



**THE WEAPONIZATION OF THE FEDERAL TRADE COMMISSION:
AN AGENCY'S OVERREACH TO HARASS ELON MUSK'S TWITTER**

Interim Staff Report of the
Committee on the Judiciary
and the
Select Subcommittee on the Weaponization of the Federal Government

U.S. House of Representatives



March 7, 2023

EXECUTIVE SUMMARY

Freedom of speech is among the most important rights guaranteed to every American. Elon Musk’s acquisition of Twitter last year served to revitalize this fundamental freedom in the digital age. Now, in wake of this acquisition, the Federal Trade Commission (FTC) is orchestrating an aggressive campaign to harass Twitter and deluge it with demands about its personnel decisions in each of the company’s departments, every internal communication relating to Elon Musk, and even Twitter’s interactions with journalists. These demands have no basis in the FTC’s statutory mission and appear to be the result of partisan pressure to target Twitter and silence Musk.

The House Committee on the Judiciary, through and with its Select Subcommittee on the Weaponization of the Federal Government, is charged with investigating “violations of the civil liberties of citizens of the United States.”¹ As part of this responsibility, and consistent with the Committee’s oversight responsibilities of the FTC, the Committee has been conducting oversight of the unusual response by the FTC to Musk’s acquisition of Twitter last year.² While the Committee and its Select Subcommittee continue to investigate these issues, this interim staff report fulfills the Committee’s ongoing obligation to identify and report on the weaponization of the federal government.³

The Committee recently obtained new, nonpublic information that falls directly within the Committee’s mandate to investigate and report on instances of the federal government’s authority being weaponized against U.S. citizens. Consisting of over a dozen FTC letters to Twitter that—in the span of less than three months following Musk’s acquisition—make more than 350 specific demands, this information shows how the FTC has been attempting to harass Twitter and pry into the company’s decisions on matters outside of the FTC’s mandate.

The timing, scope, and frequency of the FTC’s demands to Twitter suggest a partisan motivation to its action. When Musk took action to reorient Twitter around free speech, the FTC regularly followed soon thereafter with a new demand letter. The ostensible legal basis for the demand letters—including monitoring Twitter’s privacy and information security program under a revised consent decree between the company and the FTC⁴—fails to provide adequate cover for the FTC’s action. A number of the FTC’s demands have little to no nexus to users’ privacy and information. For example, the FTC has demanded that Twitter provide, among other things:

- Information relating to journalists’ work protected by the First Amendment, including their work to expose abuses by Big Tech and the federal government;⁵

¹ H.R. Res. 12, § 1(b)(D) 118th Cong. (2023) (enacted) (attached hereto as App. 1).

² See Letter from Ranking Member Jim Jordan to FTC Chair Lina Khan (May 4, 2022) (attached hereto as App. 2); Letter from Congressman Scott Fitzgerald, Ranking Member Jim Jordan, and others to FTC Chair Lina Khan (May 24, 2022) (attached hereto as App. 3).

³ See H.R. Res. 12, *supra* n.1.

⁴ *Twitter, Inc.*, Decision and Order, C-4316, FTC (May 26, 2022) (attached hereto as App. 4) (hereinafter “FTC Order”); see also *United States v. Twitter, Inc.*, No. 3:22-cv-3070 (N.D. Cal. May 26, 2022), ECF No. 11 (Stipulated Order) (attached hereto as App. 5).

⁵ Request 1, Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Dec. 13, 2022).

- Every single internal communication “relating to Elon Musk,” by any Twitter personnel—including communications sent or received by Musk—not limited by subject matter, since the day Musk bought the company;⁶
- Information about whether Twitter is “selling its office equipment”;⁷
- All of the reasons why Twitter terminated former Twitter employee and FBI official Jim Baker;⁸
- When Twitter “first conceived of the concept for Twitter Blue,” Twitter’s new \$8/month verified account subscription;⁹ and
- Information disaggregated by “each department, division, and/or team,” regardless of whether the work done by these units had anything to do with privacy or information security.¹⁰

The Committee does not dispute that protecting user privacy and mitigating information security risks are important duties. Because of its consent decree with Twitter, the FTC has the authority to monitor how Twitter is protecting users’ private information, such as their phone numbers and email addresses.¹¹ But the FTC is currently imposing some demands on Twitter that have no rational basis in user privacy. There is no logical reason, for example, why the FTC needs to know the identities of journalists engaging with Twitter. There is no logical reason why the FTC, on the basis of user privacy, needs to analyze all of Twitter’s personnel decisions. And there is no logical reason why the FTC needs every single internal Twitter communication about Elon Musk.

* * *

The strong inference from these facts is that Twitter’s rediscovered focus on free speech is being met with politically motivated attempts to thwart Elon Musk’s goals. The FTC’s demands did not occur in a vacuum. They appear to be the result of loud voices on the left—including elected officials—urging the federal government to intervene in Musk’s acquisition and management of the company. The FTC’s harassment of Twitter is likely due to one fact: Musk’s self-described “absolutist” commitment to free expression in the digital town square.

⁶ Request 17, Letter FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Nov. 30, 2022); *see also* Request 1, Letter from FTC Staff Attorney, FTC Division of Enforcement to Twitter’s Head of Product, Legal, *Twitter, Inc.*, No. C-4316 (Feb. 1, 2023) (same).

⁷ Request 13, FTC Letter (Dec. 13, 2022), *supra* n.5.

⁸ Request 4, Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Dec. 9, 2022).

⁹ Request 8(d), Letter from FTC Staff Attorney, FTC Division of Enforcement Regarding Twitter Blue and Resignations to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Nov. 10, 2022); *see also* Request 3(d), Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Nov. 21, 2022) (request for when Twitter “first conceived of the concept for Blue Verified”).

¹⁰ Request 1, FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; Request 1, Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter Regarding Terminations, *Twitter, Inc.*, No. C-4316 (Nov. 10, 2022).

¹¹ *See* FTC Order, *supra* n.4.

TABLE OF CONTENTS

Executive Summary 1

Table of Contents 3

I. The FTC’s Harassment Campaign against Twitter..... 4

 A. The FTC’s Demands about the Twitter Files and Journalist Interactions 5

 B. The FTC’s Demands about Twitter Blue and the Company’s Revenue Streams 8

 C. The FTC’s Demands for All Elon Musk-related Communications and Other Inappropriate Demands 10

 D. The FTC’s Reliance on Its Existing Consent Decree Is a Pretext to Harass Twitter 11

II. The FTC’s Actions Appear to be the Result of Left-wing Pressure 14

III. Conclusion 18

Appendix..... 19

I. THE FTC'S HARASSMENT CAMPAIGN AGAINST TWITTER

On April 25, 2022, Elon Musk announced his intention to buy Twitter.¹² Previously describing himself as a free speech absolutist,¹³ Musk proclaimed at the time: “Free speech is the bedrock of a functioning democracy, and Twitter is the digital town square where matters vital to the future of humanity are debated.”¹⁴



Elon Musk completed his acquisition of Twitter on October 27, 2022.¹⁵ Just two weeks later, the FTC launched the first of over a dozen demand letters to the company.¹⁶ Between just November 10 and January 18, the FTC issued over 350 requests—an average of roughly 35 requests per week.¹⁷ The FTC’s demand letters often followed shortly after Musk took a step that was controversial to activists on the left.¹⁸ While aspects of the FTC’s demands of Twitter may have had some plausible relevance to Twitter’s compliance with the consent decree, several demands did not. In addition, the scope, timing, and volume of the requests, following substantial left-wing pressure to use the consent decree to go after Musk, strongly support an inference that the motivation of many of the demands is political.

¹² *Elon Musk to Acquire Twitter* (provided by Twitter, Inc.), PR NEWSWIRE (Apr. 25, 2022), <https://www.prnewswire.com/news-releases/elon-musk-to-acquire-twitter-301532245.html>; see Elon Musk (@elonmusk), TWITTER (Apr. 25, 2022, 3:43 PM), <https://twitter.com/elonmusk/status/1518677066325053441?lang=en>.

¹³ See, e.g., Elon Musk (@elonmusk), TWITTER (Mar. 5, 2022, 12:15 AM), <https://twitter.com/elonmusk/status/1499976967105433600?lang=en>; see also Dan Milno, *How ‘free speech absolutist’ Elon Musk would transform Twitter*, THE GUARDIAN (Apr. 14, 2022).

¹⁴ Elon Musk (@elonmusk), TWITTER (Apr. 25, 2022), *supra* n.12; *Elon Musk to Acquire Twitter*, PR NEWSWIRE, *supra* n.12.

¹⁵ Billy Perrigo, *Elon Musk Finalizes Deal to Buy Twitter*, TIME (Oct. 27, 2022).

¹⁶ FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10.

¹⁷ See FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10; Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Nov. 15, 2022); FTC Letter (Nov. 21, 2022), *supra* n.9; FTC Letter (Nov. 30, 2022), *supra* n.6; Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Dec. 6, 2022); FTC Letter (Dec. 9, 2022), *supra* n.8; FTC Letter (Dec. 13, 2022), *supra* n.5; Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Jan. 3, 2023); Letter from FTC Staff Attorney, FTC Division of Enforcement to Counsel for Twitter, *Twitter, Inc.*, No. C-4316 (Jan. 18, 2023).

¹⁸ Cf. Elon Musk (@elonmusk), TWITTER (Nov. 19, 2022, 7:53 PM), <https://twitter.com/elonmusk/status/1594131768298315777> (“Trump will be reinstated.”); FTC Letter (Nov. 21, 2022), *supra* n.9.

A. The FTC’s Demands about the Twitter Files and Journalist Interactions

On December 2, 2022, journalist Matt Taibbi published the first edition of the Twitter Files, a series of reports documenting how Twitter was previously used by government actors to censor speech online.¹⁹ On December 10, Musk tweeted that “Twitter is both a social media company and a crime scene.”²⁰ Three days later, on December 13, the FTC demanded details of Twitter’s interactions with journalists, including “Bari Weiss, Matt Taibbi, Michael Shellenberger, Abigail Shrier,” and the identities of all other journalists to whom Twitter had potentially provided access of its internal records.²¹

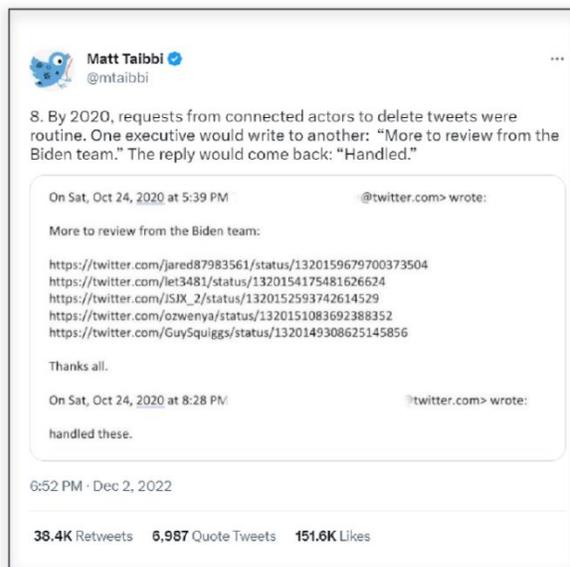


¹⁹ Matt Taibbi (@mtaibbi), TWITTER (Dec. 2, 2022, 6:34 PM), <https://twitter.com/mtaibbi/status/1598822959866683394?lang=en>.

²⁰ Elon Musk (@elonmusk), TWITTER (Dec. 10, 2022, 2:56 PM), <https://twitter.com/elonmusk/status/1601667312930590721?lang=en>.

²¹ Request 1, FTC Letter (Dec. 13, 2022), *supra* n.5.

The Twitter Files are a series of eighteen reports,²² and counting, that began soon after Elon Musk acquired Twitter. The most recent edition was published on March 2.²³ Twitter allowed the journalists, as part of their reporting on government censorship by proxy, to review internal communications and correspondence between Twitter employees and federal agencies, including the Federal Bureau of Investigation.²⁴ The journalists' reporting did *not* concern private user data or information that Twitter users wanted private. Quite the opposite, the reporting in the Twitter Files concerned content that users attempted to publicly share but that the government had pressured Twitter to restrict.²⁵



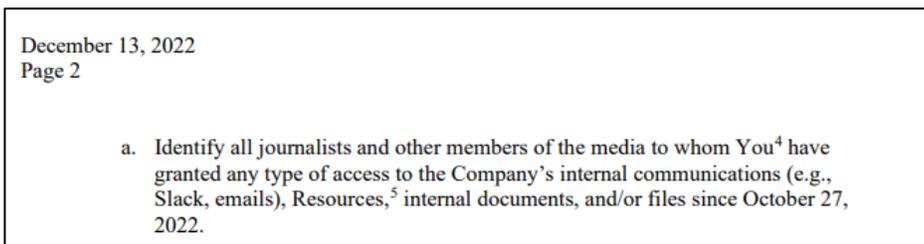
²² See Matt Taibbi (@mtaibbi), TWITTER (Dec. 2, 2022), *supra* n.19; Bari Weiss (@bariweiss) TWITTER (Dec. 8, 2022, 7:15 PM), https://twitter.com/bariweiss/status/1601007575633305600?s=20&t=ilqbULreQtFhJ_mVOCOoQ; Matt Taibbi (@mtaibbi), TWITTER (Dec. 9, 2022, 6:04 PM), <https://twitter.com/mtaibbi/status/1601352083617505281>; Michael Shellenberger (@ShellenbergerMD), TWITTER (Dec. 10, 2022, 6:28 PM), <https://twitter.com/ShellenbergerMD/status/1601720455005511680?s=20&t=jppprcOnLGDKC426tJ0uLA>; Bari Weiss (@bariweiss) TWITTER (Dec. 12, 2022, 1:06 PM), <https://twitter.com/bariweiss/status/1602364197194432515?s=20&t=6Ub9NU39Uhx1rOQdqf9f6g>; Matt Taibbi (@mtaibbi), TWITTER (Dec. 16, 2022, 4:00 PM), <https://twitter.com/mtaibbi/status/1603857534737072128?s=20&t=jOrUd1Ta8GPnhq1XVwZBLw>; Michael Shellenberger (@ShellenbergerMD), TWITTER (Dec. 19, 2022, 11:09 AM), <https://twitter.com/ShellenbergerMD/status/1604871630613753856?s=20&t=eCTz19ucVpfIKlo-pgwLQ>; Lee Fang (@lhfang), TWITTER (Dec. 20, 2022, 3:02 PM), <https://twitter.com/lhfang/status/1605292454261182464?s=20&t=SGeGDuZZN9eZ7cYVGnHOXQ>; Matt Taibbi (@mtaibbi), TWITTER (Dec. 24, 2022, 12:20 PM), https://twitter.com/mtaibbi/status/1606701397109796866?s=20&t=K5THm_CCLPrRig6XIFi7g; David Zweig (@davidzweig), TWITTER (Dec. 26, 2022, 9:10 AM), <https://twitter.com/davidzweig/status/1607378386338340867?s=20&t=NiuAY7UaXXiefwZN7e66LQ>; Matt Taibbi (@mtaibbi), TWITTER (Jan. 3, 2023, 3:27 PM), <https://twitter.com/mtaibbi/status/1610372352872783872?s=20&t=37uOcXgrG6IapxEIoRWvkQ>; Matt Taibbi (@mtaibbi), TWITTER (Jan. 3, 2023, 4:54 PM), <https://twitter.com/mtaibbi/status/1610394197730725889?s=20&t=j4oONRN5hwxTyNfGn1-s6A>; Alex Berenson (@AlexBerenson), TWITTER (Jan. 9, 2023, 2:08 PM), https://twitter.com/AlexBerenson/status/1612526697038897167?s=20&t=DhQ_5IksIhwChTWhfogB5Q; Matt Taibbi (@mtaibbi), TWITTER (Jan. 12, 2023, 12:29 PM), <https://twitter.com/mtaibbi/status/1613589031773769739?s=20&t=G4k4hjcs88Bq235wSI3QIA>; Lee Fang (@lhfang), TWITTER (Jan. 16, 2023, 10:30 AM), <https://twitter.com/lhfang/status/1615008625575202818?s=20&t=c2a6Ez2nx5i-yrFEimrpQw>; Matt Taibbi (@mtaibbi), TWITTER (Jan. 27, 2023, 12:49 PM), <https://twitter.com/mtaibbi/status/1619029772977455105?s=20&t=YXrgzXGKpBZl0jBLxFOxSw>; Matt Taibbi (@mtaibbi), TWITTER (Feb. 18, 2023, 7:13 PM), <https://twitter.com/mtaibbi/status/1627098945359867904?lang=en>; Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023, 12:00 PM), <https://twitter.com/mtaibbi/status/1631338650901389322>.

