United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

September 10, 2025

VIA ELECTRONIC TRANSMISSION

Mr. Mark Zuckerberg
Chairman and Chief Executive Officer
Meta Platforms, Inc.

Dear Mr. Zuckerberg:

We write today about Facebook's reported interactions with elements of the Chinese Government. According to disclosures to Chairman Grassley's office, in 2017 Facebook employees planned to meet with Cyber Administration of China (CAC) officials to discuss AI, Oculus, content moderation, and application programming interfaces (APIs), which allow for the exchange of data across various systems. [1] The disclosures to Chairman Grassley's office include documents related to "Project Aldrin," which was a "version of [Facebook] that complies with China's content laws." [2] According to a 2015 document titled "Aldrin Security Risks," Facebook knew of the risks associated with the Chinese regime. [3] That document said that "[e]very country in the world has cyber espionage capabilities," and that the "traditional focus" of Chinese espionage was "[d]efense secrets, [i]ntellectual property, [b]usiness processes, [c]ompetitive market intelligence, [p]opulations representing internal dissent, and [d]isputed territories."[4] The document also outlined technical risks, geopolitical risks, and internal risks to Facebook's software and infrastructure, standing with other countries, and internal intellectual property.[5] Despite Facebook's knowledge of risks to data security, to include data of American users, the company allegedly decided to move forward with meeting and working with the CAC and Project Aldrin.[6] We would like to know whether this behavior has continued with the company ten years later.

Additionally, recent whistleblower disclosures to Chairman Grassley's office have raised further concerns regarding Meta's data privacy and security at their WhatsApp subsidiary. According to information provided to his office, as of February 2025, 87,599 employees across Meta and its platforms have access to WhatsApp user "Device Information," 41,225 employees across Meta and its platforms have access to WhatsApp user "Phone Number[s]," and 40,332 employees across Meta and its platforms have access to WhatsApp user "Email Address[es]."[7] It's been alleged to Chairman Grassley's office that this type and volume of access may violate a 2020 FTC Consent Order where Meta was required to impose restrictions on how the company and its subsidiaries, to include WhatsApp, handle this type of information.

Disclosures to Chairman Grassley's office also allege that WhatsApp was at risk of a "large scale" external data exfiltration by a bad actor.[8] Specifically, in 2024, WhatsApp conducted an operation by the Red Team

[1] Notes and Documents on File with Committee Staff.
[2] Notes and Documents on File with Committee Staff; Isaiah Richard, *Meta Attempted to Expand to China by Creating a Censorship Tool, Says Facebook Whistleblower* (Mar. 9, 2025), https://www.techtimes.com/articles/309605/20250309/meta-attempted-expand-china-creating-censorship-tool-says-facebook-whistleblower.htm.
[3] Notes and Documents on File with Committee Staff.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*

Operations Group (RTOG), which assessed "the extent to which an attacker with WhatsApp engineering permissions could cause harm."[9] According to the RTOG's report:

> An attacker can exfiltrate any data leading to a significant loss of sensitive information, financial damage, and potential reputation harm for the organization due to unauthorized access and distribution of confidential data.[10]

Should Meta dispute the allegations raised to Chairman Grassley's office, we welcome an explanation. Please answer the following no later than September 24, 2025:

1. Did Facebook staff meet with the officials from the CAC? If so, provide all records.[11]

2. Provide all records relating to Project Aldrin.

3. Provide a list of all instances where accounts and content were removed from Meta and/or its platforms at the request of a foreign government, including the Chinese government. Provide the date and name of the government requesting the removal and whether the request was approved or denied.

4. With respect to the allegation that Meta has not complied with the aforementioned 2020 FTC Consent Order, how does the company respond? Do employees that don't have a business need for access to the data have access? What steps have been taken to comply with the Consent Order?

5. What steps were taken by Meta after the RTOG report to shore up data protection, especially data protection for American users?

6. Has any U.S. consumer data ever been exfiltrated, or attempted to be exfiltrated, from WhatsApp servers? If so, provide the dates and who perpetrated the attack.

Sincerely,

Charles E. Grassley
Chairman
Senate Committee on the Judiciary

Josh Hawley
Chairman
Senate Committee on the Judiciary
Subcommittee on Crime and Counterterrorism

Marsha Blackburn
Chairman
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law

[9] *Id.*
[10] *Id.*
[11] "Records" include any written, recorded, or graphic material of any kind, including letters, memoranda, reports, notes, electronic data (emails, email attachments, and any other electronically created or stored information), calendar entries, inter-office communications, meeting minutes, phone/voice mail or recordings/records of verbal communications, and drafts (whether they resulted in final documents).