Twitter says users' phone numbers provided for security were spied on and used for ad purposes by lying Twitter executives

Tony Romm, The Washington Post

Twitter said Tuesday that it may have mishandled an unspecified number of users' email addresses and phone numbers, allowing that data to be used "inadvertently" for advertising purposes.

The incident marks the latest security mishap for the social-networking company, but one that could carry with it some legal headaches. Federal regulators penalized Facebook earlier this year for a similar situation.

In a blog post, Twitter explained that users share email addresses and phone numbers with the company for safety and login verification purposes, such as two-factor authentication, which allows people to receive a one-time code that they input along with their password in order to access their account.

The trouble, however, stems from the fact that advertisers can upload their own contact lists to match their customers with Twitter's users. In doing so, Twitter said it "may have matched

people on Twitter" to a marketer's list "based on the email or phone number the Twitter account holder provided for safety and security purposes."

"We cannot say with certainty how many people were impacted by this, but in an effort to be transparent, we wanted to make everyone aware," Twitter said. "No personal data was ever shared externally with our partners or any other third parties."

The incident could invite trouble for Twitter in Washington, where regulators who investigated and penalized Facebook for a series of privacy scandals took issue with its handling of phone numbers. In that case, the Federal Trade Commission alleged Facebook deceived users because it "did not disclose, or did not adequately disclose" that phone numbers provided through its security tool for the purpose of two-factor authentication "also would be used by Facebook to target advertisements to those users."

Adding to Twitter's potential troubles, the company finalized an agreement with the FTC in 2011 that alleged the company failed to protect users from security threats. The resulting settlement requires the company to maintain a comprehensive data security policy and refrain from misrepresenting the way it handles and protects users' data, violations of which could carry fines.

"Given that Facebook got dinged for this exact practice, I think it likely meets the threshold of material omission or even deception under Section 5 on its own. That's further compounded by the fact that Twitter is also under order already by the FTC, " said Ashkan Soltani, a former chief technologist at the FTC, citing the portion of law that prohibits unfair or deceptive acts and practices.

Twitter has revealed a number of additional data-security incidents this year. It told users that it may have "inadvertently" collected and shared some location data with an unnamed third-party partner. It also informed users of Twitter's Android smartphone app that a system issue turned off a setting that made their tweets private. Twitter did not disclose the number of users affected in either instance.

Perhaps the most significant security mishap came in August, however, when Twitter CEO Jack Dorsey had his personal account hacked. The move prompted Twitter to disable a feature that allowed users to tweet by text.