Report

Fastly Transparency Report

August 1, 2024 to December 31, 2024

fastly

Introduction

Fastly, Inc. (“Fastly” or “we”) is committed to protecting the privacy, confidentiality, and integrity of our customers’ data. This transparency report provides general information about the law enforcement authority and government agency requests that we receive for this data and how we address those requests.

Originally designed to accelerate applications and services at global scale through our content delivery services, our platform has since evolved to support cloud-native architectures, edge computing, unified application security, and emerging AI workloads. While our service offerings have expanded, Fastly is not a traditional hosting provider. Consequently, we are often unlikely to have in our possession data that law enforcement authorities and government agencies may request.

Any request from a law enforcement authority or government agency for information from Fastly is handled in accordance with our **Law Enforcement Guidelines**, which we provide to the requesting party. Absent emergency circumstances (for example, those involving danger of death or serious physical harm), Fastly will not disclose customer information or content to law enforcement authorities or government agencies unless properly served with a valid and binding legal demand that compels Fastly to produce the requested information. Where reasonable, we will object to overbroad or otherwise inappropriate demands.

This report also provides information consistent with our obligations under Article 15 of the European Union’s Digital Services Act, Regulation (EU) 2022/2065 (the “DSA”). Data on Member State Authority requests applicable to Fastly’s services may be duplicative of data provided in the general **Requests Received by Country** section of this report. See the section titled **Digital Services Act Reporting** below for more information.

Inclusion of information in this report is subject to applicable nondisclosure requirements or orders to which Fastly may be subject.

If you have any questions about this report please contact support@fastly.com

1. Information and Request Types

Information about the types of law enforcement authority and government agency requests Fastly typically receives and the types of information requested is below.

Except as specified in the **Digital Services Act Reporting** section, this report only includes data on the request types covered in this section . Fastly did not provide “Customer Information” or “Customer Content” in response to any request type not included in this section.

Information Types

Customer Information

Customer Information includes customer names, contact information, services purchased, and billing information. It may also include login information, usage history, domain ownership, and other basic information about our customers’ use of our services. Customer Information does not include Customer Content. Customer-designated abuse contact information is also not included in this report as Customer Information. As an intermediary, when we receive requests for Customer Information, we provide a customer-designated abuse contact to the requesting agency or authority (in accordance with Section 4.4 of our **terms of service**) so our customers can resolve the request directly.

Customer Content

Customer Content includes customer data submitted to or caused to be submitted to our services by our customers or their end users. This may include end user IP addresses or other transactional information processed by a customer’s application or website. As an intermediary, when we receive requests for Customer Content, we provide a customer-designated abuse contact to the requesting agency or authority (in accordance with Section 4.4 of our **terms of service**) so our customers can resolve the request directly.

Request Types

Subpoenas and Court Orders

Where compelled by law, Fastly will disclose Customer Information in response to valid and binding subpoenas and court orders. Fastly will only provide Customer Content in response to a subpoena or court order where legally required to do so. When reasonable, Fastly will take steps to challenge subpoenas and court orders.

Search Warrants

Fastly will only produce Customer Content when served with a valid search warrant issued under procedures set forth in the Federal Rules of Criminal Procedure and the United States Constitution or equivalent procedures that compels Fastly to produce such information. Where reasonable, Fastly will take steps to challenge search warrants.

Emergency Requests

Customer Information and Customer Content are occasionally requested by law enforcement on an emergency basis, where danger of death or serious physical harm requires disclosure without delay. Fastly evaluates and responds to such requests in accordance with our **Law Enforcement Guidelines**.

Preservation Requests

Fastly will preserve Customer Information and, in rare cases where Fastly could be considered a content host, Customer Content pursuant to a valid request for preservation in accordance with our **Law Enforcement Guidelines**.

Request Types Continued

International Requests

Fastly only responds to law enforcement requests from outside of the United States where issued pursuant to applicable laws and through official channels such as, a Mutual Legal Assistance Treaty request, a request from a country meeting the obligations under the CLOUD Act, or letters rogatory.

