

Congress of the United States

Washington, DC 20515

December 9, 2025

Mr. Mark Zuckerberg
Chairman and Chief Executive Officer
Meta Platforms, Inc.
1 Hacker Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg,

We write to express our serious concerns regarding recently published research revealing Meta's use of a technical loophole to deliberately circumvent users' privacy choices and track users on the Android platform. We seek clarity on how Meta will locate and permanently delete data collected through this practice and what changes Meta will implement in its internal decision-making processes to prevent future privacy violations that override users' explicit intentions and expectations.

Unbeknownst to Meta's users, Meta's new tracking method followed them across the web even if the user tried to keep their browsing private. In May 2025, researchers revealed that Meta had been abusing Android features intended exclusively for testing and development to dismantle long-standing security protections built into the mobile operating system.¹ By exploiting these features, Meta enabled its apps, like Facebook and Instagram, to covertly surveil users' behavior on websites embedding the Meta Pixel, which appears on more than 20% of all websites.² Each time a user visited one of these sites, the Pixel would quietly initiate a covert connection to Meta's apps.³ This allowed Meta to link ephemeral web browsing behavior directly with a user's Meta account regardless of a user's intent or privacy choices. Even users who had chosen every available safeguard—opting out of cookies, using a VPN, or enabling incognito mode—were still tracked against their will, as Meta continued to listen through these hidden channels.

Not only does this practice thwart a user's privacy choices, but it also bypasses a core industry standard designed to protect phone users' security and privacy by preventing apps from accessing

¹ "Research Co-Led by IMDEA Networks Discovers a Privacy Abuse Involving Meta and Yandex Bridging Persistent Identifiers to Browsing Histories." *IMDEA Networks Institute*, 16 May 2025, <https://networks.imdea.org/research-co-led-by-imdea-networks-discovers-a-privacy-abuse-involving-meta-and-yandex-bridging-persistent-identifiers-to-browsing-histories>.

² Traverso, Samuele, et al. "The Hitchhiker's Guide to Facebook Web Tracking with Invisible Pixels and Click IDs." *Proceedings of the ACM Web Conference 2023*, 30 Apr. 2023, <https://dl.acm.org/doi/fullHtml/10.1145/3543507.3583311>.

³ LocalMess. "Meta and Yandex Found Bypassing Sandboxing with Localhost Pixel Snooping." *GitHub Pages*, May 2025, <https://localmess.github.io/>.

each other's data.⁴ Meta's decision to circumvent this boundary reflects a deliberate effort to deceive users who believed themselves protected by their phone's security standards or their own privacy choices. It also puts website operators in a compromising position, exposing their users' data to cross-app surveillance through a tracking tool they believed was limited to on-site analytics.

Despite early public reports about this behavior dating back to late 2024, Meta made no attempt to shut down or acknowledge the exploit until May 2025, when researchers published their findings.⁵ This delay suggests that Meta knowingly and willfully continued to surreptitiously and deceptively track users despite repeated warnings and pushback from the security community. They also did not alert Meta Pixel users, who unknowingly facilitated this tracking on their websites and may now face regulatory exposure.

Meta's deceptive practices were egregious enough that even representatives from Alphabet, maker of the Android system, stated that this behavior "blatantly violate[s] our security and privacy principles."⁶ It is also technologically similar to the mechanism utilized by Yandex, a Russian search engine with close ties to the Kremlin, to achieve the same type of snooping on users through background apps. Researchers have gone so far as to liken the Yandex approach explicitly to malware.⁷ It is difficult to interpret Meta's behavior as anything other than targeted data collection and spying that is explicitly designed to subvert basic security and privacy protections.

Meta's claim that this is a simple misunderstanding between its engineers and the Android platform strains credulity.⁸ The deceptive user tracking required a technically precise and deliberate deployment of cross-app communication via localhost snooping; a method so specific that it could not plausibly have been accidental. The fact that similar techniques have been flagged as malware by security researchers only underscores how dishonest and intentional this implementation appears to be.

Notably, this is far from the first time Meta Pixel has collected sensitive personal information without user consent. Since at least 2021, regulators and independent researchers have documented its transmission of hospital patient data, FAFSA applicant details, intimate health

⁴ Adhikari, Suhaas. "Protect Yourself from Meta's Latest Attack on Privacy." *Electronic Frontier Foundation*, 6 June 2025, <https://www.eff.org/deeplinks/2025/06/protect-yourself-metas-latest-attack-privacy>.

⁵ Osborne, Charlie. "Meta Pauses Android Tracking Tech after Researchers Reveal Privacy Breach." *The Register*, 3 June 2025, https://www.theregister.com/2025/06/03/meta_pauses_android_tracking_tech/.

