United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510–6475

February 6, 2023

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

Dear Mr. Zuckerberg:

We write you with regard to recently unsealed documents in connection with pending litigation your company, Meta, is engaged in. It appears from these documents that Facebook has known, since at least September 2018, that hundreds of thousands of developers in countries Facebook characterized as "high-risk," including the People's Republic of China (PRC), had access to significant amounts of sensitive user data. As leaders of the Senate Intelligence Committee, we write today with a number of questions regarding these documents and the extent to which developers in these countries were granted access to American user data.

In 2018, the *New York Times* revealed that Facebook had provided privileged access to key application programming interfaces (APIs) to Huawei, OPPO, TCL, and other device-makers based in the PRC.[1] Under the terms of agreements with Facebook dating back to at least 2010, these device manufacturers were permitted to access a wealth of information on Facebook's users, including profile data, user IDs, photos, as well as contact information and even private messages.[2] In the wake of these revelations, as well as broader revelations concerning Facebook's lax data security policies related to third-party applications, our staffs held numerous meetings with representatives from your company, including with senior executives, to discuss who had access to this data and what controls Facebook was putting in place to protect user data in the future.

[1] Michael LaForgia and Gabriel J.X. Dance, "Facebook Gave Data Access to Chinese Firms Flagged by U.S. Intelligence," *New York Times* (June 5, 2018), available at https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html

[2] Gabriel J.X. Dance, Nicholas Confessore, and Michael LaForgia, "Facebook Gave Device Makers Deep Access to Data on Users and Friends," *New York times* (June 3, 2018), available at https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html

Given those discussions, we were startled to learn recently, as a result of this ongoing litigation and discovery, that Facebook had concluded that a much wider range of foreign-based developers, in addition to the PRC-based device-makers, also had access to this data. According to at least one internal document, this included nearly 90,000 separate developers in the People's Republic of China (PRC), which is especially remarkable given that Facebook has never been permitted to operate in the PRC.[3] The document also refers to discovery of more than 42,000 developers in Russia, and thousands of developers in other "high-risk jurisdictions," including Iran and North Korea, that had access to this user information.

As Facebook's own internal materials note, those jurisdictions "may be governed by potentially risky data storage and disclosure rules or be more likely to house malicious actors," including "states known to collect data for intelligence targeting and cyber espionage."[4] As the Chairman and Vice Chairman of the Senate Select Committee on Intelligence, we have grave concerns about the extent to which this access could have enabled foreign intelligence service activity, ranging from foreign malign influence to targeting and counter-intelligence activity.

In light of these revelations, we request answers to the following questions on the findings of Facebook's internal investigation:

1) The unsealed document notes that Facebook conducted separate reviews on developers based in the PRC and Russia "given the risk associated with those countries."
   - What additional reviews were conducted on these developers?
   - When was this additional review completed and what were the primary conclusions?
   - What percentage of the developers located in the PRC and Russia was Facebook able to definitively identify?
   - What communications, if any, has Facebook had with these developers since its initial identification?
   - What criteria does Facebook use to evaluate the "risk associated with" operation in the PRC and Russia?
2) For the developers identified as being located within the PRC and Russia, please provide a full list of the types of information to which these developers had access, as well as the timeframes associated with such access.

[3] Exhibit 6, "App Developer Investigation & Enforcement: September 2018 Status and Re-Scoped Approach," Facebook (September 17, 2018), available at https://storage.courtlistener.com/recap/gov.uscourts.cand.327471/gov.uscourts.cand.327471.1100.6.pdf

[4] Exhibit 6, "App Developer Investigation & Enforcement: September 2018 Status and Re-Scoped Approach," Facebook (September 17, 2018), available at https://storage.courtlistener.com/recap/gov.uscourts.cand.327471/gov.uscourts.cand.327471.1100.6.pdf

3) Does Facebook have comprehensive logs on the frequency with which developers from high-risk jurisdictions accessed its APIs and the forms of data accessed?
4) Please provide an estimate of the number of discrete Facebook users in the United States whose data was shared with a developer located in the each country identified as a "high-risk jurisdiction" (broken out by country).
5) The internal document indicates that Facebook would establish a framework to identify the "developers and apps determined to be most potentially risky[.]"
    - How did Facebook establish this rubric?
    - How many developers and apps based in the PRC and Russia met this threshold? How many developers and apps in other high-risk jurisdictions met this threshold?
    - What were the specific characteristics of these developers that gave rise to this determination?
    - Did Facebook identify any developers as too risky to safely operate with? If so, which?
6) The internal document references your public commitment to "conduct a full audit of any app with suspicious activity."
    - How does Facebook characterize "suspicious activity" and how many apps triggered this full audit process?
7) Does Facebook have any indication that any developers' access enabled coordinated inauthentic activity, targeting activity, or any other malign behavior by foreign governments?
8) Does Facebook have any indication that developers' access enabled malicious advertising or other fraudulent activity by foreign actors, as revealed in public reporting?[5]

Thank you for your prompt attention.

Sincerely,

Mark R Warner

Mark R. Warner
Chairman

Marco Rubio
Vice Chairman

[5] Craig Silverman and Ryan Mac, "Facebook Profits as Users Are Ripped Off by Scam Ads," (December 10, 2020), available at https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam