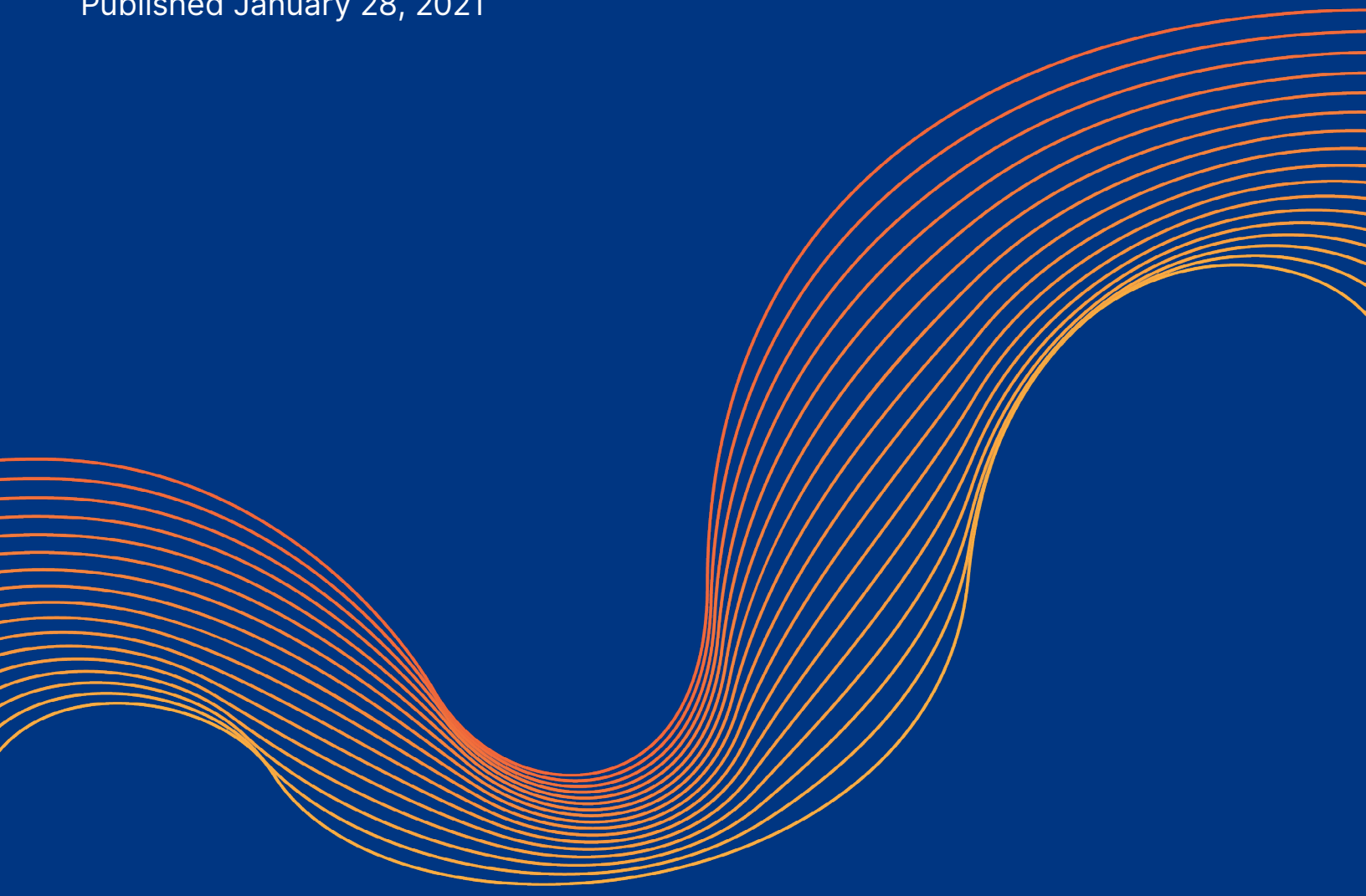
WHITEPAPER

CLOUDFLARE

Cloudflare's policies around data privacy and law enforcement requests

Published January 28, 2021



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

Cloudflare's network and business are all ultimately built on customer trust. We seek to continually earn and maintain that trust by building and deploying products that help improve the security of our system, encrypt data at rest or in transit, and allow our customers to determine how traffic is inspected across different locations around the world.

But not all challenges can be solved with engineering. For this reason, we also have policies and procedures that guide how we manage customer and end-user data on our systems — and how we address government and other legal requests for data.

This paper outlines these policies and provides links to more detailed information about various facets of our approach to data privacy and compliance. Specifically, it covers:

- Our view on the changing data privacy landscape
- Our policies around data privacy and data requests

The changing data privacy landscape

The explosion of cloud services — and the fact that data may be stored outside the countries of residence of those who generated it — has been a challenge for governments conducting law enforcement investigations. Online service providers of all kinds often serve as an access point for those electronic records.

