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

September 12, 2022

Parag Agrawal
Chief Executive Officer
Twitter, Inc.
1355 Market Street
Suite 900
San Francisco, CA 94103

Dear Mr. Agrawal:

We write regarding recent allegations that Twitter has turned a blind eye to foreign intelligence infiltration, does not adequately protect user data, and has provided misleading or inaccurate information about its security practices to government agencies. These allegations raise serious concerns given Twitter's significant role in the U.S. communications landscape and its global reach. In light of these allegations, the Senate Judiciary Committee has scheduled a hearing for September 13, 2022, and we have extended an invitation to you, through your counsel, to appear at that hearing.

On August 23, 2022, multiple news outlets released a lengthy disclosure containing allegations made by Peiter "Mudge" Zatko, the former head of security at Twitter.[1] The disclosure paints a disturbing picture of a company that has fallen short of basic security standards in the technology industry, failed to adequately mitigate attempts by foreign governments to gain access to sensitive user information, and willfully misled government regulators. Among other serious concerns, the disclosure suggests that more than half of the company's full-time employees have privileged access to Twitter's production systems, enabling several thousand employees to access sensitive user data—while, at the same time, Twitter reportedly lacks sufficient capacity to reliably know who has accessed specific systems and data and what they did with it. In addition, the disclosure raises questions about Twitter's capacity to adequately address misinformation and disinformation, particularly in non-English speaking countries. A draft of an independent report requested by Mr. Zatko and included with the disclosure suggests that Twitter may take "a largely reactive approach to misinformation, disinformation and spam in which action is taken on content and threats only if it is flagged by reporters or news headlines, partners, or political officials due to the lack of people and sufficient tools to do proactive analysis."[2]

---

[1] *See, e.g.*, Joseph Menn, Elizabeth Dwoskin, and Cat Zakrzewski, "Former security chief claims Twitter buried 'egregious deficiencies'," THE WASHINGTON POST (Aug. 23, 2020), https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam/.

[2] Current State Assessment at 8, https://www.washingtonpost.com/technology/interactive/2022/twitter-

The disclosure also raises the prospect that your company's data security practices may enable foreign governments and intelligence agencies to access sensitive data identifying Twitter users. This is not a theoretical concern. Last month, a federal jury convicted a former Twitter employee of acting as an unregistered foreign agent for the Kingdom of Saudi Arabia.[3] While employed by Twitter, the defendant accepted payments in exchange for accessing and conveying the private information of Twitter users to the Saudi Royal family and other Saudi officials. He is one of two former Twitter employees charged by the Justice Department in connection with their efforts to provide Saudi officials with the personal information of dissidents and activists critical of the Saudi regime, including email addresses, phone numbers, and IP addresses—data that could enable Saudi officials to identify and locate these Twitter users.[4]

With tens of millions of users in the U.S. and hundreds of millions of users worldwide, your company collects and is responsible for vast troves of sensitive data. This data can reveal not just a user's activity on Twitter, but also their personally identifiable information—and even their geolocation. If accurate, Mr. Zatko's allegations demonstrate an unacceptable disregard for data security that threatens national security and the privacy of Twitter's users.

To enable us to better understand your company's data security practices and further assess Mr. Zatko's disclosures, please provide written responses to each of the following questions as soon as possible, but no later than September 26, 2022:

1. What are your policies and procedures for protecting user data from insider threats posed by foreign intelligence?

    a. Following the discovery of Ahmad Abouammo's and Ali Alzabarah's unlawful engagement with the Kingdom of Saudi Arabia, how were these policies and/or procedures updated and/or improved?

    b. What training, guidance, and/or other instruction is given to Twitter employees regarding how they should prepare for, guard against, and report any suspected attempts at foreign government intrusion into the company?

    c. How, if at all, does Twitter secure its live production systems and/or user data from potential access by foreign government operatives? To what degree are Twitter's security teams capable of determining whether foreign government operatives or other nefarious actors have attempted to access sensitive systems or user data?

---

whistleblower-sec-spam/?document=undefined.