Wiretap, Pen Register, Trap and Trace

Fastly did not disclose Customer Information or Customer Content in response to this type of request during the period of this report, and any such requests are not included in the reporting below. Fastly evaluates and responds to such requests in accordance with our **Law Enforcement Guidelines**.

United States National Security Requests

If Fastly were to receive a Foreign Intelligence Service Court (FISA) order or National Security Letter, it could be compelled to disclose Customer Information or Customer Content. FISA orders and National Security Letters are subject to additional disclosure and reporting requirements and detailed information about such requests is excluded from this Transparency Report. However, the reportable number of such requests received by Fastly during the period of this report is between 0 and 250, the lowest reportable band.

2. Requests Received by Country

Information about the law enforcement authority and government agency requests covered by this report and received from August 1, 2024, to December 31, 2024, is below. Request types are consolidated for each applicable country with reportable data.

Fastly only shares “Customer Information” and “Customer Content” with law enforcement authorities or government agencies subject to a valid and binding legal demand and will work to minimize or reduce the scope of any such disclosure where possible.

Requests Received by Country

Country	Requests for Customer Information	Disclosures of Customer Information by Fastly	Requests for Customer Content	Disclosures of Customer Content by Fastly
Germany	1	0	0	0
United States	5	1	0	0
Total	**6**	**1**	**0**	**0**

3. Digital Services Act Reporting

In compliance with Article 15 of the DSA, this Transparency Report provides an overview of our content moderation activities and required reporting.

Originally designed to accelerate applications and services at global scale through our content delivery services, our platform has since evolved to support cloud-native architectures, edge computing, unified application security, and emerging AI workloads. While our service offerings have expanded, Fastly is not a traditional hosting provider. Consequently, we are unable to remove content hosted by our customers, and reports regarding content cached by our services should be sent directly to our customers.

Fastly qualifies as an intermediary service provider under the DSA. Fastly's services primarily include "caching" services as defined in the DSA. Shortly prior to the period of this report, Fastly also began providing services that may be considered "hosting" services under the DSA. These services are included in the report, but Fastly received no applicable (i) requests from Member State Authorities (as defined under the DSA), or (ii) notices for "illegal" content based on the mechanisms provided by Fastly for third party notices during the period covered by this report.

As a caching and hosting provider under the DSA, Fastly is not required to engage in content moderation at its own initiative. Any content moderation Fastly undertakes is in response to valid notices received in accordance with our **US Digital Millennium Copyright Act And EU Digital Services Act Compliance And Reporting Guidelines** or pursuant to a Member State Authority order.

Orders Received from Member State Authorities

Information about the Member State Authority orders covered by this report and received from August 1, 2024, to December 31, 2024, is below.

Member State	Totals
Germany	1
Total	**1**

Third Party Notices Regarding “Illegal” Content

Fastly received 0 notices submitted in accordance with Article 16 of the DSA applicable to hosting services during the period of this report.

Content Moderation Engaged in at Fastly’s Own Initiative

Fastly does not engage in content moderation at its own initiative.

Internal Complaint-Handling Systems

Fastly does not engage in content moderation at its own initiative and processed 0 complaints through an internal complaint-handling system during the period of this report.

Automated Means for Content Moderation

Fastly uses a third-party tool to help process notices about alleged illegal content. This tool is integrated into Fastly’s notice and action mechanism to (i) help categorize incoming notices from Fastly’s abuse email alias and webform, (ii) create tickets, (iii) serve automated responses, and (iv) record actions taken by Fastly’s content response team. Our notice and action mechanism and associated processes are manually overseen by our content response team.

Unless it is reasonably apparent to us that our customer has already received a notice regarding particular content or there are other applicable privacy or legal concerns, we will forward all the information provided in the notice, including contact information, to our customer pursuant to Section 4 of our **Terms of Service**.

Generally, the decision to take down the alleged illegal content is made by our customer except where, given the nature of the notice, Fastly determines intervention or additional steps are required (e.g. CSAM).