²³ Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023), *supra* n.22.

²⁴ *Matt Taibbi REVEALS Future Twitter Files Releases | Breaking Points*, YOUTUBE (Dec. 15, 2022), <https://www.youtube.com/watch?v=gExHIgWqDSO> (discussing access provided, how it has evolved, and noting that the journalists did not have “global access to every single document”).

²⁵ See, e.g., Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023), *supra* n.22 (describing how entities funded by the federal government requested Twitter to take down thousands of “inauthentic” accounts that belonged to real Americans).

Tellingly, the FTC’s first demand in its letter sent after the initial installment of the Twitter Files did not concern what private user information may have been at risk. Instead, the FTC demanded that Twitter “[i]dentify all journalists and other members of the media to whom” Twitter has granted access to since Musk bought the company.²⁶ The FTC even named some of the specific journalists—“Bari Weiss, Matt Taibbi, Michael Shellenberger, [and] Abigail Shrier”—with whom Twitter has engaged on the Twitter Files.²⁷ The FTC also demanded to know any “other members of the media to whom You have granted any type of access to the Company’s internal communications” for any reason whatsoever.²⁸



There is no reason the FTC needs to know every journalist with whom Twitter was engaging. Even more troubling than the burden on the company, the FTC’s demand represents a government inquiry into First Amendment-protected activity. It is an agency of the federal government demanding that a private company reveal the names of the journalists who are engaged in reporting about matters of public interest, including potential government misconduct. While the FTC’s inquiry would be inappropriate in any setting, it is especially inappropriate in the context of journalists disclosing how social media companies helped the government to censor online speech.

²⁶ Request 1, FTC Letter (Dec. 13, 2022), *supra* n.5.

²⁷ *Id.*

²⁸ *Id.*, Request 1(a) (footnote omitted).

B. The FTC's Demands about Twitter Blue and the Company's Revenue Streams

Many of the FTC's demands relate to Twitter Blue, an \$8-per-month subscription service that provides Twitter a revenue stream separate from its advertising revenue.²⁹ After Musk announced his intention to buy Twitter in April 2022 and continuing after the acquisition was completed in October, activists on the left called for companies to stop advertising on Twitter.³⁰ Some speculated, if not cheered on, Twitter's predicted financial demise.³¹

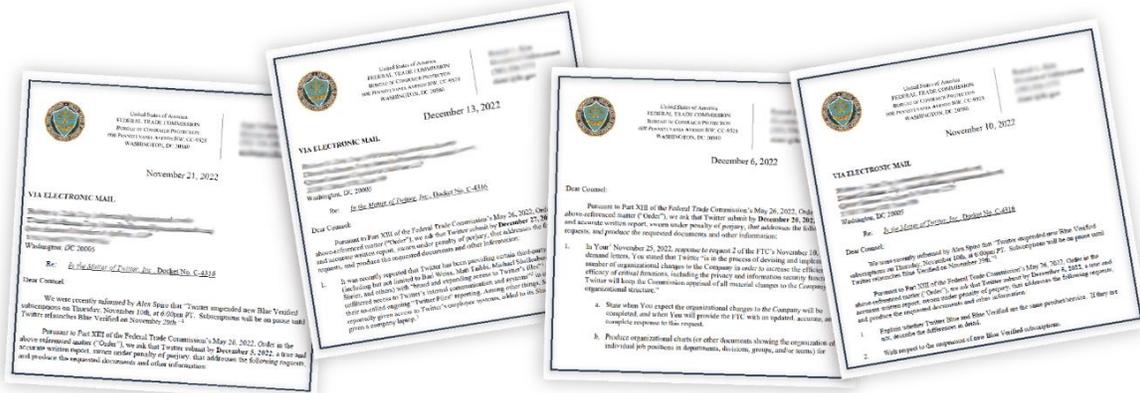


²⁹ See, e.g., FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter (Nov. 21, 2022), *supra* n.9; FTC Letter (Nov. 30, 2022), *supra* n.6; see also James Surowiecki, *Why Elon Musk Is Blowing Up Twitter's Business*, THE ATLANTIC (Nov. 18, 2022).

³⁰ See, e.g., Glorinda Rodriguez, *Activists put pressure on advertisers to drop Twitter ads over Musk takeover, employee layoffs*, ABC NEWS (Nov. 4, 2022); Letter from Accountable Tech and others to Twitter's Advertisers (May 3, 2022) (attached hereto as App. 6); *Calling on Advertisers to Pause Their Spend on Twitter*, STOP HATE FOR PROFIT (Nov. 4, 2022) ("[W]e are calling on advertisers to pause their spend globally until it becomes clear whether Twitter remains committed to being a safe place for advertisers as well as society overall.").

³¹ See, e.g., Alex Kirshner, *The Advertising Industry Is Bringing Elon Musk to His Knees*, THE ATLANTIC (Nov. 8, 2022); Naomi Nix and Jeremy B. Merrill, *Advertisers are dropping Twitter. Musk can't afford to lose any more.*, WASH. POST (Nov. 22, 2022); Halisia Hubbard, *Twitter has lost 50 of its top 100 advertisers since Elon Musk took over, report says*, NPR (Nov. 25, 2022); Suzanne Vranica, Patience Haggin, and Alexa Corse, *Elon Musk's Campaign to Win Back Twitter Advertisers Isn't Going Well*, WALL ST. J. (Dec. 22, 2022).

On October 27, Musk completed his purchase of Twitter and began to reshape Twitter’s focus and its workforce.³² A few days later, Twitter announced the roll-out of its new subscription service, Twitter Blue.³³ On November 10, the FTC sent two demand letters asking for voluminous information about Twitter’s personnel actions—terminations and resignations—and about the Twitter Blue service.³⁴ To date, the FTC has submitted nearly 60 requests related to Twitter Blue.³⁵ Some of the FTC’s demands about Twitter Blue—such as when the service was “first conceived”—appear to serve little purpose other than to pile on to the already burdensome requests.³⁶ One such demand came just two days after Twitter reactivated President Trump’s account.³⁷ In this letter, the FTC demanded nearly twenty additional categories of information about Twitter Blue.³⁸




 United States of America
 FEDERAL TRADE COMMISSION
 BUREAU OF CONSUMER PROTECTION
 600 PENNSYLVANIA AVENUE NW, CC-952R
 WASHINGTON, DC 20580

November 21, 2022

Specify the date when You first conceived of the concept for Blue Verified and the date(s) when You first made Blue Verified available to consumers.

³² Thomas Barrabi and Theo Way, *Elon Musk completes \$44B Twitter takeover, begins firing execs*, N.Y. POST (Oct. 27, 2022).

³³ Elon Musk (@elonmusk), TWITTER (Nov. 1, 2022, 1:36 PM), <https://twitter.com/elonmusk/status/1587498907336118274>.

³⁴ FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10.

³⁵ FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter (Nov. 21, 2022), *supra* n.9; FTC Letter (Nov. 30, 2022), *supra* n.6; FTC Letter (Dec. 6, 2022), *supra* n.17; FTC Letter (Dec. 9, 2022), *supra* n.8; FTC Letter (Dec. 13, 2022), *supra* n.5.

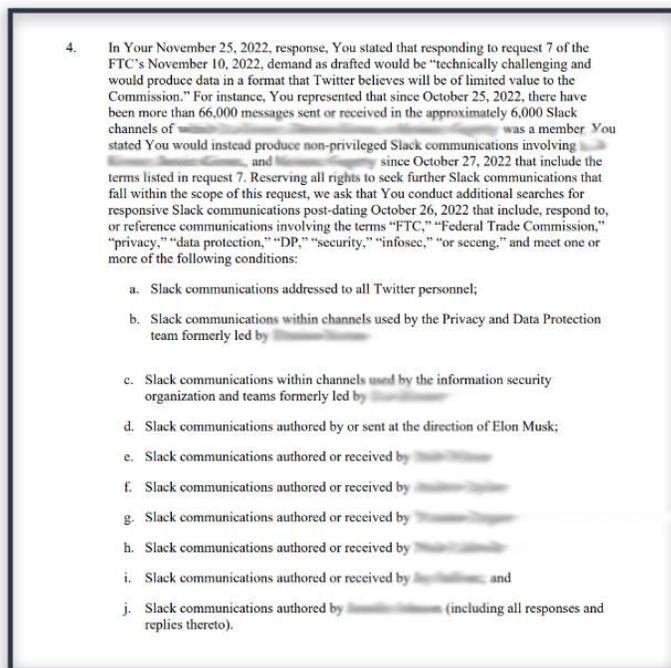
³⁶ *See, e.g.*, Request 8(d), FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; *see also* Request 3, FTC Letter (Nov. 21, 2022) (request for when Twitter “first conceived of the concept for Blue Verified”), *supra* n.9.

³⁷ *Cf.* Elon Musk (@elonmusk), TWITTER (Nov. 19, 2022, 7:53 PM), <https://twitter.com/elonmusk/status/1594131768298315777> (“Trump will be reinstated.”); FTC Letter (Nov. 21, 2022), *supra* n.9.

³⁸ *See* FTC Letter (Nov. 21, 2022), *supra* n.9.

C. The FTC’s Demands for All Elon Musk-related Communications and Other Inappropriate Demands

In total, the FTC has now sent Twitter well over a dozen demand letters since Musk acquired the company.³⁹ These letters include demands for both written narratives and document productions.⁴⁰ In one 10-week stretch, the FTC averaged one new letter and 35 new requests per week.⁴¹ In addition to their frequency, the breadth of many of these demands make them particularly—perhaps intentionally—burdensome.



For example, on November 30, the FTC demanded that Twitter produce every internal Twitter communication—“including but not limited to emails, memos, and Slack communications”—“relating to Elon Musk,” including all communications sent or received by Musk himself.⁴² This demand came after the FTC had already asked for all communications for three employees in one request⁴³ and eight search terms in another request for just Slack communications.⁴⁴ Based on a subsequent FTC letter to Twitter, it appears that the company combined the requests (i.e., limiting its search by the three custodians *and* the eight search terms *and* only Slack communications), which still produced more than 66,000 hits across 6,000 Slack channels.⁴⁵ This one example illustrates that the FTC’s collective demands presented a substantial burden on the company’s operations.

³⁹ See, e.g., *supra* n.17; Letter from FTC Staff Attorney, FTC Division of Enforcement to Twitter’s Head of Product, Legal, Twitter, Inc., No. C-4316 (Jan. 23, 2023); FTC Letter (Feb. 1, 2023), *supra* n.6.

⁴⁰ *Id.*

⁴¹ See *supra* n.17.

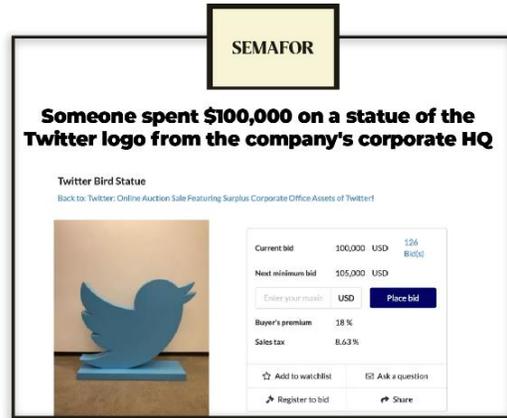
⁴² Request 17, FTC Letter (Nov. 30, 2022), *supra* n.6; Request 1, FTC Letter (Feb. 1, 2023), *supra* n.6.

⁴³ Request 6, FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9.

⁴⁴ *Id.*, Request 7.

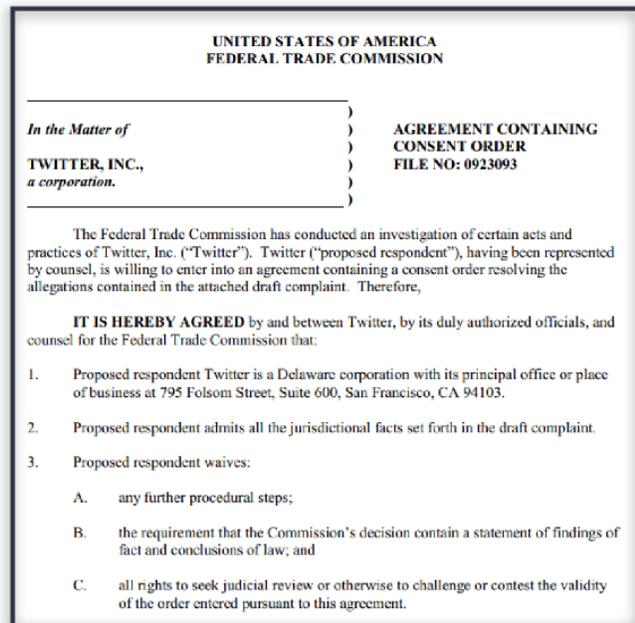
⁴⁵ See Request 4, FTC Letter (Dec. 6, 2022), *supra* n.17 (describing Twitter’s response dated November 25, 2022, and asking for additional communications from ten related sub-topics or custodians); see also *id.*, Request 3.

In other invasive demands, the FTC has demanded to know Twitter’s explanation for firing Jim Baker, a former FBI General Counsel who helped to censor the Hunter Biden laptop story on Twitter as a company executive in October 2020.⁴⁶ The FTC even demanded information about “whether, as part of its reduction in workforce or other cost-cutting measures, Twitter is also selling its office equipment.”⁴⁷



D. The FTC’s Reliance on Its Existing Consent Decree Is a Pretext to Harass Twitter

In 2022, FTC Chair Lina Khan claimed to the Committee the FTC “acts only in the public interest” and is “confined by [its] statutory authorities”⁴⁸ as the FTC considered whether to use its enforcement authority against Twitter in the wake of Musk’s potential acquisition of the company. The information obtained by the Committee makes clear that the FTC has inappropriately stretched its regulatory power to harass Twitter. The FTC is doing so consistent with the approach that partisan actors and interest groups have urged it to do: misusing a revised consent decree between the FTC and Twitter to justify its campaign of harassment.



⁴⁶ Request 4, FTC Letter (Dec. 9, 2022), *supra* n.8.

⁴⁷ Request 13, FTC Letter (Dec. 13, 2022), *supra* n.5.

⁴⁸ Response from FTC Chair Lina Khan to Ranking Member Jim Jordan (May 6, 2022) (attached hereto as App. 7).

In a 2011 consent agreement, Twitter settled claims that the company had improper safeguards against unauthorized access to users' personal information.⁴⁹ Twitter agreed to monitoring to ensure the platform maintained and protected user information in the future.⁵⁰ The limited nature of the settlement concerned "the security, privacy, and confidentiality of nonpublic consumer information."⁵¹ In a subsequent settlement in May 2022, Twitter paid a fine and agreed to implement a privacy and information security program by November 22, 2022, on account of violating the 2011 consent decree in this regard.⁵²

Twitter's May 2022 settlement concerned conduct that predated Musk's acquisition of Twitter and was limited in scope to the company's misuse of consumers' email addresses and phone numbers.⁵³ Like similar misconduct by Facebook, Twitter self-reported that it had collected consumers' telephone numbers and email addresses for security purposes, such as for account recovery or for two-factor authentication, but failed to disclose to users that it would also use that consumer information for targeted advertising.⁵⁴

II. LIMITATIONS ON USE OF TELEPHONE NUMBERS OR EMAIL ADDRESSES SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives must not use, provide access to, or disclose, for the purpose of serving advertisements, any telephone number or email address obtained from a User before the effective date of this Order for the purpose of enabling an account security feature (e.g., two-factor authentication, password recovery, re-authentication after detection of suspicious or malicious activity). Nothing in Provision II will limit Respondent's ability to use, provide access to, or disclose such telephone numbers or email addresses if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

Although each of the counts against Twitter related only to this specific fact pattern,⁵⁵ the FTC's enforcement actions in wake of news of Musk's acquisition of Twitter have not been so limited. Just two weeks after Musk's acquisition, the FTC publicly announced that it was "tracking recent developments at Twitter with deep concern" and warned that the "revised

⁴⁹ Press Release, *FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information*, FTC (Mar. 11, 2011).

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² Press Release, *FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads*, FTC (May 25, 2022); see FTC Order, *supra* n.4; Stipulated Order, *supra* n.4.

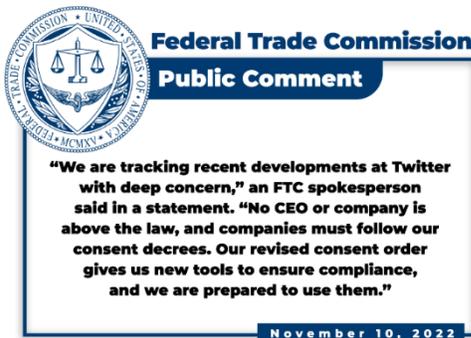
⁵³ *Id.*

⁵⁴ *Concurring Statement of Commissioner Christine S. Wilson and Commissioner Noah Joshua Phillips*, Matter No. 2023062 (Twitter), FTC (May 25, 2022) ("Twitter allegedly collected telephone numbers and email addresses from consumers for security purposes, but then used that information for targeted advertisements") (attached hereto as App. 8); *but see Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter*, Matter No. 2023062 (Twitter), FTC (May 25, 2022) (attached hereto as App. 9).

⁵⁵ See *United States v. Twitter, Inc.*, No. 3:22-cv-3070 (N.D. Cal. May 26, 2022), ECF No. 1, at ¶¶ 60-75; see also *Concurring Statement of Commissioner Christine S. Wilson and Commissioner Noah Joshua Phillips*, *supra* n.54 ("This Twitter order includes a data use restriction tied to the core allegation of illegality in the complaint: the company may not use for advertising any phone numbers or email addresses that had been gathered for security purposes.").

consent order gives us new tools to ensure compliance, and we are prepared to use them.”⁵⁶ That same day, citing its consent decree with the company, the FTC began its barrage of demands of Twitter with two letters including over a dozen specific demands to the company.⁵⁷

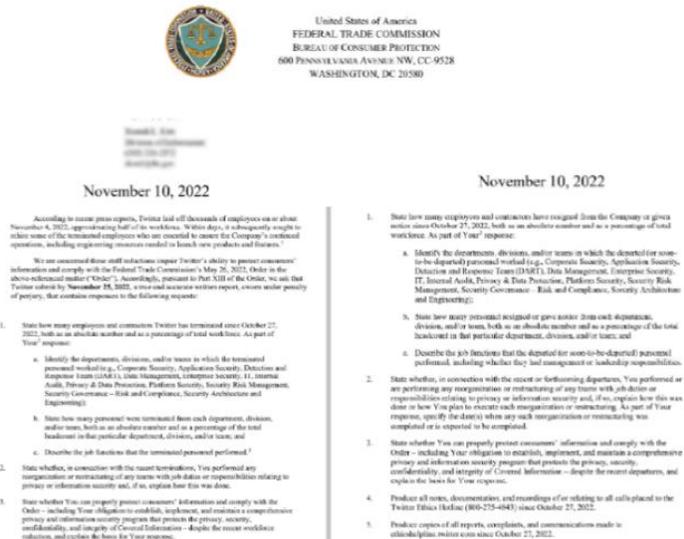
The timing of the FTC’s actions strongly suggests that its reliance on the consent decree is a pretext. Musk acquired Twitter on October 27, 2022.⁵⁸ Two weeks later, on November 10, the FTC sent two letters with over a dozen requests.⁵⁹ But Twitter’s new privacy and information security program—*i.e.*, the program ostensibly providing the main basis for the FTC’s demands—did not have to be established and implemented until November 22, per the terms of an FTC order from May 2022.⁶⁰



Federal Trade Commission
Public Comment

“We are tracking recent developments at Twitter with deep concern,” an FTC spokesperson said in a statement. “No CEO or company is above the law, and companies must follow our consent decrees. Our revised consent order gives us new tools to ensure compliance, and we are prepared to use them.”

November 10, 2022



United States of America
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION
600 PENNSYLVANIA AVENUE NW, CC-9528
WASHINGTON, DC 20580

November 10, 2022

According to recent press reports, Twitter laid off thousands of employees on or about November 4, 2022, representing half of its workforce. Where data is subsequently sought to relate some of the terminated employees who are essential to ensure the Company’s continued operations, including engineering resources needed to launch new products and features.

We are concerned these staff reductions impair Twitter’s ability to protect consumers’ information and comply with the Federal Trade Commission’s May 26, 2022, Order in the above-referenced matter (“Order”), accordingly, pursuant to Part XII of the Order, we ask that Twitter submit by November 24, 2022, a new and accurate written report, a new and/or update policy, that contain responses to the following requests:

1. State how many employees and contractors have terminated since October 27, 2022, both as an absolute number and as a percentage of total workforce. As part of Your response:
 - a. Identify the departments, divisions, and/or teams in which the terminated personnel worked (e.g., Content Security, Application Security, Detection and Response Team (DART), Job Management, Information Security, IT, Internal Audit, Privacy & Data Protection, Platform Security, Security Risk Management, Security Governance—Risk and Compliance, Security Architecture and Engineering).
 - b. State how many personnel were terminated from each department, division, and/or team, both as an absolute number and as a percentage of the total headcount in that particular department, division, and/or team, and
 - c. Describe the job functions that the terminated personnel performed.¹
2. State whether, in connection with the recent terminations, You performed any reorganization or restructuring of any team with job duties or responsibilities relating to privacy or information security and, if so, explain how this was done.
3. State whether You can properly protect consumers’ information and comply with the Order—including Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information—despite the recent workforce reduction, and explain the basis for Your response.

1. State how many employees and contractors have resigned from the Company or given notice since October 27, 2022, both as an absolute number and as a percentage of total workforce. As part of Your response:
 - a. Identify the departments, divisions, and/or teams in which the departed (or soon-to-be-departed) personnel worked (e.g., Content Security, Application Security, Detection and Response Team (DART), Job Management, Information Security, IT, Internal Audit, Privacy & Data Protection, Platform Security, Security Risk Management, Security Governance—Risk and Compliance, Security Architecture and Engineering).
 - b. State how many potential resignal or gave notice from each department, division, and/or team, both as an absolute number and as a percentage of the total headcount in that particular department, division, and/or team, and
 - c. Describe the job functions that the departed (or soon-to-be-departed) personnel performed, including whether they had management or leadership responsibilities.
2. State whether, in connection with the recent or forthcoming departures, You performed or are performing any reorganization or restructuring of any team with job duties or responsibilities relating to privacy or information security and, if so, explain how this was done or how You plan to execute such reorganization or restructuring. As part of Your response, specify the date(s) when any such reorganization or restructuring was completed or is expected to be completed.
3. State whether You can properly protect consumers’ information and comply with the Order—including Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information—despite the recent departures, and explain the basis for Your response.
4. Produce all notes, documents, and recordings of or relating to all calls placed to the Twitter Ethics Hotline (800-275-6843) since October 27, 2022.
5. Produce copies of all reports, complaints, and communications made to whistleblower review since October 27, 2022.

In other words, the FTC started this heavy-handed compliance monitoring two weeks after Musk acquired Twitter, but two weeks before there was even a program in place to monitor. In fact, the FTC sent a total of four demand letters, which included over two dozen requests, before the deadline that the FTC imposed.⁶¹

V. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, **must, within one hundred eighty (180) days of issuance of this Order, establish and implement, and thereafter maintain a comprehensive privacy and information security program (the “Program”) that protects the privacy, security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must at a minimum:**

⁵⁶ Brad Dress, *FTC says it’s ‘tracking the developments at Twitter with deep concern’*, THE HILL (Nov. 10, 2022).
⁵⁷ See FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10.
⁵⁸ Thomas Barrabi and Theo Wray, *Elon Musk completes \$44B Twitter takeover, begins firing execs*, N.Y. POST (Oct. 27, 2022).
⁵⁹ See FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10.
⁶⁰ See Sec. V, FTC Order, *supra* n.4.
⁶¹ See FTC Letter Regarding Twitter Blue and Resignations (Nov. 10, 2022), *supra* n.9; FTC Letter Regarding Terminations (Nov. 10, 2022), *supra* n.10; FTC Letter (Nov. 15, 2022), *supra* n.17; FTC Letter (Nov. 21, 2022), *supra* n.9.

II. THE FTC'S ACTIONS APPEAR TO BE THE RESULT OF LEFT-WING PRESSURE

Elon Musk's acquisition of Twitter, and his affirmation of online freedom of speech, generated an enormous amount of backlash among elected officials and activists on the left.⁶² In response to the acquisition, key voices on the left called for the federal government to intervene to "block" the purchase. Some groups, including the organization where FTC Chair Khan once worked, urged the FTC to use the existing consent decree with Twitter as a vehicle to attempt to thwart Musk's efforts to reorient the company. As this report shows, the FTC did just that.

The pressure campaign began almost immediately after Musk announced his interest in purchasing Twitter. Some in Congress criticized the planned acquisition and Musk's intention to allow more speech on the platform. In May 2022, then-Judiciary Committee Chairman Jerrold Nadler (D-NY) lamented Musk's proposed changes to content moderation, warning it would allow so-called "disinformation" to proliferate.⁶³ Congressman David Cicilline (D-RI), then-Chairman of the House Antitrust Subcommittee, criticized the acquisition, saying "there are a lot of reasons to be concerned."⁶⁴ Congresswoman Alexandria Ocasio-Cortez (D-NY) claimed without any evidence that Musk's takeover of Twitter would precipitate an "explosion of hate crimes."⁶⁵ Not to be outdone, Senator Elizabeth Warren (D-MA) decried the deal as "dangerous for our democracy."⁶⁶



⁶² See, e.g., Jordan Boyd, *The Left Is Freaking Out Over Elon Musk Because Twitter Rigs The Game For Democrats*, THE FEDERALIST (Apr. 14, 2022); Ben Weingarten, *Elon Musk's Battle For Twitter Is A Proxy War For Americans Against The Ruling Class*, THE FEDERALIST (Apr. 20, 2022); Brian Schwartz, *Biden officials worry Musk will allow Trump to return to Twitter*, CNBC (Apr. 25, 2022); Mike Lillis, *Democrats sound alarm about Musk bringing Trump back to Twitter*, THE HILL (May 13, 2022).

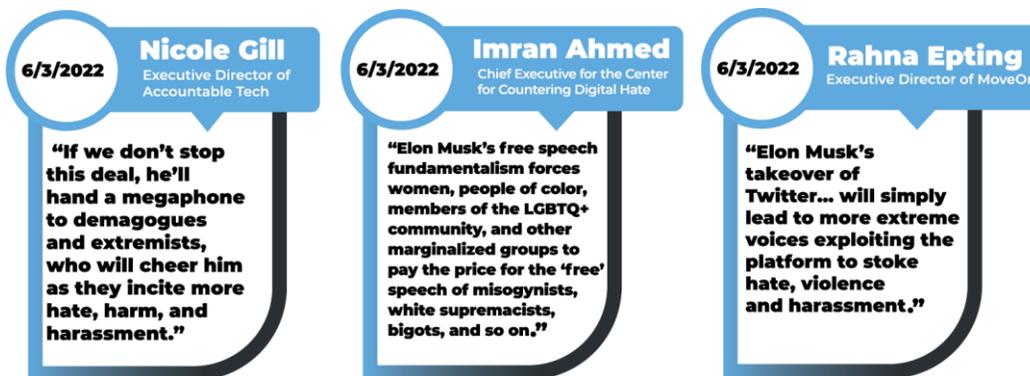
⁶³ Karl Herchenroeder, *Musk Twitter Deal Renews Partisan Debate Over Speech*, COMM'NS DAILY (May 2, 2022).

⁶⁴ *Antitrust Chair Cicilline on Big Tech Bill in Limbo*, BLOOMBERG (Aug. 22, 2022).

⁶⁵ Alexandria Ocasio-Cortez (@AOC), TWITTER (Apr. 29, 2022, 2:41 PM), <https://twitter.com/AOC/status/1520111152411389954>.

⁶⁶ Elizabeth Warren (@SenWarren), TWITTER (Apr. 25, 2022, 5:22 PM), <https://twitter.com/SenWarren/status/1518702084048179200>.

Organizations on the left immediately mobilized against Musk, creating a “Stop the Deal” website to serve as the hub for the “multi-pronged effort.”⁶⁷ This pro-censorship coalition mischaracterized Musk’s commitment to the First Amendment, warned of a parade of horrors, and initiated a litany of personal attacks, including:



These organizations demanded that the FTC and other federal agencies act quickly to prevent Musk’s acquisition of Twitter.⁶⁸

The Open Markets Institute (OMI), a left-wing political advocacy organization where current FTC Chair Lina Khan used to work,⁶⁹ urged regulators at the FTC to “block” the purchase.⁷⁰ At the time, Judiciary Committee Republicans investigated whether the FTC had inappropriate coordination with third parties about its response to Musk’s acquisition of Twitter, which the FTC denied.⁷¹ The FTC, however, refused to disclose its communications with the White House.⁷²

On October 27, 2022, Musk completed the purchase and officially became the CEO of Twitter.⁷³ Again, left-wing hysteria erupted immediately. OMI released a public statement claiming that Musk’s ownership of Twitter “poses a number of immediate and direct threats to American democracy, free speech, and national security.”⁷⁴ OMI asserted that “the deal violates existing law” and that the FTC and other regulators “have ample authority to block it.”⁷⁵ A few weeks later, OMI sent a letter to FTC Chair Khan, Jonathan Kanter, Assistant Attorney General

⁶⁷ *Stop The Deal: Nonprofit Coalition Launches Campaign Against Elon Musk’s Twitter Takeover*, ACCOUNTABLE TECH (June 3, 2022), <https://accountabletech.org/media/stop-the-deal-nonprofit-coalition-launches-campaign-against-elon-musks-twitter-takeover/>; *see also* Letter from Accountable Tech and others to Twitter’s Advertisers (May 3, 2022), *supra* n.30 (attached hereto as App. 6).

⁶⁸ *Id.*

⁶⁹ Nancy Scola, *How a liberal think tank is driving 2020 Dems to crack down on Big Tech*, POLITICO (June 14, 2019).

⁷⁰ *See* Barry Lynn, *OMI Statement on Elon Musk and Twitter*, OPEN MARKETS INSTITUTE (Apr. 26, 2022) (attached hereto as App. 10).

⁷¹ Response from FTC Chair Lina Khan to Ranking Member Jim Jordan (May 6, 2022) (attached hereto as App. 7).

⁷² Response from FTC Chair Lina Khan to Ranking Member Jim Jordan and others (June 24, 2022) (attached hereto as App. 11).

⁷³ Thomas Barrabi and Theo Wayt, *Elon Musk completes \$44B Twitter takeover, begins firing execs*, N.Y. POST (Oct. 27, 2022).

⁷⁴ Barry Lynn, *Open Markets Institute Statement in response to Elon Musk Buying Twitter*, OPEN MARKETS INSTITUTE (Oct. 27, 2022) (attached hereto as App. 12).

⁷⁵ *Id.*

of the Antitrust Division at the Department of Justice (DOJ), and Jessica Rosenworcel, Chair of the Federal Communications Commission (FCC), demanding that each of their offices “fully investigate Elon Musk’s takeover of the communications platform Twitter” because the U.S. government should be “using *every* existing authority” at its disposal.⁷⁶ OMI conceded that “FTC enforcement of its consent decree with Twitter on privacy” is “not sufficient,” and “that this deal does not fit easily into some of the categories your agencies have relied on in recent years to determine when and how to investigate takeovers or certain corporate actions”;⁷⁷ but OMI assured the FTC, DOJ, and the FCC that they have very “ample authority to fully review this takeover, and if necessary to unwind or restructure the deal and/or regulate the actions of the combined corporations.”⁷⁸

Another fourteen left-wing organizations—including the Center for American Progress, Common Cause, MoveOn, and Public Citizen—demanded that the FTC investigate whether Musk had already “violate[d] the company’s existing consent decree.”⁷⁹ Partisan activists agreed, publicly advocating that the consent decree provided sufficient legal grounds for the FTC to achieve the left’s political ends.⁸⁰



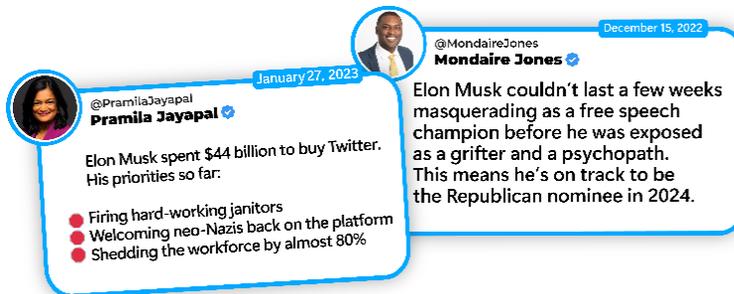
⁷⁶ Letter from OMI to FTC, DOJ, and FCC (Nov. 16, 2022) (emphasis in original) (attached hereto as App. 13).

⁷⁷ *Id.*

⁷⁸ *Id.* For good measure, OMI also noted that “[a]t least six other departments, agencies, and offices have a responsibility to work with [the FTC, DOJ, and the FCC] on a thorough investigation of Mr. Musk’s takeover and management of Twitter, and his management of Starlink: the Committee on Investment in the United States (CFIUS), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (CFPB), the Department of Defense, the Department of Treasury, and the Federal Reserve.”

⁷⁹ *The FTC, Congress, and Advertisers Must Hold Elon Musk and Twitter Accountable, Say Progressive Groups*, AMERICAN PROGRESS (Dec. 21, 2022) (attached hereto as App. 14).

⁸⁰ See, e.g., Brian Fung, *Musk’s Twitter may have already violated its latest FTC consent order, legal experts say*, CNN (Nov. 11, 2022).



Following the completed acquisition, Democrats in Washington renewed their pressure campaign.⁸¹ Seven Democrat senators issued a joint press release calling for the FTC to investigate Musk’s so-called “alarming steps” at Twitter.⁸² These senators demanded that the FTC “vigorously oversee its consent decree” with Twitter, and outlined the different purported grounds on which Elon Musk could have already violated the terms of the decree in his first few weeks of ownership.⁸³ Even President Biden signaled support for government intervention, saying that “there’s a lot of ways” the government could review the transaction.⁸⁴



While efforts to have other agencies “block” the deal failed,⁸⁵ the persistent, fever-pitched pressure campaign by left-wing activists and Democrats implored the FTC to use the user-privacy consent decree as a cudgel against Twitter. It appears that the FTC has done exactly that.

⁸¹ See, e.g., Pramila Jayapal (@PramilaJayapal), TWITTER (Jan. 27, 2023, 2:08 PM), <https://twitter.com/PramilaJayapal/status/1619049608960741381>; Mondaire Jones (@MondaireJones), TWITTER (Dec. 15, 2022, 10:13 PM), <https://twitter.com/MondaireJones/status/1603589202867884034>; *Klobuchar After Musk Takeover: Twitter Is 'Making Money Off Of This Violence'*, NBC News, YOUTUBE (Oct. 30, 2022)

<https://www.youtube.com/watch?v=UJRKDvyeHSU> (Senator Amy Klobuchar, Chair of the Senate Judiciary Subcommittee on Competition Policy, Antitrust, and Consumer Rights, stated after the acquisition that she did not trust Musk to run Twitter, and lamented that Musk was spreading “pro-Trump, [Make America Great Again]-crowd rhetoric).

⁸² Letter from Democratic Senators to FTC Chair Lina Khan (Nov. 17, 2022) (attached hereto as App. 15).

⁸³ *Id.*

⁸⁴ Rebecca Kern, *Musk's foreign investors in Twitter are 'worthy' of review, Biden says*, POLITICO (Nov. 9, 2022).

⁸⁵ In addition to the FTC, the FBI was also involved in reviewing the transfer of Twitter’s ownership, with officials looking “into the potential counterintelligence risks posed by the deal.” Faiz Siddiqui, Jeff Stein, and Joseph Menn, *U.S. exploring whether it has authority to review Musk’s Twitter deal*, WASH. POST (Nov. 2, 2022). And just days before the deal ultimately went through, there were reports that the Biden Administration would consider subjecting

III. CONCLUSION

Our democratic republic depends on American citizens having the right to express themselves freely in the town square, whether that forum is in person or in a digital space. As Justice Brandeis counseled almost a century ago, the best remedy for false speech is “more speech, not enforced silence.”⁸⁶ Elon Musk recognizes this truth and he has reshaped Twitter to revitalize freedom of speech online.

The FTC wields enormous authority to regulate large swaths of the modern American economy. The information presented in this interim staff report demonstrates the threat posed by wildly inappropriate use of this power. The FTC has no business demanding to know with which journalists a private company is communicating. The FTC has no need for all of Twitter’s communications related to its CEO. And yet, on the basis of an existing consent decree about user privacy, the FTC made these demands—and more—of Twitter. These demands should be exposed for what they are: pure and absolute attempts to harass, intimidate, and target an American business.

The Committee and the Select Subcommittee remain steadfast in our mission to investigate the weaponization of the federal government and to pursue legislative reforms to stop it.

the deal to review by the Committee on Foreign Investment in the United States (CFIUS), an interagency panel led by the Treasury Department, which involves DHS, the State Department, and the Defense Department, among others. Jennifer Jacobs and Saleha Mohsin, *Twitter Tumbles as US Weighs Security Reviews for Musk Deals*, BLOOMBERG (Oct. 20, 2022). This reporting was followed by Twitter’s stock plunging five percent and jeopardized the deal. *Id.* And even though, on November 15—weeks after the deal went through—Secretary of the Treasury Janet Yellen said “[w]e really have no basis – to the best of my knowledge – to examine [Musk’s] finances of his company” she had to walk back her statements, claiming on November 30 that “it would be appropriate for CFIUS to take a look” at the Twitter deal. Christopher Condon and Gregory Korte, *Janet Yellen changes course and says she ‘misspoke’ when she said there was ‘no basis’ for the government to review Elon Musk’s Twitter buy*, FORTUNE (Nov. 30, 2022).

⁸⁶ *Whitney v. California*, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

APPENDIX

Appendix 1 – House Resolution 12, 118th Congress

Appendix 2 – May 4, 2022 Letter from Ranking Member Jim Jordan to FTC Chair Lina Khan

Appendix 3 – May 24, 2022 Letter from Congressman Scott Fitzgerald, Ranking Member Jim Jordan, et al. to FTC Chair Lina Khan

Appendix 4 – *In the Matter of Twitter, Inc.*, No. C-4316, FTC Decision and Order (May 2022)

Appendix 5 – *United States v. Twitter, Inc.*, No. 3:22-cv-3070 (N.D. Cal. May 26, 2022), ECF No. 11 (Stipulated Order)

Appendix 6 – May 3, 2022 Letter from Accountable Tech and others to Twitters’ Advertisers

Appendix 7 – May 6, 2022 Response from FTC Chair Lina Khan to Ranking Member Jim Jordan

Appendix 8 – FTC Matter No. 2023062 (Twitter), Concurring Statement of Commissioner Christine S. Wilson and Commissioner Noah J. Phillips

Appendix 9 – FTC Matter No. 2023062 (Twitter), Statement of Chair Lina M. Khan Joined by Commissioner Rebecca K. Slaughter

Appendix 10 – Statement from the Open Markets Institute (April 2022)

Appendix 11 – June 24, 2022 Response from FTC Chair Khan to Ranking Member Jim Jordan

Appendix 12 – Statement from the Open Markets Institute (Oct. 2022)

Appendix 13 – Nov. 16, 2022 Letter from the Open Markets Institute to FTC, DOJ, and FCC

Appendix 14 – Statement from Progressive Groups to the FTC, Congress, and Advertisers (Dec. 21, 2022)

Appendix 15 – Nov. 17, 2022 Letter from Democratic Senators to FTC Chair Khan

Appendix 1

.....
(Original Signature of Member)

118TH CONGRESS
1ST SESSION

H. RES.

Establishing a Select Subcommittee on the Weaponization of the Federal Government as a select investigative subcommittee of the Committee on the Judiciary.

IN THE HOUSE OF REPRESENTATIVES

Mr. JORDAN submitted the following resolution; which was referred to the Committee on _____

RESOLUTION

Establishing a Select Subcommittee on the Weaponization of the Federal Government as a select investigative subcommittee of the Committee on the Judiciary.

1 *Resolved,*

2 **SECTION 1. SELECT SUBCOMMITTEE ON THE**
3 **WEAPONIZATION OF THE FEDERAL GOVERN-**
4 **MENT.**

5 (a) ESTABLISHMENT; COMPOSITION.—

6 (1) ESTABLISHMENT.—There is hereby estab-
7 lished for the One Hundred Eighteenth Congress a
8 select investigative subcommittee of the Committee

1 on the Judiciary called the Select Subcommittee on
2 the Weaponization of the Federal Government (here-
3 inafter referred to as the “select subcommittee”).

4 (2) COMPOSITION.—

5 (A) The select subcommittee shall be com-
6 posed of the chair and ranking minority mem-
7 ber of the Committee on the Judiciary, together
8 with not more than 13 other Members, Dele-
9 gates, or the Resident Commissioner appointed
10 by the Speaker, of whom not more than 5 shall
11 be appointed in consultation with the Minority
12 Leader. The Speaker shall designate one mem-
13 ber of the select subcommittee as its chair. Any
14 vacancy in the select subcommittee shall be
15 filled in the same manner as the original ap-
16 pointment.

17 (B) Each member appointed to the select
18 subcommittee shall be treated as though a
19 member of the Committee on the Judiciary for
20 purposes of the select subcommittee.

21 (b) INVESTIGATIVE FUNCTIONS AND AUTHORITY.—

22 (1) INVESTIGATIVE FUNCTIONS.—The select
23 subcommittee is authorized and directed to conduct
24 a full and complete investigation and study and, not
25 later than January 2, 2025, issue a final report to

1 the House of its findings (and such interim reports
2 as it may deem necessary) regarding—

3 (A) the expansive role of Article II author-
4 ity vested in the Executive Branch to collect in-
5 formation on or otherwise investigate citizens of
6 the United States, including ongoing criminal
7 investigations;

8 (B) how executive branch agencies work
9 with, obtain information from, and provide in-
10 formation to the private sector, non-profit enti-
11 ties, or other government agencies to facilitate
12 action against American citizens, including the
13 extent, if any, to which illegal or improper, un-
14 constitutional, or unethical activities were en-
15 gaged in by the Executive Branch or private
16 sector against citizens of the United States;

17 (C) how executive branch agencies collect,
18 compile, analyze, use, or disseminate informa-
19 tion about citizens of the United States, includ-
20 ing any unconstitutional, illegal, or unethical
21 activities committed against citizens of the
22 United States;

23 (D) the laws, programs, and activities of
24 the Executive Branch as they relate to the col-
25 lection of information on citizens of the United

1 States and the sources and methods used for
2 the collection of information on citizens of the
3 United States;

4 (E) any other issues related to the viola-
5 tion of the civil liberties of citizens of the
6 United States; and

7 (F) any other matter relating to informa-
8 tion collected pursuant to the investigation con-
9 ducted under this paragraph at any time during
10 the One Hundred Eighteenth Congress.

11 (2) AUTHORITY.—

12 (A) The select subcommittee may report to
13 the House or any committee of the House from
14 time to time the results of its investigations and
15 studies, together with such detailed findings
16 and legislative recommendations as it may deem
17 advisable.

18 (B) Any markup of legislation shall be held
19 at the full Committee level consistent with
20 clause 1(l) of rule X of the Rules of the House
21 of Representatives.

22 (c) PROCEDURE.—

23 (1) Rule XI of the Rules of the House of Rep-
24 resentatives and the rules of the Committee on the
25 Judiciary shall apply to the select subcommittee in

1 the same manner as a subcommittee except as fol-
2 lows:

3 (A) The chair of the select subcommittee
4 may, after consultation with the ranking minor-
5 ity member, recognize—

6 (i) members of the select sub-
7 committee to question a witness for periods
8 longer than five minutes as though pursu-
9 ant to clause 2(j)(2)(B) of such rule XI;
10 and

11 (ii) staff of the select subcommittee to
12 question a witness as though pursuant to
13 clause 2(j)(2)(C) of such rule XI.

14 (B) The Committee on the Judiciary (or
15 the chair of the Committee on the Judiciary, if
16 acting in accordance with clause 2(m)(3)(A)(i)
17 of rule XI) may authorize and issue subpoenas
18 to be returned at the select subcommittee.

19 (C) With regard to the full scope of inves-
20 tigative authority under subsection (b)(1), the
21 select subcommittee shall be authorized to re-
22 ceive information available to the Permanent
23 Select Committee on Intelligence, consistent
24 with congressional reporting requirements for
25 intelligence and intelligence-related activities,

1 and any such information received shall be sub-
2 ject to the terms and conditions applicable
3 under clause 11 of rule X.

4 (2) The provisions of this resolution shall gov-
5 ern the proceedings of the select subcommittee in
6 the event of any conflict with the rules of the House
7 or of the Committee on the Judiciary.

8 (d) SERVICE.—Service on the select subcommittee
9 shall not count against the limitations in clause 5(b)(2)(A)
10 of rule X of the Rules of the House of Representatives.

11 (e) SUCCESSOR.—The Committee on the Judiciary is
12 the “successor in interest” to the select subcommittee for
13 purposes of clause 8(c) of rule II of the Rules of the House
14 of Representatives.

15 (f) SUNSET.—The select subcommittee shall cease to
16 exist 30 days after filing the final report required under
17 subsection (b).

Appendix 2

ONE HUNDRED SEVENTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6216
(202) 225-3951
judiciary.house.gov

May 4, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chair Khan:

The day after Twitter’s board of directors agreed to sell Twitter to Mr. Elon Musk, the Open Markets Institute (OMI), an extreme left-wing political advocacy organization,¹ called on Biden regulators at the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and the Justice Department to “block” the purchase.² We are concerned that OMI—where you were previously employed as Legal Director³—may be trying to leverage its close relationship with you to take action to further limit free speech online. The author of OMI’s statement has called you a “dear friend,” a “close colleague,” and someone who “understands the nature of the crisis and how to use existing law and authority to master it.”⁴

¹ One commentator has noted that “OMI’s loudest voices are largely unencumbered by economic or legal education” Nancy Scola, *How a liberal think tank is driving 2020 Dems to crack down on Big Tech*, POLITICO (June 14, 2019), <https://www.politico.com/story/2019/06/14/open-market-institute-silicon-valley-monopolies-1507673>. And it has been reported that the author of OMI’s statement recently participated in the Antitrust Section Spring Meeting of the American Bar Association and “rattled off a list of social ills, including outsized influence of tech companies, environmental problems and wealth inequality.” Christine S. Wilson, *Marxism and Critical Legal Studies Walk into the FTC: Deconstructing the Worldview of the Neo-Brandeisians*, REMARKS FOR THE JOINT CONFERENCE ON PRECAUTIONARY ANTITRUST: THE RULE OF LAW AND INNOVATION UNDER ASSAULT 5 (Apr. 8, 2022) (citation omitted), https://www.ftc.gov/system/files/ftc_gov/pdf/Marxism%20and%20Critical%20Legal%20Studies%20Walk%20into%20the%20FTC%20Deconstructing%20the%20Worldview%20of%20the%20Neo-Brandeisians.pdf. He “told attendees that “[t]his all—to a great degree—[is] your doing. It is your doing because you conspired to use a false science, an idiot science, to blind the law to dangerous concentrations of power, to blind the citizenry to the fist of monopoly.”” *Id.* (first alternation in original) (citation omitted).

² See generally Press Release, OMI Statement on Elon Musk and Twitter (Apr. 26, 2022), <https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/6268076a3b1aa57bfcdbd0487/1650984811013/OMI+Musk+and+Twitter.pdf>.

³ See Press Release, Lina Khan’s Confirmation as Commissioner on the Federal Trade Commission is Momentous (June 15, 2021), <https://www.openmarketsinstitute.org/publications/lina-khans-confirmation-as-commissioner-on-the-federal-trade-commission-is-momentous>.

⁴ *Id.*

OMI claims without evidence that Mr. Musk’s purchase is a “threat to free communications and debate in the United States.”⁵ In reality, Mr. Musk has proposed “softening [Twitter’s] stance on content moderation,” which will increase speech, and he has said that “Twitter should be more cautious when deciding to take down tweets or permanently ban users’ accounts.”⁶ OMI’s desire to restrict and suppress free speech online helps explain why it supports a package of ill-advised Democrat-led antitrust bills that will lead to more censorship, and thus less speech, in the digital arena.⁷

OMI appears to believe that the FTC will be receptive to its cavalier effort to influence a federal agency that is run by its former employee. It is true that the Biden FTC is moving to promote progressive values that undermine capitalism and threaten innovation.⁸ And under your leadership, the Biden FTC has sought to “recast[] antitrust law into a tool to enable government to control capitalism,”⁹ which disrupts free markets and is inconsistent with fundamental American freedoms. Perhaps this is why OMI seems to think it may have a friendly ear in the FTC.

To assist the Committee in its oversight of the FTC, please provide a written response to the following questions:

1. Did you or anyone else at the FTC solicit or play any role in drafting OMI’s statement?
2. Has the FTC taken any actions in response to the statement released by OMI?

Please answer these questions as soon as possible but no later than 5:00 p.m. on May 18, 2022.

⁵ Press Release, *supra* note 2, at 2.

⁶ Cara Lombardo et al., *Twitter Accepts Elon Musk’s Offer to Buy Company in \$44 Billion Deal*, WALL ST. J. (Apr. 25, 2022).

⁷ See Press Release, Open Markets Applauds New Bipartisan Legislation to Rein in Big Tech as Important First Step (June 11, 2021), <https://www.openmarketsinstitute.org/publications/open-markets-applauds-new-bipartisan-legislation-to-rein-in-big-tech-as-important-first-step>; Rep. Jim Jordan & Mark Meadows, Opinion, *Rep. Jim Jordan & Mark Meadows: Big Tech merged with Big Government – radical Dems’ bills would transform US*, FOX NEWS (June 22, 2021) (“Make no mistake, Big Tech is out to get conservatives and must be reined in. But these bills do nothing to fight Big Tech’s anti-conservative bias and censorship. These Democrat bills will only make things worse. If you think Big Tech is bad now, just wait until Apple, Amazon, Facebook and Google are working in collusion with Big Government.”).

⁸ See, e.g., Draft FTC Strategic Plan for FY 2022-2026, FTC, at 21 (Oct. 2021) (listing the objective to “[a]dvance racial equity, and all forms of equity, and support underserved and marginalized communities through the FTC’s competition mission”); Bryan Koenig, *Nontraditional Questions’ Appearing In FTC Merger Probes*, LAW 360 (Sept. 24, 2021) (“[W]hen quizzed about the need for the less traditional input, ‘staff have been unable to articulate how these issues relate to the agency’s mission to promote competition, leaving the outside world guessing as to the role they play in agency decision making” (citation omitted)), <https://www.law360.com/articles/1425218>.

⁹ Robert Bork Jr., *Why Free Thinkers Need to Block Lina Khan’s FTC Nomination*, REAL CLEAR MARKETS (June 15, 2021), https://www.realclearmarkets.com/articles/2021/06/15/why_free_thinkers_need_to_block_lina_khans_ftc_nomination_781419.html.

The Honorable Lina Khan

May 4, 2022

Page 3

Furthermore, this letter serves as a formal request to preserve all records and materials relating to Mr. Musk's pending acquisition of Twitter. You should construe this preservation notice as an instruction to take all reasonable steps to prevent the destruction or alteration, whether intentionally or negligently, of all documents, communications, and other information, including electronic information and metadata, that is or may be potentially responsive to this congressional inquiry. This instruction includes all electronic messages sent using your official and personal accounts or devices, including records created using text messages, phone-based message applications, or encryption software.

Thank you for your prompt attention to this matter.

Sincerely,

A handwritten signature in blue ink that reads "Jim Jordan". The signature is written in a cursive, flowing style.

Jim Jordan
Ranking Member

cc: The Honorable Jerrold L. Nadler, Chairman
The Honorable Noah J. Phillips, Commissioner, Federal Trade Commission
The Honorable Rebecca K. Slaughter, Commissioner, Federal Trade Commission
The Honorable Christine S. Wilson, Commissioner, Federal Trade Commission

Appendix 3

Congress of the United States
Washington, DC 20510

The Honorable Lina Khan
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

May 24, 2022

Dear Chair Khan:

We write to express concerns about the Federal Trade Commission's (FTC) approach to reviewing Elon Musk's \$44 billion purchase of Twitter given the recent politicization at the FTC.

Big Tech has been relentlessly attacking free speech over the past several years, and Twitter specifically has gained a reputation for heavy-handed censorship of conservative views that are not popular in Silicon Valley. These censorship activities undermine our country's First Amendment principles and poison public discourse. Mr. Musk has proposed reversing Twitter's harsh and one-sided content moderation policies and replacing them with a more measured approach that only removes clearly unlawful tweets and user accounts.¹

We are concerned that the politicization seen at the FTC during the Biden Administration will slow or even halt Twitter's moves toward more free speech under the leadership of Elon Musk. Since the start of the Administration, the Biden FTC has taken radical measures that abandon traditional procedures and norms of civility and bipartisanship, while pushing the limit of the statutory bounds Congress placed on it. Measures such as suspending early termination of merger review transactions with no competitive concerns for well over a year,² using a zombie vote to adopt prior approval for merging parties and divestiture buyers on future transactions for 10 years,³ and frequent use of pre-consummation warning letters have damaged the FTC's reputation as an unbiased enforcement agency.⁴

¹ Elon Musk, Twitter post, April 26, 2022, 3:33 p.m., <https://twitter.com/elonmusk/status/1519036983137509376?s=20&t=PB7uC6fFnUJHXjd5ZCtrFA>.

² Press Release, Fed. Trade Comm'n, FTC, DOJ Temporarily Suspend Discretionary Practice of Early Termination (Feb. 4, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/02/ftc-doj-temporarily-suspend-discretionary-practice-early-termination>.

³ Dissenting Statement of Commissioners Christine S. Wilson and Noah Joshua Phillips Regarding the Statement of the Commission on Use of Prior Approval Provisions in Merger Orders (Oct. 29, 2021), https://www.ftc.gov/system/files/documents/public_statements/1598095/wilson_phillips_prior_approval_dissenting_statement_102921.pdf.

⁴ Holly Vedova, Dir., Bureau of Competition, Adjusting merger review to deal with the surge in merger filings, FED. TRADE COMM'N COMPETITION MATTERS BLOG (Aug. 3, 2021), <https://www.ftc.gov/enforcement/competition-matters/2021/08/adjusting-merger-review-deal-surge-merger-filings>.

Even worse, the lack of transparency surrounding withdrawn enforcement guidance without replacing it with new rules of the road and moving away from the traditional “consumer welfare standard⁵” have led to fears of politicization of the FTC. These fears are validated when the FTC appears to take direction from the White House and partisan third-party organizations. Just a few months ago, the FTC heeded the White House’s call to investigate oil and gas companies for price gouging to distract from the Administration’s own policies that clamp down on domestic production.⁶ Even more recently, the Open Markets Institute’s call to block Mr. Musk’s purchase of Twitter coincided with your own investigation of the deal.⁷

Decisions related to Twitter’s governance will shape digital free speech in the years to come. In light of our concerns regarding the FTC’s politicization, and the risk that partisan pressures will encourage the FTC to continue exceeding its statutory authorities, we ask that you provide us with the following information:

1. All documents and communication between or among the Federal Trade Commission and any third-party organizations referring or relating to Mr. Musk’s purchase of Twitter;
2. All documents and communication between or among the Federal Trade Commission and members and staff of the White House Competition Council referring or relating to Mr. Musk’s purchase of Twitter;
3. All documents and communications, including all plans, proposals, or other communications, referring or relating to the FTC’s purpose in making inquiries related to Mr. Musk’s purchase of Twitter that deviate from typical reviews;

We ask that you respond to this inquiry no later than May 31st, 2022.

⁵ [The New Progressives Fight Against Consumer Welfare - WSJ](#)

⁶Letter to President Biden Calling Out Administration for Distracting from Disastrous Energy Policies, November 29, 2021, <https://fitzgerald.house.gov/media/press-releases/fitzgerald-armstrong-lead-house-colleagues-calling-out-biden-administrations>.

⁷ <https://republicans-judiciary.house.gov/wp-content/uploads/2022/05/2022-05-04-JDJ-to-FTC-Musk-purchase.pdf>.

Sincerely,



Scott Fitzgerald
Member of Congress



Jim Jordan
Ranking Member



Louie Gohmert
Member of Congress



Andy Biggs
Member of Congress



Dan Bishop
Member of Congress

Appendix 4

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Lina M. Khan, Chair**
 Noah Joshua Phillips
 Rebecca Kelly Slaughter
 Christine S. Wilson

In the Matter of

TWITTER, INC., a corporation.

DECISION AND ORDER

Docket No. C-4316

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed presenting the draft Complaint to the Commission. If issued, the draft Complaint would charge Respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 45(a)(1) and (l), 53(b), and 56(a)(1).

Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Respondent admits the facts necessary to establish jurisdiction.

