Whistleblower details foreign agents placed at Twitter, lack of data safeguards

September 13 2022, by Gopal Ratnam, CQ-Roll Call

Credit: Pixabay/CC0 Public Domain

Peiter Zatko, the former Twitter security chief who turned whistleblower, told the Senate Judiciary Committee on Tuesday that the social media company's security practices were so weak that foreign governments were able to place agents on the company's payroll.

Zatko also told lawmakers that U.S. regulators are unable to police tech

companies, singling out the Federal Trade Commission as being in over its head and allowing tech companies to "grade their own homework." The U.S. practice of slapping companies with one-time fines is "priced in" by Twitter and other tech companies as the cost of doing business, he said.

His testimony followed complaints that he filed with the FTC, the Securities and Exchange Commission, and the Justice Department. The Washington Post first disclosed his revelations last month.

Despite the hearing, Congress isn't expected to take action to police the behavior of Twitter or other social media companies. Two Senate bills that would address data privacy for children and minors have been approved by the Senate Commerce Committee, but they haven't received floor action.

Senate Judiciary member Amy Klobuchar, D-Minn., cited the lack of action at the Tuesday hearing. "We have not passed one bill out of the U.S. Senate when it comes to competition, when it comes to privacy, when it comes to better funding agencies," she said. "I think we'd better be putting the mirror on ourselves."

Zatko said the Indian government was able to place an agent in Twitter's India office as an employee while the company and the government were negotiating over the platform's content policies. "I saw with great confidence a foreign agent placed from India to understand the negotiations," he said, "and how well they were going for or against" India's ruling Bharatiya Janata Party.

The Indian government since 2021 has asked Twitter to remove as many as 1,400 accounts, according to a Bloomberg News report in July that cited unnamed sources. Twitter challenged the Indian government's orders in court in June; the outcome is pending.

Senate Judiciary Chairman Richard J. Durbin, D-Ill., called Zatko's allegations concerning. The area of great concern is the access of [foreign governments](#) and foreign agencies to data that American users may be providing to the platform, he said, adding that Americans have "no idea that they are vulnerable to that possibility."

In August, a former Twitter manager accused of spying for Saudi Arabia was convicted in San Francisco on six criminal counts. Prosecutors said an adviser to Saudi Arabia's Crown Prince Mohammed bin Salman recruited Ahmad Abouammo to use his insider knowledge to access Twitter accounts and dig up [personal information](#) about Saudi dissidents.

Zatko said Twitter had few of the standard security practices used at several tech and other companies with protocols specifying which employees have access to what computer systems and/or maintenance logs of employee activity. Thousands of engineers at Twitter have access to the company's production system or the computer networks that host the social media platform and users' data, he said.

Many companies create a separate network where new employees are trained, and new offerings are tested before being launched on the production system, Zatko said.

Twitter didn't maintain logs of which engineers accessed what systems, he said. As a result, thousands of employees have access to all the information from Twitter users, making the company a rich target for intelligence gathering on users by foreign governments, Zatko said.

President Barack Obama's Twitter account was hacked in 2009. Hackers also accessed Obama's account in 2020 as well as those of then-presidential candidate Joe Biden, Tesla founder Elon Musk and 100 others.

Zatko described a company so focused on adding new users and increasing revenue that it spared no time, resources or personnel to put security measures in place. Twitter allowed Chinese companies that may have had ties to the government to advertise on the platform even though it is banned in China, Zatko said. Users who clicked on those ads may have exposed themselves to data collection by the Chinese companies, he said.

"Twitter was a company that was managed by risk and by crises, instead of one that manages risk and crises," Zatko said.

The company's top executives didn't want to hear about security weaknesses, Zatko said.

US regulators 'over their head'

Zatko said U.S. federal agencies are woefully inadequate in policing tech companies, noting that the FTC in particular was unable to fully enforce a 2011 consent decree with Twitter about safeguarding users' data.

"I think the FTC, honestly, is a little over their head … compared to the size of the big tech companies and the challenge they have against them," he said.

Twitter was more afraid of foreign regulators—including France's data protection agency, known as CNIL—than of the FTC, Zatko said. Unlike the FTC, which levies one-time fines, France and other foreign regulatory bodies are more likely to impose structural remedies on tech companies that could hurt bottom lines and get the attention of investors, Zatko said.

In May, the FTC fined Twitter $150 million for violating a 2011 consent decree by collecting customers' personal information for the stated

purpose of security and then exploiting it commercially.

2022 CQ-Roll Call, Inc., All Rights Reserved. Distributed by Tribune Content Agency, LLC.