

EXHIBIT 11

[← Back to Reports](#)

Integrity Reports, First Quarter 2024

UPDATED DEC 4, 2024

We're publishing our first quarter reports for 2024, including the [Community Standards Enforcement Report](#), [Adversarial Threat Report](#), [Widely Viewed Content Report](#), the [Government Requests for User Data](#) and [Content Restrictions Based on Local Law](#) for the second half of 2023 and the [Intellectual Property Transparency Report](#) for 2023. All of the reports are available on our [Transparency Center](#).

Some report highlights include:

Community Standards Enforcement Report

- Prevalence of violating content remained relatively consistent across a wide range of violation areas. Prevalence of violating content is estimated using samples of content views from across Facebook or Instagram. We [fixed](#) a bug where a small amount of irrelevant data was sampled, which has been resolved and did not result in any significant change to prevalence.
- An increase in actioned content for Violence and Incitement on Instagram due to updates to our detection technology that improved identification of hostile speech.
- A decrease in the prevalence of Violent and Graphic Content on Instagram to prior levels after a spike due to world events in Q4 2023.
- A decrease in prevalence for Adult Nudity and Sexual Activity on Instagram after rectifying a loophole by which bad actors were able to evade detection.
- An increase in actioned content for Child Endangerment and Sexual Exploitation (CSAM) on Instagram resulting from technology improvements to address spammy CSAM comments.
- An increase in actioned content for Suicide and Self Injury on Instagram due to accuracy improvements in our detection technology.

In Q4, we continue to make progress on removing content that violates our Community Standards with prevalence remaining relatively consistent across most areas. In addition:

You can read the full report [here](#).

Adversarial Threat Report

In our Q1 Adversarial Threat report, we're sharing threat research into six new covert influence operations that we've disrupted around the world, including in Bangladesh, China, Croatia, Iran, Israel, and an unknown origin CIB network that targeted Moldova and Madagascar. Many of these cross-internet campaigns were detected and removed early in their audience building efforts. In addition, we're including our latest findings into a long running covert influence operation from Russia, known as Doppelganger. Finally, as part of our mid-year update on the global threat landscape, we're sharing some key insights that stood out to us in our threat research to date. This threat research helps inform our defenses as we work to protect public debate globally this year, including ahead of its many elections. You can read the full report [here](#).

Government Requests for User Data

During the second half of 2023, global government requests for user data increased 11% from 271,692 to 301,553. US requests declined, while India became the top requester, with a growth of 30% increase in requests, followed by Brazil, Germany and France.

In the US, we've received 73,390 requests– a decrease of 0.7% – from the first half of 2023, which includes non-disclosure orders prohibiting Meta from notifying the user 74.5% of the time. Emergency requests accounted for 5.7% of the total request in the US, remaining steady from the first half of 2023.

Additionally, as a result of transparency updates introduced in the 2016 USA Freedom Act, the US government lifted non-disclosure orders on 9 National Security Letters, which we received between 2019 and 2021. These requests, along with the US government's authorization letters, are available [here](#).

Further, based on a regular review of our reporting processes, we have made adjustments to our reporting of Foreign Intelligence Surveillance Act (FISA) content requests from three prior cycles. Specifically, the reported range of reports from H2 2022 has been made more precise (from 145,000-149,999 to 146,000-146,499); the range of reports from H1 2022 has been reduced (from 145,000-149,999 to 135,500-135,999); and the range of reports for H1 2021 has been increased (from 125,000-125,499 to 128,500 to 128,999). We continually review our processes and protocols to help ensure the accuracy of our reporting.

As we have said in prior reports, we scrutinize every government request we receive to make sure it is legally valid, no matter which government makes the request. We comply with government requests for user information where we have a good-faith belief that the law requires us to do so. In addition, we assess whether a request is consistent with internationally recognized standards on human rights, including due process, privacy, free expression and the rule of law. When we do comply, we produce information that is narrowly tailored to that request. If we determine that a request appears to be deficient or overly broad, we push back

and will fight in court, if necessary. We do not provide governments with “back doors” to people’s information. For more information about how we review and respond to government requests for user data and the safeguards we apply, please refer to our FAQs.

You can read more on requests made from H2 2023 [here](#).

Content Restrictions Based on Local Law

For many years, we’ve published biannual transparency reports, which include the volume of content restrictions we make when content is reported as violating local law but doesn’t go against our Community Standards. This report includes information where in limited countries we are obligated to automatically restrict content, at scale and in country, based on local law requirements, which is reflected in the comparatively higher volumes of content restrictions.