The Commission considered the matter and determined that it had reason to believe Respondent has violated the Decision and Order the Commission previously issued in *In re Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011) and the FTC Act, and that a Complaint should issue stating its charges in that respect. After due consideration, the Commission issues the Complaint, makes the following Findings, and issues the following Order:

FINDINGS

1. Respondent Twitter, Inc. (“Twitter”) is a Delaware corporation with its principal office or place of business at 1355 Market Street, Suite 900, San Francisco, CA 94103.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.
3. The Complaint charges violations of Section 5 of the FTC Act, 15 U.S.C. § 45, and violations of Provision I of an order previously issued by the Commission, 15 U.S.C. § 56(a)(1).

4. Respondent waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.

5. Respondent and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

ORDER

DEFINITIONS

For the purpose of this Order, the following definitions apply:

A. **“Covered Incident”** means any instance affecting 250 or more Users in which: (1) any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization; or (2) individually identifiable Covered Information collected or received, directly or indirectly, by Respondent, was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization. “Covered Incident” does not include instances where the only unauthorized access, acquisition, or exposure was due to a User communicating through Respondent’s services (e.g., public tweets, protected tweets, retweets, or direct messages) information that was obtained from sources other than Respondent.

B. **“Covered Information”** means information from or about an individual consumer including, but not limited to: (1) a first or last name; (2) geolocation information sufficient to identify a street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging User identifier or a screen name; (4) a mobile or other telephone number; (5) photos and videos; (6) Internet Protocol (“IP”) address, User ID, or other persistent identifier that can be used to recognize a User over time and across different devices, websites, or online services; (7) a Social Security number; (8) a driver’s license or other government issued identification number; (9) financial account number; (10) credit or debit information; (11) date of birth; (12) biometric information; or (13) any information combined with any of (1) through (12) above. “Covered Information” does not include information that a User intends to make public using Respondent’s services.

C. **“Representatives”** means Respondent’s officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.

D. **“Resources”** means networks, systems, and software.

E. **“Respondent”** means Twitter, Inc. (“Twitter”), and its successors and assigns. For purposes of Parts V and VI, Respondent means Twitter, Inc., its successors and assigns, and any business that Respondent controls directly or indirectly, except for any business that: (1) does not provide services that are offered to U.S. residents; or (2) does not collect, maintain, use, disclose,

access, or provide access to the Covered Information of U.S. residents to enable Respondent's microblogging, social networking, or communications services.

F. **"Timeline Notice"** means a message Respondent places in a User's Twitter timeline (*i.e.*, the main screen the User sees when opening Twitter which displays a stream of tweets from accounts the User has chosen to follow) that stays near the top (*i.e.*, within the first five (5) tweets) of a User's Twitter timeline: (1) for at least six (6) months from the effective date of the Order; (2) until the User clicks on the "Learn More about your options" button embedded in the message; or (3) until the User scrolls past the message in their timeline, whichever occurs earlier.

G. **"User"** means an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent's products and services.

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Respondent and its Representatives, directly or through any corporation, subsidiary, division, website, mobile app, or other device, in connection with the offering of any product or service in or affecting commerce, must not misrepresent, in any manner, expressly or by implication, the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, misrepresentations related to:

A. Respondent's privacy and security measures to prevent unauthorized access to Covered Information;

B. Respondent's privacy and security measures to honor the privacy choices exercised by Users;

C. Respondent's collection, maintenance, use, disclosure, or deletion of Covered Information;

D. The extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls;

E. The extent to which Respondent makes or has made Covered Information accessible to any third parties;

F. The extent to which Respondent targets advertisements to Users or enables third parties to target advertisements to Users; or

G. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

II. LIMITATIONS ON USE OF TELEPHONE NUMBERS OR EMAIL ADDRESSES SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives must not use, provide access to, or disclose, for the purpose of serving advertisements, any telephone number or email address obtained from a User before the effective date of this Order for the purpose of enabling an account security feature (*e.g.*, two-factor authentication, password recovery, re-authentication after detection of suspicious or malicious activity). Nothing in Provision II will limit Respondent's ability to use, provide access to, or disclose such telephone numbers or email addresses if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

III. REQUIRED NOTICE TO CONSUMERS

IT IS FURTHER ORDERED that, within fourteen (14) days after the effective date of this Order, Respondent must provide a Timeline Notice to all current U.S. Users who joined Twitter prior to September 17, 2019, that states: “**Twitter’s Use of Your Personal Information for Tailored Advertising** As we stated on Oct. 8, 2019, we may have served you targeted ads based on an email address or phone number you provided to us to secure your account.”, and includes a “Learn more about your options” button that links to a webpage showing the information in Exhibit A.

IV. REQUIRED MULTI-FACTOR AUTHENTICATION OPTIONS

IT IS FURTHER ORDERED that, as of the effective date of this Order, Respondent must allow Users to utilize multi-factor authentication without providing a telephone number to access their Twitter accounts, such as by integrating authentication applications or allowing the use of security keys. The Company may use equivalent, widely-adopted industry authentication options that do not require Users to provide a telephone number and that are not multi-factor, if the person or persons responsible for the Program under Provision V.C: (1) approve(s) in writing the use of such equivalent authentication options; and (2) document(s) a written explanation of how the authentication options are widely-adopted and at least equivalent to the security provided by multi-factor authentication.

V. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, must, within one hundred eighty (180) days of issuance of this Order, establish and implement, and thereafter maintain a comprehensive privacy and information security program (the “Program”) that protects the privacy, security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Program;
- B. Provide the written program, and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing

body exists, to a senior officer of Respondent responsible for the Program at least once every calendar quarter;

C. Designate a qualified employee or employees to coordinate and be responsible for the Program;

D. Assess and document, at least once every twelve (12) months and promptly following the resolution of a Covered Incident (not to exceed ninety 90 days after the discovery of the Covered Incident), internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information that could result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondent identifies to the privacy, security, confidentiality, or integrity of Covered Information identified in response to Provision V.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, or destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information. Such safeguards must also include:

1. Prior to implementing any new or modified product, service, or practice that collects, maintains, uses, discloses, or provides access to Covered Information, conducting an assessment of the risks to the privacy, security, confidentiality, or integrity of the Covered Information;
2. For each new or modified product, service, or practice that does not pose a material risk to the privacy, security, confidentiality, or integrity of Covered Information, documenting a description of each reviewed product, service, or practice and why such product, service, or practice does not pose such a material risk;
3. For each new or modified product, service, or practice that poses a material risk to the privacy, security, confidentiality, or integrity of Covered Information, conducting a privacy review and producing a written report (“Privacy Review”) for each such new or modified product, service, or practice. The Privacy Review must:
 - (a) Describe how the product, service, or practice will collect, maintain, use, disclose, or provide access to Covered Information, and for how long;
 - (b) Identify and describe the types of Covered Information the product, service, or practice will collect, maintain, use, disclose, or provide access to;
 - (c) If the Covered Information will be collected from a User, describe the context of the interaction in which Respondent will collect such Covered Information (*e.g.*, under security settings, in pop-up messages in the timeline, or in response to a prompt reading, “Get Better Ads!”);

- (d) Describe any notice that Respondent will provide Users about the collection, maintenance, use, disclosure, or provision of access to the Covered Information;
- (e) State whether and how Respondent will obtain consent from Users for the collection, maintenance, use, disclosure, or provision of access to Covered Information;
- (f) Identify any privacy controls that will be provided to Users relevant to the collection, maintenance, use, disclosure, or provision of access to the Covered Information;
- (g) Identify any third parties to whom Respondent will disclose or provide access to the Covered Information;
- (h) Assess and describe the material risks to the privacy, security, confidentiality, and integrity of Covered Information presented by the product, service, or practice;
- (i) Assess and describe the safeguards to control for the identified risks, and whether any additional safeguards need to be implemented to control for such risks;
- (j) Explain the reasons why Respondent deems the notice and consent mechanisms described in Provisions V.E.3(d) and V.E.3(e) sufficient;
- (k) Identify and describe any limitations on the collection, maintenance, use, disclosure, or provision of access to Covered Information based on: (i) the context of the collection of such Covered Information; (ii) notice to Users; and (iii) any consent given by Users at the time of collection or through subsequent authorization;
- (l) Identify and describe any changes in how privacy and security-related options will be presented to Users, and describe the means and results of any testing Respondent performed in considering such changes, including but not limited to A/B testing, engagement optimization, or other testing to evaluate a User's movement through a privacy or security-related pathway;
- (m) Include any other safeguards or other procedures that would mitigate the identified risks to the privacy, security, confidentiality, and integrity of Covered Information that were not implemented, and each reason that such alternatives were not implemented; and
- (n) Include any decision or recommendation made as a result of the review (*e.g.*, whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);

4. Safeguards to prevent the collection, maintenance, use, disclosure, or access to Covered Information beyond the limitations identified in Provision V.E.3(k), including:
 - (a) Regular training, at least once a year, for any employees and independent contractors whose responsibilities include the collection, maintenance, disclosure, use, or provision of access to Covered Information, on the permissible collection, maintenance, disclosure, use, or provision of access to Covered Information and any related limitations;
 - (b) Written attestations by those employees and independent contractors that they will not collect, maintain, disclose, use, or provide access to the Covered Information in a manner inconsistent with those limitations;
 - (c) Designation of a senior officer, or senior level team composed of no more than five (5) persons, to be responsible for any decision to collect, maintain, use, disclose, or provide access to the Covered Information; and
 - (d) Treating any new method of collecting, maintaining, using, disclosing, providing access to, or deleting the Covered Information as a new or modified product, service, or practice requiring the reviews set forth in Provisions V.E.1-3;
 5. Regular privacy and information security training programs for all employees and independent contractors on at least an annual basis, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;
 6. Technical measures to monitor Respondent's Resources to identify unauthorized attempts to: (a) access, modify, or exfiltrate Covered Information from Respondent's Resources; or (b) access or take over Users' accounts; and
 7. Data access policies and controls for all: (a) databases storing Covered Information; (b) Resources that provide access to Users' accounts; and (c) Resources containing information that enables or facilitates access to Respondent's internal network and systems;
- F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information, and modify the Program based on the results;
- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, and modify the Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of Respondent's network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources; and (2) penetration testing of Respondent's network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision V.D of this Order, or any other circumstances that Respondent knows or has reason to believe may have an impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Program at least once every twelve (12) months and modify the Program based on the results.

VI. INDEPENDENT PROGRAM ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision V of this Order titled Mandated Privacy and Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)") who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the Program; (3) retain all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents relating to Respondent's compliance with this Order may be withheld from the Commission by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim. Respondent may obtain separate assessments for (1) privacy and (2) information security from multiple Assessors, so long as each of the Assessors meets the qualifications set forth above;

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion;

C. The reporting period for the Assessments must cover: (1) the first three-hundred-and-sixty-five (365) days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must, for the entire assessment period: (1) determine whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assess the effectiveness of Respondent's implementation and maintenance of Provisions V.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were

identified in any prior Assessment required by this Order; and (5) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Program and did not rely primarily on assertions or attestations by Respondent's management. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision V.E of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard; and

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062." All subsequent biennial Assessments must be retained by Respondent until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VII. COOPERATION WITH THIRD-PARTY ASSESSOR(S)

IT IS FURTHER ORDERED that Respondent and its Representatives, whether acting directly or indirectly, in connection with any Assessment required by Provision VI of this Order titled Independent Program Assessments by a Third Party, must:

- A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;
- B. Provide or otherwise make available to the Assessor information about Respondent's Resources(s) and all of Respondent's IT assets so that the Assessor can determine the scope of the Assessment, and have visibility to Resource(s) and IT assets deemed in scope; and
- C. Disclose all material facts to the Assessor(s), and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of Provisions V.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program.

VIII. CERTIFICATIONS

IT IS FURTHER ORDERED that Respondent must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for the Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification; and
- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062."

IX. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after Respondent's discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;
- C. A description of each type of Covered Information that was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;
- D. The number of Users whose Covered Information was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of any materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW,

Washington, DC 20580. The subject line must begin, “*In re Twitter, Inc.*, FTC File No. 202-3062.”

X. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For five (5) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities relating to the subject matter of this Order, and all agents and representatives who participate in any acts or practices subject to this Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order, which can be obtained electronically.

XI. COMPLIANCE REPORTING AND NOTICES

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

- A. Two-hundred and forty (240) days after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent: (1) identifies the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identifies all of Respondent’s businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes the activities of each business, including the goods and services offered and the means of advertising, marketing, and sales; (4) describes in detail whether and how Respondent is in compliance with each Provision of this Order; and (5) provides a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; (3) the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent.

C. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.

D. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “In re Twitter, Inc., FTC File No. 202-3062.”

XII. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person that Respondent contracts with directly and that provides services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies or records of all U.S. consumer complaints concerning the subject matter of the Order, and any responses to such complaints;

D. A copy of each unique advertisement or other marketing material making a representation subject to this Order;

E. A copy of each widely-disseminated representation by Respondent or its Representatives that describe the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, (1) statements relating to any change in any product, service, or practice that relates to the privacy, security, confidentiality, or integrity of such information, and (2) statements relating to: (a) Respondent’s privacy and security measures to prevent unauthorized access to Covered Information; (b) Respondent’s privacy and security measures to honor the privacy choices exercised by Users; (c) Respondent’s collection, maintenance, use, disclosure, or deletion of Covered Information; (d) the extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls; (e) the extent to which Respondent makes or has made Covered Information accessible to any third parties; (f) the extent to which Respondent allows third parties to serve advertisements to Users; or (g) the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules;

F. All materials relied upon in making the statements in Provisions XII.D and XII.E, and copies of each materially different notice provided to Users and mechanisms for obtaining a User's consent for the collection, use, or disclosure of Covered Information (including screenshots/screencasts and User interfaces, consent flows, and paths a User must take to reach such settings);

G. All materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

H. For 5 years from the date received, copies of all subpoenas, information provided in response to such subpoenas, and all material correspondence with law enforcement, if such communication relate to Respondent's compliance with this Order;

I. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order; and

J. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XIII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce records for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIV. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than twenty (20) years;
- B. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: May 26, 2022

Appendix 5

1
2 **UNITED STATES DISTRICT COURT**
3 **NORTHERN DISTRICT OF CALIFORNIA**

4 UNITED STATES OF AMERICA,

5 Plaintiff,

6 v.

7 TWITTER, INC., a corporation,

8 Defendant.

9 **Case No. 3:22-cv-3070 TSH**

10 **STIPULATED ORDER FOR**
11 **CIVIL PENALTY,**
12 **MONETARY JUDGMENT, AND**
13 **INJUNCTIVE RELIEF**

14 **STIPULATED ORDER FOR CIVIL PENALTY, MONETARY**
15 **JUDGMENT, AND INJUNCTIVE RELIEF**

16 The United States of America, acting upon notification and authorization to the Attorney
17 General by the Federal Trade Commission (“Commission” or “FTC”), filed its Complaint for
18 Civil Penalties, Permanent Injunction, and Other Equitable Relief (“Complaint”) in this matter
19 pursuant to Sections 5(a) and (l), 13(b), and 16(a)(1) of the Federal Trade Commission Act
20 (“FTC Act”), 15 U.S.C. §§ 45(a) and (l), 53(b), and 56(a)(1). Defendant has waived service of
21 the summons and the Complaint. Plaintiff and Defendant stipulate to the entry of this Stipulated
22 Order for Civil Penalty, Monetary Judgment, and Injunctive Relief (“Stipulated Order”) to
23 resolve the claims for civil penalties and injunctive relief set forth in the Complaint.

