WHY YOUR BUSINESS' USE OF PERSONAL DATA MATTERS:

THE FTC REACHES $150 MILLION SETTLEMENT WITH TWITTER FOR "DECEPTIVELY USING ACCOUNT SECURITY DATA" TO SELL ADS

NOVEMBER 2022

PREPARED BY:

Matt Meinel
Managing Consultant
mmeinel@thinkbrg.com

Belemir Demirbag
Extern
bdemirbag@thinkbrg.com

INTELLIGENCE THAT WORKS

BRG

In May 2022, the Federal Trade Commission (FTC) and Twitter settled, subject to court approval, for Twitter to pay a $150 million penalty for "deceptively using account security data to sell targeted ads" for profit." [1]

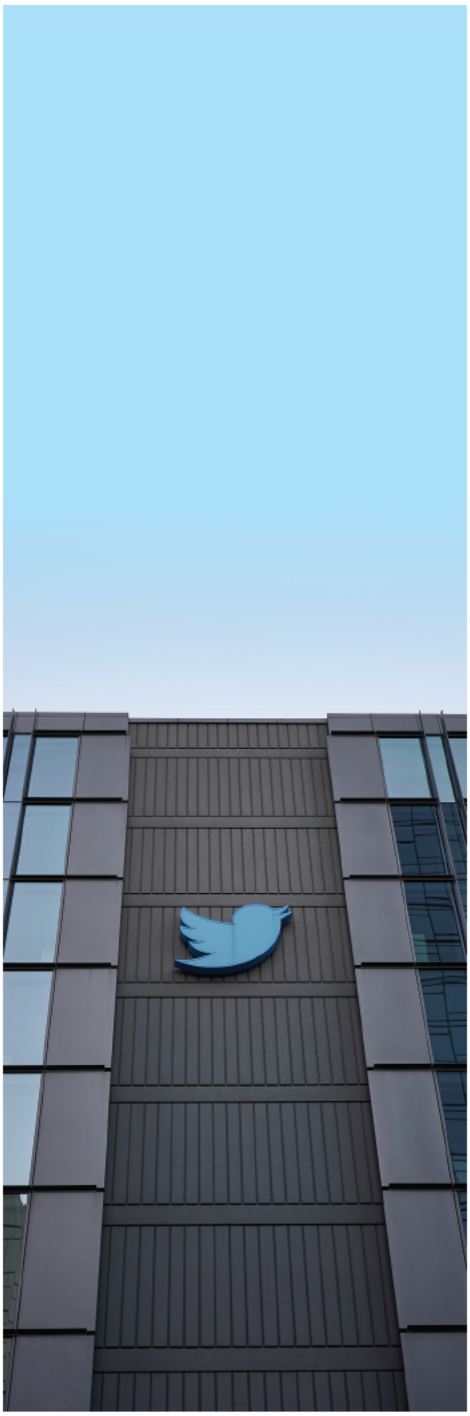
The Facts

Between 2013 and 2019, Twitter requested that over 140 million users provide their email addresses and phone numbers to help secure their accounts through multifactor authentication (MFA) and account recovery. Twitter did not offer other means of implementing MFA—such as tokens or security keys—that did not involve user's personal data.

Later, Twitter decided to repurpose those email addresses and phone numbers collected for security by using that personal data as identifiers for targeted advertising. It did so without notifying consumers of the secondary use of personal data collected for the purpose of improving account security. This type of activity is known in data protection compliance circles as a "purpose limitation violation." In other words, notifying an individual that you are collecting data for one purpose and then using it for another without further notice or consent.

Twitter's Privacy Notice

Twitter's general privacy notice implied a purpose limitation to its use of personal data and said Twitter may use personal data, including email and phone numbers, for advertising.[2] However, according to FTC, at the point of collection of the personal data for MFA, Twitter led users to believe that the emails and phone numbers provided would only be used for securing individual accounts, with no mention of advertising.[3]



1 Federal Trade Commission, "FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads," press release (May 25, 2022). https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads

2 Twitter, Twitter Privacy Policy (effective June 10, 2022). https://twitter.com/en/privacy#update

3 FTC, "On FTC's Twitter Case: Enhancing Security Without Compromising Privacy" (May 25, 2022). https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/05/ftcs-twitter-case-enhancing-security-without-compromising-privacy

The FTC's Action

In 2011, the FTC entered an order against Twitter prohibiting it from misrepresenting its privacy and security practices to deceive consumers, in violation of the FTC Act.

Here, the FTC determined that Twitter's notice at the point of collection superseded Twitter's more general privacy notice; therefore, consumers did not have notice that the email addresses and phone numbers would be used for advertising. Specifically, the FTC noted:

> *Generic, broad claims buried in a lengthy document do not override more specific, just-in-time statements made to consumers specifically in the context of when they are providing their information – in this case, about the use of contact information for security purposes. If a company says at the point of collection that consumers' information will be used for a particular purpose, consumers should be able to rely on that promise.*[4]

In other words, even though Twitter's privacy policy disclosed that phone numbers and email addresses would be used for targeted advertising, the FTC looked at ***what the consumer would reasonably expect based on the point at which they provide the personal data.*** In that context, the FTC found that Twitter had deceived consumers about the use of their personal data, in violation of the FTC Act and a 2011 consent decree[5] between the FTC and Twitter.

Additionally, the FTC is requiring Twitter to provide users with additional methods for MFA, such as mobile authentication apps and security keys, so users have the option not to share additional personal data to secure their accounts.

Key Takeaways

- Narrow, point-of-collection privacy notices may supersede a company's more general privacy notice.
- Companies must practice the privacy principle of "Purpose Limitation" by using personal data only for the purpose for which it was collected.
- If a company wishes to use personal data for another purpose (known as "secondary use"), it must disclose that purpose at the time of collection.
- Even where the purpose is cybersecurity and protecting consumers, companies should only collect data necessary to achieve the goal.

4. Ibid.
5. FTC, *In the Matter of Twitter, Inc.*, Docket No. C-4316 (March 2, 2011). https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf

About Berkeley Research Group

Berkeley Research Group, LLC (BRG) is a global consulting firm that helps leading organizations advance in three key areas: disputes and investigations, corporate finance, and performance improvement and advisory. Headquartered in California with offices around the world, we are an integrated group of experts, industry leaders, academics, data scientists, and professionals working across borders and disciplines. We harness our collective expertise to deliver the inspired insights and practical strategies our clients need to stay ahead of what's next. Visit thinkbrg.com for more information.

THINKBRG.COM