During this reporting period, the volume of content restrictions based on local law for Facebook and Instagram increased globally from 200,000 in H1 2023 to 48,000,000 in H2 2023, driven by obligations in Indonesia where over 47 million items were restricted under the Electronic Information and Transactions (EIT) Law and KOMINFO Regulation 5/2020 on Private Electronic Services Operator for gambling content.

In addition, based on a regular review of our reporting processes, we have also added instances where we restricted access to content to comply with court orders and requests under the European Union’s General Data Protection Regulation as well as in South Korea where we are obligated to automatically restrict content, at scale and in country, under the Telecommunications Business Act for illegally filmed sexual content.

We continually review our processes and protocols to help ensure the accuracy of our reporting. You can read more [here](#).

Intellectual Property

We report on the volume and nature of copyright, trademark and counterfeit reports we receive each year as well as our proactive actions against potential piracy and counterfeits. In 2023, we saw an increase in reports of intellectual property infringement, much of which was attributable to fraudulent reports impersonating legitimate rights owners; we announced [new resources](#) for brands to protect against fraudulent reporting earlier this year, and expect to see the impact of those efforts in future transparency reports.

We’ve also improved our transparency reporting by adding more metrics like ads takedowns based on reports we received, as well as proactive actions — the former of which was previously included in the overall Facebook and Instagram enforcement volumes but is now broken out separately for the first time. Finally, we saw a decrease in proactive counterfeit

enforcement volumes, driven mainly by improvements in the precision of our enforcement measures and the previously mentioned addition of new ads metrics.

We are committed to helping businesses and people protect their intellectual property rights. Our IP Report outlines that in 2023, we took down:

- 14,092,779 pieces of content based on 7,034,447 copyright reports
- 2,463,444 pieces of content based on 2,035,439 trademark reports
- 3,912,603 pieces of content based on 622,057 counterfeit reports

You can read more [here](#).

NCMEC Cybertips

As part of our ongoing work to provide young people with safe, positive online experiences, we're continuing to provide more transparency into our efforts to find and report child exploitation to the National Center for Missing and Exploited Children (NCMEC). We began sharing this data last year.

In Q1 2024, we reported the following number of CyberTips to NCMEC from Facebook and Instagram:

- Facebook and Instagram sent over **5.2 million NCMEC Cybertip Reports** for child sexual exploitation.
 - Of these reports, over **90 thousand** involved inappropriate interactions with children. CyberTips relating to inappropriate interactions with children may include an adult soliciting child sexual abuse material (CSAM) directly from a minor or attempting to meet and cause harm to a child in person. These CyberTips also include cases where a child is in apparent imminent danger.
 - Over **5.1 million** reports related to shared or re-shared photos and videos that contain CSAM.

Other Integrity Updates

- **"Made with AI" labels on organic media:** We think it's important to help people navigate AI and help them know when realistic content they're seeing has been created using AI, especially right now when people are often coming across AI-generated content for the first time. Earlier this month, we began [adding](#) "Made with AI" to certain AI-generated images, video, and audio that are posted organically on Facebook, Instagram, and Threads. We are able to add these labels when we detect industry standard AI image indicators or when people disclose that they're uploading AI-generated content. For images created with Meta AI, we already have visible and invisible watermarks to help people identify them. In certain cases, we also [require](#) advertisers to disclose when they digitally create or alter a political or

social issue ad using third-party GenAI tools. We are engaging with stakeholders to develop a transparency approach around generative AI use in ads.

- US2020 Research Paper: In May the research journal PNAS [published](#) the fifth [paper](#) in our groundbreaking US 2020 Facebook and Instagram Election Study [project](#) with external academics. This paper examined the effect of Facebook and Instagram users deactivating the platforms in the weeks leading up to the US2020 election, similar to a study [previously published](#) by the lead academic authors Matthew Gentzkow and Hunt Allcott in 2020. The findings were consistent with previous publications in showing “close to zero” effect on key political attitudes, beliefs or behaviors during that time period. The project’s foundational data is [archived](#) and available for other researchers to run their own analysis and check the validity of the findings.



Policies



Community Standards

Meta Advertising Standards

Other policies

How Meta improves

Age-Appropriate Content

Features



Research tools



Enforcement



Governance



Security



Reports



[English \(US\)](#)

[Privacy Policy](#)

[Terms of Service](#)

[Cookies](#)