UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

Statement of Chair Lina M. Khan
Joined by Commissioner Rebecca Kelly Slaughter
In the Matter of Twitter, Inc.
Commission File No. 2023062

May 25, 2022

Americans increasingly find themselves having to surrender personal data to use technologies that are central to economic and social life, and many report feeling a total loss of control over how this data is used.[1] Indeed, evidence suggests that the current configuration of commercial data practices do not actually reveal how much users value privacy or security, and there is growing recognition that the "notice-and-consent" framework has notable shortcomings.[2] The FTC must harness its full set of tools to ensure we are keeping pace with these new realities, including by exploring the need for agency promulgated rules. In the meantime, we must also hold companies accountable for violating existing laws, including through deceptive disclosures.

According to the Complaint in this matter, Twitter obtained data from users on the pretext of harnessing it for security purposes but then ended up also using the data to target users with ads. The relief we are obtaining from Twitter for this alleged violation of both the law and a past FTC order drives home two key consumer protection principles. First, stating that data is being collected for one purpose and then using it for another purpose is deceptive. The FTC Act prohibits companies from engaging in bait-and-switch tactics with individuals' data.[3] Second, burying disclosures in lengthy privacy policies or terms of service documents does not cure deceptive statements the company makes at the time it collects users' information. Users do not assume the responsibility of wading through privacy policies to uncover provisions that override or negate what the company told them directly.

Twitter's Prior and Present Unlawful Practices, As Alleged in the Complaint

Consumers use passwords to access their email, social media accounts, bank accounts, medical records, and more. These credentials are a primary shield for some of our most confidential and personal information, but they are also a common target for hackers or

[1] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[2] *See, e.g.*, Daniel Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 22-32 (2021).
[3] Our recent order in CafePress stands for this proposition that consumers can bank on claims that data will be used in a limited way or for limited purposes. Agreement Containing Consent Order, *Residual Pumpkin Entity, LLC, and PlanetArt LLC (d/b/a CafePress),* Comm'n File No. 192-3209 (Mar. 15, 2022).

malicious actors. As a result, many data breaches can be traced back to stolen or compromised consumer credentials.[4] In response to these online threats and harms, businesses and consumers alike have adopted cybersecurity approaches, like multi-factor authentication, to protect their accounts and data from unauthorized third-party access and use. Multi-factor authentication allows consumers to use two or more forms of evidence to verify their identity when attempting to log into or otherwise access a network, device, application, or service.

In 2011, the Commission charged Twitter with violating Section 5 of the FTC Act for the company's failures to provide reasonable security safeguards to prevent unauthorized access to users' information and to honor privacy choices exercised by Twitter users. This enforcement action resulted in a consent order that barred Twitter from misrepresenting how the company handles "nonpublic consumer information," such as email addresses and phone numbers, and the security measures that it has in place.[5]

From May 2013 to September 2019 Twitter prompted users to provide a telephone number or email address for the express purpose of enabling multi-factor authentication to verify their Twitter accounts, assisting with account recovery, and re-authenticating users' accounts. According to the complaint, Twitter during this period failed to disclose that it also used the telephone numbers and email addresses that users provided for security purposes to target advertisements to those users. Although Twitter's privacy policy made reference to the fact that contact information would be used for advertising purposes,[6] the complaint charges that this disclosure was deficient and did not remedy the misleading representations made to users when Twitter collected their personal information for security purposes. This allegedly deceptive practice potentially affected more than 140 million Twitter users, while boosting Twitter's primary source of revenue. In October 2019, Twitter publicly self-reported its misuse of users' personal information.[7]

Today's announcement of an enforcement action and resolution alleges that Twitter violated Section 5 of the FTC Act, the EU-US and Swiss-US Privacy Shield frameworks, and the FTC's 2011 Order with Twitter. The case reflects diligent work by FTC staff, and we thank the team for their efforts to hold Twitter accountable.

---

[4] VERIZON, DATA BREACH INVESTIGATIONS REPORT, at 7 (2022), https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/summary-of-findings/ (noting that 61% of data breaches involved credentials).

[5] Press Release, Fed. Trade Comm'n, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information (Mar. 11, 20211), https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-accepts-final-settlement-twitter-failure-safeguard-personal-information-0.

[6] *See Twitter Privacy Policy*, TWITTER, https://twitter.com/en/privacy#update (effective June 10, 2022; last visited May 25, 2022).

[7] @TwitterSupport, TWITTER (Oct. 8, 2019, 4:02 PM), https://twitter.com/twittersupport/status/1181661080033955840?ref_src=.

The Commission's Settlement with Twitter[8]

The settlement imposes a series of requirements on Twitter. A few in particular are worth highlighting.

First, Twitter must notify affected parties of its allegedly deceptive conduct. Requiring parties to provide notice ensures that individuals and businesses can determine whether they need to take any action and decide whether they want to continue doing business with a firm that was charged with engaging in wrongdoing.

Second, Twitter must provide users with multi-factor authentication tools that do not require users to share their phone number, such as mobile authentication apps or security keys.[9] Research shows that these alternatives provide greater security, as they can protect users against credential phishing. Ensuring that the remedies we seek reflect the latest in security research and learning is critical. We are grateful that we have been able to increase the number of technologists, security researchers, and other technical experts at the agency over the last year, and we are keen to continue building out this skillset at the FTC. Given that a growing portion of our work requires investigating digital tools and services, embedding technologists in our investigative teams can further boost the sophistication and efficacy of our enforcement work.

Third, Twitter must pay $150 million in civil penalties for its alleged recidivism. Civil penalties are key for deterring law violations, and we believe the FTC must approach civil penalties with an eye to complete deterrence. We are confident that in this matter the civil penalty amount obtained ensures that Twitter is not profiting from its allegedly unlawful conduct.

We are grateful to the FTC team for the thorough investigation into Twitter's alleged violation and the role of individual decisionmakers and for securing a strong settlement.

[8] Our colleagues Commissioners Wilson and Phillips invite a framework of comparing enforcement resolutions in two entirely different matters—an exercise that the defense bar also frequently demands. We respectfully reject this invitation. No two law violations—or law violators—are exactly alike. Every potential action the Commission takes, whether it is to litigate or to weigh the merits of a proposed settlement, is distinct and requires close and careful consideration of several factors, including: the alleged violations, the effect of those violations on consumers and markets, the structure and incentives of the defendant's business model, the defendant's past history of lawbreaking, the ability of the order to affect specific and general deterrence, and the resources of the Commission. Charting and tallying may have some visual appeal, but it is no substitute for case-by-case analysis, nor can it make apples-to-apples out of oranges and bananas.

[9] The FTC first requires this security mechanism in its March enforcement action against CafePress. *See* CafePress Decision and Order ¶ 7 (requiring use of multi-factor authentication in place of security questions and answers).