⁶ Harwell, Drew. "Facebook and Instagram Exploited Android Loophole to Track Users, Researchers Say." *The Washington Post*, 6 June 2025, <https://www.washingtonpost.com/technology/2025/06/06/meta-privacy-facebook-instagram/>.

⁷ IMDEA Networks Institute. *Ibid*.

⁸ Goodin, Dan. "Meta and Yandex are de-anonymizing Android users' web browsing identifiers", *Ars Technica*, 3 June 2025, <https://arstechnica.com/security/2025/06/meta-and-yandex-are-de-anonymizing-android-users-web-browsing-identifiers/>.

metrics, and even tax-return figures to Meta's advertising systems.^{9,10} Federal and state regulators, along with courts from California to Norway, have repeatedly sanctioned online platforms and digital services using the Meta Pixel and questioned Meta's own role in these violations. This persistent pattern demonstrates that the Meta's covert tracking we address today is part of a broader corporate strategy, not an isolated lapse. As our lives become increasingly connected and online, protecting user privacy is more important than ever. We demand Meta adopt stronger internal safeguards and structural reforms that demonstrate a sustained commitment to rebuilding user trust.

As Members of the Energy & Commerce Committee and other concerned offices, we take seriously our responsibility to protect consumers from deceptive practices by dominant technology platforms. Given the duration, technical specificity, and pattern of similar misconduct, we request detailed answers to the following questions no later than January 31st, 2026.

1. When did Meta begin using localhost snooping to covertly track users?
2. What internal documentation (e.g., design reviews or risk assessments) was created to document the implementation and use of this new tracking method? Does this documentation indicate this was a repurposing of developer-only tools?
3. What consideration, if any, did Meta give to how this tracking method might collect user data not otherwise available?
4. Who approved or authorized the use of this tracking method?
5. How many users were tracked using this method, and how many websites embedding the Meta-Pixel initiated background connections to Meta apps?
6. Did Meta create or modify any user profiles, behavioral segments, or machine learning models using data obtained through this exploit?
7. Did Meta collect any sensitive categories of data through this covert localhost tracking method, such as hospital patient data, FAFSA applicant details, intimate health metrics, or tax-return figures? If so, what categories of sensitive data were involved, and how were they handled?
8. Did Meta produce a "Privacy Review Statement" to assess the privacy risks of this new tracking method as required by Meta's 2019 consent decree with the FTC?¹¹ Did the statement note any privacy risks and whether new safeguards were needed?

⁹Bajak, Frank. "Lawmakers Question Education Department about Facebook Student Aid Tracking after Markup Investigation." *The Markup*, 11 May 2022, <https://themarkup.org/pixel-hunt/2022/05/11/lawmakers-question-education-department-about-facebook-student-aid-tracking-after-markup-investigation>.

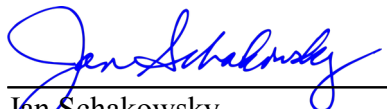
¹⁰Bajak, Frank. "Facebook Is Receiving Sensitive Medical Information from Hospital Websites." *The Markup*, 16 June 2022, <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>.


¹¹ https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf


9. Was Meta aware of Yandex's similar use of localhost-based tracking, and did it exchange any information with Yandex or other companies about this technique?
10. What internal discussion or consideration did Meta have in response to the feedback from researchers as early as 2024 describing this tracking as a security issue?
11. Why did Meta continue to track users using this method until May 2025, despite the earlier reports?
12. What steps is Meta taking to notify affected users, particularly those who had opted out of cookies, used private browsing modes, or otherwise attempted to protect their privacy?
13. Were website operators who implemented the Meta Pixel ever informed that it could be used for cross-app tracking?
14. Will Meta commit to permanently deleting all data collected through this method, including any derived behavioral models, user profiles, or ad segments?
15. Will Meta allow an independent third-party audit to verify full deletion of all collected and derivative data associated with this practice?
16. Has Meta deployed a form of localhost snooping on other operating systems or browsers, including iOS or desktop environments?
17. Has Meta used other developer or debugging tools in a live production context to collect data from Meta users, or for any other use?
18. Do any other Meta SDKs, APIs, or developer tools beyond the Meta Pixel use comparable methods to circumvent platform security boundaries or gather cross-contextual user data?

Thank you for your prompt response to these questions and we look forward to hearing back.

Sincerely,


Jan Schakowsky
Member of Congress


Kathy Castor
Member of Congress


Doris Matsui
Member of Congress