For service providers like Cloudflare, government requests for data can be fraught. The work law enforcement and other government authorities do is important. At the same time, the data law enforcement and other government authorities are seeking from us does not belong to us. By using our services, our customers have put us in a position of trust over that data. Maintaining that trust is fundamental to our business and our values.

These tensions are compounded by the fact that different governments have different standards for the protection of personal data. The United States, for example, prohibits companies from disclosing the content of communications — including to non-U.S. governments — in all but certain legally defined circumstances. The European Union, which has long considered privacy to be a fundamental human right, protects all EU personal data through the General Data Protection Regulation (GDPR). Although these protections overlap in certain respects, they differ both in their scope and whom they protect.

The differences between legal frameworks matter, particularly when it comes to whether legal requests for information from foreign governments are determined to be consistent with privacy requirements. In recent years, for example, the Court of Justice of the European Union (CJEU) has concluded on multiple occasions that U.S. legal restrictions on gathering data, along with certain voluntary commitments like the Privacy Shield (or its predecessor, the U.S.-EU Safe Harbor) are not adequate to comply with EU privacy requirements, largely because of U.S. laws that allow legal authorities to collect information on non-U.S. citizens for foreign intelligence purposes. Indeed, the European Data Protection Board (EDPB) has taken the position that a U.S. criminal law request for data — outside of a legal process in which countries in the EU maintain some control over the information being produced — is not a legitimate basis for the transfer of personal data subject to GDPR.

At heart, these are fights over when it is appropriate for one government to use legal orders or other legal processes to access data about another country's citizens. And these are not just fights happening in Europe. Although their policy responses are not consistent, an increasing number of countries now see access to their citizens' data as a national security concern.

Cloudflare's policies around data privacy and data requests

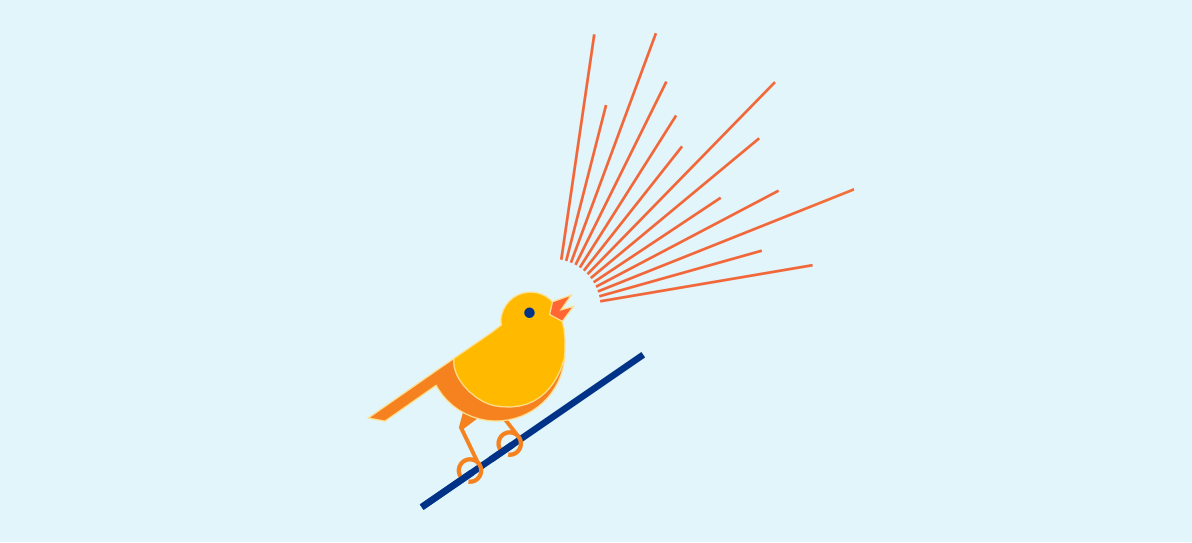
Cloudflare has long maintained policies to address concerns about access to personal data. We've done so both because we believe it's the right thing to do and because the conflicts of law we are seeing today seemed inevitable. These policies cover:

- Public commitments on how we treat private data and how we handle law enforcement requests for that data
- How we inform our customers about data requests.

In general, when there is a conflict between two different legal standards, we default to the one that is most privacy-protective. And we always require legal process. Because once you have opened the gate to data, it can be difficult to close.

Our public commitments around private data and law enforcement requests

Beginning with our very first transparency report detailing law enforcement requests for data in 2013, we've made public commitments about how we approach requests for data and public statements about things we have never done. We call the public statements about things we have never done warrant 'canaries', with the idea that they serve a signaling function to the outside world.



These 'canaries' serve two functions. First, they are a public statement that we would not take these actions willingly. Second, they can be a mechanism to convey information — by removal of the statement from the site — that we might otherwise be restricted from disclosing.