[3] Press Release, "Former Twitter Employee Found Guilty of Acting as an Agent of a Foreign Government and Unlawfully Sharing Twitter User Information," U.S. DEP'T OF JUSTICE (Aug. 10, 2022), https://www.justice.gov/opa/pr/former-twitter-employee-found-guilty-acting-agent-foreign-government-and-unlawfully-sharing.

[4] Press Release, "Two Former Twitter Employees and a Saudi National Charged as Acting as Illegal Agents of Saudi Arabia, U.S. Dep't of Justice (Nov. 7, 2019), https://www.justice.gov/opa/pr/two-former-twitter-employees-and-saudi-national-charged-acting-illegal-agents-saudi-arabia.

d. How does Twitter ensure that employees located in foreign countries are protected from influence by foreign governments? What additional oversight policies and/or procedures are in place to ensure that these employees are not actively working on behalf of foreign governments?

e. What steps does Twitter take during the hiring process to screen candidates for potential linkages to foreign intelligence services? What additional screening procedures, if any, were implemented following the discovery of Abouammo's and Alzabarah's engagement with the Kingdom of Saudi Arabia?

2. What are your company's policies and procedures for limiting employee access to user data and Twitter's live production environment?

   a. What percentage and number of Twitter employees have at least some level of access to live production systems and/or user data? Please respond to the same question for Twitter engineers.

   b. What policies and/or procedures are in place to monitor and control access to Twitter's live production environment and user data? What policies and/or procedures are in place to ensure that data is registered and tagged in accordance with domestic and international legal requirements?

   c. To what degree do engineers at Twitter use live production data and test new software directly on the company's commercial service, as opposed to segregated test systems? Please describe whether customer or test data is used in the process and at what stages, and at what stage of development new software is tested directly on the company's commercial service as opposed to a segregated test system. If new software is not tested in a segregated test system, using test data, please explain why Twitter does not follow this practice, which many of its peer companies do.

   d. The whistleblower disclosure claims that Twitter has serious information security vulnerabilities, "with over 50% of Twitter's 500,000 data center servers with non-compliant kernels or operating systems, and many unable to support encryption at rest," "over 30% of [employee] devices reporting they had disabled software and security updates," and "no mobile device management for employee phones[.]" Is this information accurate? If you dispute these claims, please provide specific and detailed information to support your response.

   e. What steps, if any, has Twitter taken to address data center redundancy concerns in order to prevent a "Black Swan" existential threat that could take the company's service offline from occurring, as described in the whistleblower disclosure?

3. Please address the following allegations that Twitter has misled regulatory agencies on multiple occasions:

a. The whistleblower disclosure claims that "when the [U.S. Federal Trade Commission (FTC)] asked Twitter whether it fully deleted the data of users who left the service, Twitter deliberately misled the FTC by stating those accounts were 'deactivated,' even when the data was not fully deleted." What is the distinction between an account and its data that is "deactivated" and an account and its data that is "fully deleted"? Please describe in detail the process, if such a process exists, by which Twitter fully deletes the data of users who leave its service.

b. The whistleblower disclosure claims that in 2020, Twitter had more than 40 security incidents, 70 percent of which were access control related, including 18 access control related breaches. How many access control related security incidents occurred in 2021, and have occurred thus far in 2022? How many of these incidents was Twitter required to report to U.S. government agencies or foreign government agencies? What steps, if any, has Twitter taken to prevent similar security incidents from occurring in the future?

c. The whistleblower disclosure claims that Twitter does not hold proper legal rights to key machine learning training materials and attempted to deceive the FTC when it inquired about these models. Please provide a list of the proper licenses or ownership rights held by Twitter regarding all training materials used by the company to build its machine learning models.

4.

a. Please produce a complete, unredacted copy of the independent report prepared at Mr. Zatko's request regarding Twitter's approach to countering misinformation and disinformation.

b. Please provide a full and complete list of all government agencies, foreign and domestic, who have approached Twitter to flag content for removal.

If you have any questions, please contact Jack Solano of Chair Durbin's staff at 202-224-7703 or Dario Camacho of Ranking Member Grassley's staff at 202-224-5225. Thank you for your prompt attention to this important request.

Sincerely,

Richard J. Durbin
United States Senator

Charles E. Grassley
United States Senator