Regulatory entities have started to recognize the value of privacy commitments, particularly when they can be enforced by contract. Indeed, the commitments we have included in our transparency reports for years are exactly the types of commitments the European Commission has recommended be included in its draft Standard Contractual Clauses for compliance with the GDPR.

Key examples of our commitments at this paper's date of publication include:

- **We have never installed law enforcement software or equipment on our network, or provided a feed of content transiting our network:** As a security company, we know that maintaining control over access to our networks is an absolute imperative. That is why our security team has focused on access controls, logging, and monitoring, and undergoes multiple third-party assessments per year. We want to ensure that our customers understand that there is no exemption in those controls for law enforcement or government actors. That's why we state both that Cloudflare has never installed law enforcement software or equipment anywhere on our network, and that we have never provided any government organization a feed of our customers' content transiting our network.
- **We have never shared encryption of authentication keys:** Cloudflare believes that strong encryption — both for content and metadata — is necessary for privacy online. If a country is seeking to prevent another government from accessing its citizens' personal information, the first step should be encryption of that personal information. But customers and regulators also need to be confident that the encryption itself is trustworthy. So we have commitments that we have never turned over our encryption or authentication keys — or our customers' encryption or authentication keys — to anyone, and that we have never weakened, compromised, or subverted our encryption at the request of law enforcement or any other third party.
- **We have never modified customer content or DNS requests:** We do not believe that our systems should be exploited to lead people to sites that they did not intend to visit or to alter the content they get online. Therefore, we've publicly stated that we have never modified customer content or modified the intended destination of DNS responses at the request of law enforcement or another third party.
- **Transparency around potential commitment breaks:** We've committed to challenge any legal order seeking to have us break these commitments, in court if necessary. Our goal was to be very clear — not only to our customers but to governments around the world — about where we were drawing our lines.

While our overall philosophy around data protection has remained unchanged since our founding, we occasionally adapt our commitments to reflect the latest changes in our products and the policy landscape. A definitive, up-to-date list of those commitments is available on our Transparency Report page.

Providing Our Customers with Notice of Government Requests

Cloudflare has long believed that our customers deserve notice when anyone — including a law enforcement agency or other government actor — uses legal process to request their data. That notice allows our customers to challenge the request if they have concerns.

Indeed, we have had a policy of providing notice to our customers since our earliest days as a company. In January 2013, when we had less than 30 employees, the FBI showed up at our door with a National Security Letter requesting information on a customer and forbidding us from discussing it with anyone other than our attorneys. At the time, National Security Letters had almost no oversight, could be written and enforced by a single branch of the US government, and gagged recipients from talking about them indefinitely.

We recognize that there might be some circumstances in which it might be appropriate for law enforcement to temporarily restrict disclosure to preserve the viability of an investigation. However, we also believe that the government should be required to justify any non-disclosure provision, and that any non-disclosure provision should be explicitly time-limited to the minimum time necessary for the purpose at hand. As such, we worked with the Electronic Frontier Foundation on a legal challenge to the letter.

The resulting court case lasted for several years, and we were gagged from talking about it until 2017. But ultimately, the FBI withdrew the letter.

Because U.S. courts have suggested that indefinite non-disclosure orders raise constitutional problems, the U.S. Department of Justice issued guidance in 2017 instructing federal prosecutors to limit non-disclosure orders to no longer than a year, except in exceptional circumstances. That has not, however, stopped all U.S. law enforcement from seeking indefinite non-disclosure orders. As of this paper's date of publishing, we have received at least 28 non-disclosure orders since 2017 that did not include an end date. Working with the American Civil Liberties Union (ACLU), Cloudflare has threatened litigation when we have received such indefinite non-disclosure orders. In each case, the government has subsequently inserted time limits on the non-disclosure requirements in those orders, allowing us to provide our customers notice of the requests.

Addressing Conflicts of Law

Maintaining compliance with laws like GDPR, particularly in the face of legal orders that might put us in the difficult position of being required to violate it, requires involving the courts. A service provider like Cloudflare can ask a court to quash legal requests because of a conflict of law, and we have committed, both in our public statements, and contractually in our Data Processing Addendum, that we would take that step if necessary to avoid such a conflict. Our view is that the conflict should be pushed back where it belongs — between the two governments that are fighting over who should be entitled to access information.

Conclusion

This article is just an introduction to our broad, deep commitments to data privacy. For more information on those commitment, check out:

- **Our overall privacy policy:** Covering what data we collect, how we use it, what data we share, and other common privacy questions.
- **Our transparency report:** Up-to-date information on legal requests we have received to disclose information about our customers.
- **Our data privacy & compliance homepage:** The latest announcements about how our policies and products support privacy and compliance needs.

Ultimately, running a global network that protects customer and end-user data — and complies with different privacy laws around the world — requires coming back to the values that we have championed since our earliest days as a company: be principled and transparent, respect privacy, require due process, and provide customers with notice so that they can make their own decisions about their data.