24 THEREFORE, IT IS ORDERED as follows:

25 **FINDINGS**

- 26 1. This Court has jurisdiction over the subject matter and all of the parties.
27 2. Venue is proper as to all parties in this District.
28 3. The Complaint states a claim upon which relief may be granted against Defendant under
Sections 5(a) and (l), 13(b), and 16(a)(1) of the FTC Act, 15 U.S.C. §§ 45(a), 45(l), 53(b), and

1 56(a)(1), including for violations of Part I of the Commission’s Decision and Order in *In re*
2 *Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. Mar. 2, 2011).

3 4. Defendant’s activities are “in or affecting commerce,” as defined in Section 4 of the FTC
4 Act, 15 U.S.C. § 44.

5 5. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28
6 U.S.C. § 2412, concerning the prosecution of this action through the date of this Stipulated
7 Order, and agrees to bear its own costs and attorney’s fees.

8 6. Defendant neither admits nor denies any of the allegations in the Complaint, except as
9 specifically stated in the Decision and Order set forth in Attachment A. Only for purposes of this
10 action, Defendant admits the facts necessary to establish jurisdiction.

11 7. Defendant and Plaintiff waive all rights to appeal or otherwise challenge or contest the
12 validity of this Stipulated Order.

13 **I. MONETARY JUDGMENT FOR CIVIL PENALTY**

14 IT IS FURTHER ORDERED that:

15 A. Judgment in the amount of ONE HUNDRED FIFTY MILLION dollars
16 (\$150,000,000.00) is entered in favor of Plaintiff against Defendant as a civil penalty pursuant to
17 Section 5(l) of the FTC Act, 15 U.S.C. § 45(l).

18 B. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of the
19 United States, ONE HUNDRED FIFTY MILLION dollars (\$150,000,000.00), which, as
20 Defendant stipulates, its undersigned counsel holds in escrow for no purpose other than payment
21 to Plaintiff. Such payment must be made within seven (7) days of entry of this Stipulated Order
22 by electronic fund transfer in accordance with instructions specified by a representative of
23 Plaintiff.

24 C. In the event of any default in payment, the entire unpaid amount, together with interest,
25 as computed pursuant to 28 U.S.C. § 1961 from the date of default to the date of payment, shall
26 immediately become due and payable.

1 D. Defendant relinquishes dominion and all legal and equitable right, title, and interest to all
2 funds paid pursuant to this Stipulated Order. Defendant shall make no claim to or demand for
3 return of the funds, directly or indirectly, through counsel or otherwise.

4 E. Defendant agrees that the facts alleged in the Complaint will be taken as true, without
5 further proof, only in any subsequent civil litigation by Plaintiff to enforce its rights to any
6 payment or monetary judgment pursuant to this Stipulated Order.

7 F. Defendant acknowledges that its Taxpayer Identification Numbers (Social Security
8 Numbers or Employer Identification Numbers), which Defendant has previously submitted to
9 Plaintiff, may be used for collecting and reporting on any delinquent amount arising out of this
10 Stipulated Order, in accordance with 31 U.S.C. § 7701.

11 **II. MODIFICATION OF DECISION AND ORDER**

12 IT IS FURTHER ORDERED that Defendant, and its successors and assigns, shall
13 consent to: (i) reopening of the proceeding in FTC Docket No. C-4316; (ii) waiver of its rights
14 under the show cause procedures set forth in Section 3.72(b) of the Commission's Rules of
15 Practice, 16 C.F.R. § 3.72(b); and (iii) modifying the Decision and Order in *In re Twitter, Inc.*,
16 C-4316, 151 FTC LEXIS 162 (F.T.C. Mar. 2, 2011), with the Decision and Order set forth in
17 Attachment A.

18 **III. ADDITIONAL PROVISIONS**

19 IT IS FURTHER ORDERED that Defendant shall provide to the Department of Justice
20 copies of all of the reports, assessments, notifications, certifications, and other documents
21 required or requested under the Decision and Order set forth in Attachment A as follows: Parts
22 VI.A, VI.E, VIII.A, IX, X.A, XI.A, and XI.B. Such documents shall be furnished via email to
23 Consumer.Compliance@usdoj.gov, with the subject line "United States v. Twitter, Inc., DJ 102-
24 4022." In the event that electronic mail is unavailable, the documents may be sent to the Director
25 of the Department of Justice's Consumer Protection Branch, and whomever he or she designates,
26 via overnight courier (not the U.S. Postal Service) to: Director, Consumer Protection Branch,
27 Department of Justice, 450 Fifth St. NW Ste. 6400-South, Washington, DC 20001, with the
28

1 subject line “United States v. Twitter, Inc., DJ 102-4022.” Defendant agrees that the Department
2 of Justice shall have the same rights as the Commission (as given in the Decision and Order set
3 forth in Attachment A) to request such documents under the specified parts, subject to any
4 applicable law or regulation. Within fourteen (14) days of receipt of a written request from a
5 representative of the Department of Justice’s Consumer Protection Branch related to the reports,
6 assessments, notifications, certifications, and other documents produced pursuant to the parts of
7 the Decision and Order identified in this paragraph, Defendant agrees to submit additional
8 compliance reports or other requested information, which must be sworn under penalty of
9 perjury. For purposes of this paragraph, “Defendant” shall have the same definition and scope as
10 the definition of “Respondent” in Paragraph E on page 3 of the Decision and Order set forth in
11 Attachment A.

12 **IV. CONTINUING JURISDICTION**

13 IT IS FURTHER ORDERED that this Court shall retain jurisdiction in this matter for
14 purposes of construction, modification, and enforcement of this Stipulated Order. The Clerk of
15 Court shall close the file.

16 SO ORDERED this 26th day of May, 2022.

17 
18 _____
19 THOMAS S. HIXSON
20 UNITED STATES MAGISTRATE JUDGE
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

SO STIPULATED AND AGREED:

Dated: May 25, 2022

FOR PLAINTIFF:

THE UNITED STATES OF AMERICA:

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

ARUN G. RAO
Deputy Assistant Attorney General

GUSTAV W. EYLER
Director
Consumer Protection Branch

LISA K. HSIAO
Assistant Director

/s/ Zachary L. Cowan
ZACHARY L. COWAN
DEBORAH S. SOHN
Trial Attorneys
U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street NW, Suite 6400-S
Washington, DC 20530
Telephone: (202) 451-7468
Zachary.L.Cowan@usdoj.gov
Deborah.S.Sohn@usdoj.gov

STEPHANIE M. HINDS
United States Attorney

MICHELLE LO
Chief, Civil Division

SHARANYA MOHAN
EMMET P. ONG
Assistant United States Attorneys
Northern District of California
450 Golden Gate Avenue
San Francisco, California 94102
Tel: (415) 436-7198
sharanya.mohan@usdoj.gov
emmet.ong@usdoj.gov

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Dated: May 24, 2022

FOR THE FEDERAL TRADE COMMISSION:

JAMES A. KOHM
Associate Director
Division of Enforcement

LAURA KOSS
Assistant Director
Division of Enforcement



REENAH L. KIM
Attorney
Division of Enforcement

ANDREA V. ARIAS
Attorney
Division of Privacy and Identity Protection

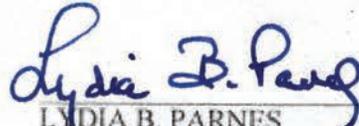
Federal Trade Commission
600 Pennsylvania Avenue, N.W.,
Mail Stop CC-9528
Washington, D.C. 20580
Tel: (202) 326-2272 (Kim); -2715 (Arias)
rkim1@ftc.gov; aarias@ftc.gov

FOR DEFENDANT TWITTER, INC.

1
2 Dated: 05/18/22


DAMIEN KIERAN
Chief Privacy Officer
Twitter, Inc.

3
4
5
6 Dated: 5/20/2022


LYDIA B. PARNES
Wilson Sonsoni Goodrich & Rosati
1700 K Street N.W., Fifth Floor
Washington, D.C. 20006
Tel: (202) 973-8800
lparnes@wsgr.com

Counsel for Twitter, Inc.

ATTACHMENT A

202-3062

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Lina M. Khan, Chair
Noah Joshua Phillips
Rebecca Kelly Slaughter
Christine S. Wilson**

In the Matter of

TWITTER, INC., a corporation.

DECISION AND ORDER

Docket No. C-4316

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed presenting the draft Complaint to the Commission. If issued, the draft Complaint would charge Respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 45(a)(1) and (l), 53(b), and 56(a)(1).

Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Respondent admits the facts necessary to establish jurisdiction.

The Commission considered the matter and determined that it had reason to believe Respondent has violated the Decision and Order the Commission previously issued in *In re Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011) and the FTC Act, and that a Complaint should issue stating its charges in that respect. After due consideration, the Commission issues the Complaint, makes the following Findings, and issues the following Order:

FINDINGS

1. Respondent Twitter, Inc. (“Twitter”) is a Delaware corporation with its principal office or place of business at 1355 Market Street, Suite 900, San Francisco, CA 94103.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

3. The Complaint charges violations of Section 5 of the FTC Act, 15 U.S.C. § 45, and violations of Provision I of an order previously issued by the Commission, 15 U.S.C. § 56(a)(1).
4. Respondent waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.
5. Respondent and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

ORDER

DEFINITIONS

For the purpose of this Order, the following definitions apply:

- A. **“Covered Incident”** means any instance affecting 250 or more Users in which: (1) any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization; or (2) individually identifiable Covered Information collected or received, directly or indirectly, by Respondent, was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization. “Covered Incident” does not include instances where the only unauthorized access, acquisition, or exposure was due to a User communicating through Respondent’s services (e.g., public tweets, protected tweets, retweets, or direct messages) information that was obtained from sources other than Respondent.
- B. **“Covered Information”** means information from or about an individual consumer including, but not limited to: (1) a first or last name; (2) geolocation information sufficient to identify a street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging User identifier or a screen name; (4) a mobile or other telephone number; (5) photos and videos; (6) Internet Protocol (“IP”) address, User ID, or other persistent identifier that can be used to recognize a User over time and across different devices, websites, or online services; (7) a Social Security number; (8) a driver’s license or other government issued identification number; (9) financial account number; (10) credit or debit information; (11) date of birth; (12) biometric information; or (13) any information combined with any of (1) through (12) above. “Covered Information” does not include information that a User intends to make public using Respondent’s services.
- C. **“Representatives”** means Respondent’s officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.
- D. **“Resources”** means networks, systems, and software.

E. “**Respondent**” means Twitter, Inc. (“Twitter”), and its successors and assigns. For purposes of Parts V and VI, Respondent means Twitter, Inc., its successors and assigns, and any business that Respondent controls directly or indirectly, except for any business that: (1) does not provide services that are offered to U.S. residents; or (2) does not collect, maintain, use, disclose, access, or provide access to the Covered Information of U.S. residents to enable Respondent’s microblogging, social networking, or communications services.

F. “**Timeline Notice**” means a message Respondent places in a User’s Twitter timeline (*i.e.*, the main screen the User sees when opening Twitter which displays a stream of tweets from accounts the User has chosen to follow) that stays near the top (*i.e.*, within the first five (5) tweets) of a User’s Twitter timeline: (1) for at least six (6) months from the effective date of the Order; (2) until the User clicks on the “Learn More about your options” button embedded in the message; or (3) until the User scrolls past the message in their timeline, whichever occurs earlier.

G. “**User**” means an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent’s products and services.

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Respondent and its Representatives, directly or through any corporation, subsidiary, division, website, mobile app, or other device, in connection with the offering of any product or service in or affecting commerce, must not misrepresent, in any manner, expressly or by implication, the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, misrepresentations related to:

A. Respondent’s privacy and security measures to prevent unauthorized access to Covered Information;

B. Respondent’s privacy and security measures to honor the privacy choices exercised by Users;

C. Respondent’s collection, maintenance, use, disclosure, or deletion of Covered Information;

D. The extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls;

E. The extent to which Respondent makes or has made Covered Information accessible to any third parties;

F. The extent to which Respondent targets advertisements to Users or enables third parties to target advertisements to Users; or

G. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to

the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

II. LIMITATIONS ON USE OF TELEPHONE NUMBERS OR EMAIL ADDRESSES SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives must not use, provide access to, or disclose, for the purpose of serving advertisements, any telephone number or email address obtained from a User before the effective date of this Order for the purpose of enabling an account security feature (*e.g.*, two-factor authentication, password recovery, re-authentication after detection of suspicious or malicious activity). Nothing in Provision II will limit Respondent's ability to use, provide access to, or disclose such telephone numbers or email addresses if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

III. REQUIRED NOTICE TO CONSUMERS

IT IS FURTHER ORDERED that, within fourteen (14) days after the effective date of this Order, Respondent must provide a Timeline Notice to all current U.S. Users who joined Twitter prior to September 17, 2019, that states: “**Twitter’s Use of Your Personal Information for Tailored Advertising** As we stated on Oct. 8, 2019, we may have served you targeted ads based on an email address or phone number you provided to us to secure your account.”, and includes a “Learn more about your options” button that links to a webpage showing the information in Exhibit A.

IV. REQUIRED MULTI-FACTOR AUTHENTICATION OPTIONS

IT IS FURTHER ORDERED that, as of the effective date of this Order, Respondent must allow Users to utilize multi-factor authentication without providing a telephone number to access their Twitter accounts, such as by integrating authentication applications or allowing the use of security keys. The Company may use equivalent, widely-adopted industry authentication options that do not require Users to provide a telephone number and that are not multi-factor, if the person or persons responsible for the Program under Provision V.C: (1) approve(s) in writing the use of such equivalent authentication options; and (2) document(s) a written explanation of how the authentication options are widely-adopted and at least equivalent to the security provided by multi-factor authentication.

V. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, must, within one hundred eighty (180) days of issuance of this Order, establish and implement, and thereafter maintain a comprehensive privacy and information security program (the “Program”) that protects the privacy, security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must at a minimum:

A. Document in writing the content, implementation, and maintenance of the Program;

B. Provide the written program, and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for the Program at least once every calendar quarter;

C. Designate a qualified employee or employees to coordinate and be responsible for the Program;

D. Assess and document, at least once every twelve (12) months and promptly following the resolution of a Covered Incident (not to exceed ninety 90 days after the discovery of the Covered Incident), internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information that could result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondent identifies to the privacy, security, confidentiality, or integrity of Covered Information identified in response to Provision V.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, or destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information. Such safeguards must also include:

1. Prior to implementing any new or modified product, service, or practice that collects, maintains, uses, discloses, or provides access to Covered Information, conducting an assessment of the risks to the privacy, security, confidentiality, or integrity of the Covered Information;
2. For each new or modified product, service, or practice that does not pose a material risk to the privacy, security, confidentiality, or integrity of Covered Information, documenting a description of each reviewed product, service, or practice and why such product, service, or practice does not pose such a material risk;
3. For each new or modified product, service, or practice that poses a material risk to the privacy, security, confidentiality, or integrity of Covered Information, conducting a privacy review and producing a written report ("Privacy Review") for each such new or modified product, service, or practice. The Privacy Review must:
 - (a) Describe how the product, service, or practice will collect, maintain, use, disclose, or provide access to Covered Information, and for how long;
 - (b) Identify and describe the types of Covered Information the product, service, or practice will collect, maintain, use, disclose, or provide access to;
 - (c) If the Covered Information will be collected from a User, describe the context of the interaction in which Respondent will collect such Covered Information (*e.g.*, under security settings, in pop-up messages in the timeline, or in response to a prompt reading, "Get Better Ads!");

- (d) Describe any notice that Respondent will provide Users about the collection, maintenance, use, disclosure, or provision of access to the Covered Information;
- (e) State whether and how Respondent will obtain consent from Users for the collection, maintenance, use, disclosure, or provision of access to Covered Information;
- (f) Identify any privacy controls that will be provided to Users relevant to the collection, maintenance, use, disclosure, or provision of access to the Covered Information;
- (g) Identify any third parties to whom Respondent will disclose or provide access to the Covered Information;
- (h) Assess and describe the material risks to the privacy, security, confidentiality, and integrity of Covered Information presented by the product, service, or practice;
- (i) Assess and describe the safeguards to control for the identified risks, and whether any additional safeguards need to be implemented to control for such risks;
- (j) Explain the reasons why Respondent deems the notice and consent mechanisms described in Provisions V.E.3(d) and V.E.3(e) sufficient;
- (k) Identify and describe any limitations on the collection, maintenance, use, disclosure, or provision of access to Covered Information based on: (i) the context of the collection of such Covered Information; (ii) notice to Users; and (iii) any consent given by Users at the time of collection or through subsequent authorization;
- (l) Identify and describe any changes in how privacy and security-related options will be presented to Users, and describe the means and results of any testing Respondent performed in considering such changes, including but not limited to A/B testing, engagement optimization, or other testing to evaluate a User's movement through a privacy or security-related pathway;
- (m) Include any other safeguards or other procedures that would mitigate the identified risks to the privacy, security, confidentiality, and integrity of Covered Information that were not implemented, and each reason that such alternatives were not implemented; and
- (n) Include any decision or recommendation made as a result of the review (*e.g.*, whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);

4. Safeguards to prevent the collection, maintenance, use, disclosure, or access to Covered Information beyond the limitations identified in Provision V.E.3(k), including:
 - (a) Regular training, at least once a year, for any employees and independent contractors whose responsibilities include the collection, maintenance, disclosure, use, or provision of access to Covered Information, on the permissible collection, maintenance, disclosure, use, or provision of access to Covered Information and any related limitations;
 - (b) Written attestations by those employees and independent contractors that they will not collect, maintain, disclose, use, or provide access to the Covered Information in a manner inconsistent with those limitations;
 - (c) Designation of a senior officer, or senior level team composed of no more than five (5) persons, to be responsible for any decision to collect, maintain, use, disclose, or provide access to the Covered Information; and
 - (d) Treating any new method of collecting, maintaining, using, disclosing, providing access to, or deleting the Covered Information as a new or modified product, service, or practice requiring the reviews set forth in Provisions V.E.1-3;
 5. Regular privacy and information security training programs for all employees and independent contractors on at least an annual basis, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;
 6. Technical measures to monitor Respondent's Resources to identify unauthorized attempts to: (a) access, modify, or exfiltrate Covered Information from Respondent's Resources; or (b) access or take over Users' accounts; and
 7. Data access policies and controls for all: (a) databases storing Covered Information; (b) Resources that provide access to Users' accounts; and (c) Resources containing information that enables or facilitates access to Respondent's internal network and systems;
- F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information, and modify the Program based on the results;
- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, and modify the Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of Respondent's network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources; and (2) penetration testing of Respondent's network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision V.D of this Order, or any other circumstances that Respondent knows or has reason to believe may have an impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Program at least once every twelve (12) months and modify the Program based on the results.

VI. INDEPENDENT PROGRAM ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision V of this Order titled Mandated Privacy and Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)") who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the Program; (3) retain all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents relating to Respondent's compliance with this Order may be withheld from the Commission by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim. Respondent may obtain separate assessments for (1) privacy and (2) information security from multiple Assessors, so long as each of the Assessors meets the qualifications set forth above;

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion;

C. The reporting period for the Assessments must cover: (1) the first three-hundred-and-sixty-five (365) days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must, for the entire assessment period: (1) determine whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assess the effectiveness of Respondent's implementation and maintenance of Provisions V.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were

identified in any prior Assessment required by this Order; and (5) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Program and did not rely primarily on assertions or attestations by Respondent's management. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision V.E of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard; and

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062." All subsequent biennial Assessments must be retained by Respondent until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VII. COOPERATION WITH THIRD-PARTY ASSESSOR(S)

IT IS FURTHER ORDERED that Respondent and its Representatives, whether acting directly or indirectly, in connection with any Assessment required by Provision VI of this Order titled Independent Program Assessments by a Third Party, must:

- A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;
- B. Provide or otherwise make available to the Assessor information about Respondent's Resources(s) and all of Respondent's IT assets so that the Assessor can determine the scope of the Assessment, and have visibility to Resource(s) and IT assets deemed in scope; and
- C. Disclose all material facts to the Assessor(s), and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of Provisions V.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program.

VIII. CERTIFICATIONS

IT IS FURTHER ORDERED that Respondent must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for the Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification; and
- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062."

IX. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after Respondent's discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;
- C. A description of each type of Covered Information that was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;
- D. The number of Users whose Covered Information was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of any materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW,

Washington, DC 20580. The subject line must begin, “*In re Twitter, Inc.*, FTC File No. 202-3062.”

X. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For five (5) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities relating to the subject matter of this Order, and all agents and representatives who participate in any acts or practices subject to this Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order, which can be obtained electronically.

XI. COMPLIANCE REPORTING AND NOTICES

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

- A. Two-hundred and forty (240) days after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent: (1) identifies the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identifies all of Respondent’s businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes the activities of each business, including the goods and services offered and the means of advertising, marketing, and sales; (4) describes in detail whether and how Respondent is in compliance with each Provision of this Order; and (5) provides a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; (3) the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent.

C. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.

D. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “In re Twitter, Inc., FTC File No. 202-3062.”

XII. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each person that Respondent contracts with directly and that provides services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all U.S. consumer complaints concerning the subject matter of the Order, and any responses to such complaints;
- D. A copy of each unique advertisement or other marketing material making a representation subject to this Order;
- E. A copy of each widely-disseminated representation by Respondent or its Representatives that describe the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, (1) statements relating to any change in any product, service, or practice that relates to the privacy, security, confidentiality, or integrity of such information, and (2) statements relating to: (a) Respondent’s privacy and security measures to prevent unauthorized access to Covered Information; (b) Respondent’s privacy and security measures to honor the privacy choices exercised by Users; (c) Respondent’s collection, maintenance, use, disclosure, or deletion of Covered Information; (d) the extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls; (e) the extent to which Respondent makes or has made Covered Information accessible to any third parties; (f) the extent to which Respondent allows third parties to serve advertisements to Users; or (g) the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules;

F. All materials relied upon in making the statements in Provisions XII.D and XII.E, and copies of each materially different notice provided to Users and mechanisms for obtaining a User's consent for the collection, use, or disclosure of Covered Information (including screenshots/screencasts and User interfaces, consent flows, and paths a User must take to reach such settings);

G. All materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

H. For 5 years from the date received, copies of all subpoenas, information provided in response to such subpoenas, and all material correspondence with law enforcement, if such communication relate to Respondent's compliance with this Order;

I. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order; and

J. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XIII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce records for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIV. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than twenty (20) years;
- B. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED:

EXHIBIT A

[To appear with the Twitter logo and Twitter's standard website header]

We may have asked for your phone number or email address to secure or authenticate your account (for example, for two-factor authentication). As we [told you](#) in October 2019, we may have used these phone numbers or email addresses to deliver tailored advertising to you on Twitter until September 2019. On [date], we entered into a settlement with the Federal Trade Commission to resolve this issue.

As of September 17, 2019, we are no longer using phone numbers or email addresses collected for safety or security purposes for advertising. We never disclosed or shared your phone number or email address with advertisers. There is no action that you need to take regarding this issue.

You have a number of options to control your privacy and security when you use Twitter:

- **Control your privacy settings.** You can find out more about your privacy settings on Twitter, including how to enable or disable personalized ads, by visiting <https://myprivacy.twitter.com>.
- **Review your multi-factor authentication settings.** By requiring both a password and a secondary code or security key to access your account, multi-factor authentication can help keep your account safe. You can use an authentication app, a security key, or a phone number for multi-factor authentication. (And if you provide us a phone number for multi-factor authentication, it will not be used for advertising purposes without your consent.) You can learn about multi-factor authentication settings by visiting <https://help.twitter.com/en/managing-your-account/two-factor-authentication>.

For more details about how we protect the information you share with us and how we use that data, we encourage you to visit the [Twitter Privacy Center](#).

We are very sorry this happened. If you have questions or comments about this notice or what we do to protect your information moving forward, you may contact Twitter's Office of Data Protection through this [form](#).

[To appear with the Twitter's standard website footer]

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of

TWITTER, Inc.,
a corporation.

Docket No. C-4316

DECISION

The Federal Trade Commission (“Commission”) issued a Decision and Order against Twitter, Inc. (“Twitter”) in Docket C-4316 on March 2, 2011 (“2011 order”).¹ On [INSERT DATE], the United States of America, acting upon notification and authorization to the Attorney General by the Commission, filed a complaint (“2022 complaint”) in federal district court alleging that Twitter violated the 2011 order by misrepresenting the extent to which it maintained and protected the privacy of nonpublic consumer information. The complaint also alleged that Twitter violated Section 5 of the FTC Act by misrepresenting how it would use telephone numbers and email addresses that users provided to enable a security feature.

On [INSERT DATE], Judge [INSERT JUDGE’S NAME] in the District for the Northern District of California entered a Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief (“Stipulated Order”) resolving the 2022 complaint. In Section II of the Stipulated Order, Twitter consented to: (1) reopening the 2011 proceeding in FTC Docket No. C-4316; (2) waiving its rights under the show cause procedures set forth in Section 3.72(b) of the Commission’s Rules of Practice, 16 C.F.R. § 3.72(b); and (3) modifying the 2011 Order with the new Decision and Order set forth below.

In view of the foregoing, the Commission has determined that it is in the public interest to reopen the proceeding in Docket No. C-4316 pursuant to Commission Rule 3.72(b), 16 C.F.R. § 3.72(b), and to issue a new order as set forth below. Accordingly,

IT IS ORDERED that this matter be, and it hereby is, reopened; and

IT IS FURTHER ORDERED that, Twitter having consented to modifying the 2011 order as set forth below, the Commission hereby modifies the 2011 order with the attached Decision and Order.

¹ *In the Matter of Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011).

Appendix 6

To whom it may concern:

Elon Musk's takeover of Twitter will further toxify our information ecosystem and be a direct threat to public safety, especially among those already most vulnerable and marginalized.

Twitter has outsized influence in shaping both public discourse and industry-wide platform governance standards. While the company is hardly a poster-child for healthy social media, it has taken welcome steps in recent years to mitigate systemic risks, ratcheting up pressure on the likes of Facebook and YouTube to follow suit. Musk intends to steamroll those safeguards and provide a megaphone to extremists who traffic in disinformation, hate, and harassment. Under the guise of 'free speech,' his vision will silence and endanger marginalized communities, and tear at the fraying fabric of democracy.

The undersigned organizations believe that Twitter should continue to uphold the practices that serve as guideposts for other Big Tech platforms. **We call on you - Twitter's top advertisers - to commit to these standards as non-negotiable requirements for advertising on the platform:**

- 1. Keep accounts including those of public figures and politicians that were removed for egregious violations of Twitter Rules - such as harassment, violence, and hateful conduct - off the platform** and continue to enforce the [civic integrity policy](#) along with the [hateful conduct policy](#). Since 2020, Twitter has applied its civic integrity policy to all users, including elected officials. Musk's statements at [Ted2022](#) last week indicate that he will roll-back permanent bans and err on the side of allowing harmful content to remain on the platform under the guise of 'free speech.' A reversal of Twitter's content moderation policies including its recently released [climate commitments](#), its protections for transgender people, and its restrictions on other forms of hate, harassment, and violence would be toxic not just for those targeted, but also for businesses advertising on the platform.
- 2. Beyond algorithmic transparency, ensure algorithmic accountability, preserve people's privacy, and commit to depolarizing the algorithm.** Consider the implications of full-scale public visibility into Twitter's algorithm and put protections in place to prevent bad actors from gaming the system. Listen to [privacy experts](#) and others whose expertise includes protecting communities that are discriminated against in speaking truth to power. Continue the work of its in-house research team called [Machine Learning Ethics, Transparency and Accountability](#) that looks at potential biases in

its algorithms including published research, for instance, on whether the algorithms that automatically crop profile photos contained inadvertent bias.

3. Continue Twitter's commitment to transparency and researcher access.

Twitter stands out for its support of researchers – both internal and external to the company. From its [API for academic research](#) to its [willingness to publish critique](#) and its internal learnings, Twitter has demonstrated a commitment to transparency and access for researchers that sets an example for other Big Tech companies and allows for accountability.

As top advertisers on Twitter, your brand risks association with a platform amplifying hate, extremism, health misinformation, and conspiracy theorists.

Under Musk's management, Twitter risks becoming a cesspool of misinformation, with your brand attached, polluting our information ecosystem in a time where trust in institutions and news media is already at an all-time low. Your ad dollars can either fund Musk's vanity project or hold him to account. We call on you to demand Musk uphold these basic standards of community trust and safety, and to pull your advertising spending from Twitter if they are not.

Sincerely,

Access Now
Accountable Tech
Black Lives Matter Global Network Foundation
Center for Countering Digital Hate
Empowering Pacific Islander Communities (EPIC)
Face the Music Collective
Fair Vote UK
Free Press
Friends of the Earth
Gender Equity Policy Institute
GLAAD
Global Project Against Hate and Extremism
Indivisible Northern Nevada
Kairos
Media Matters for America
MediaJustice
NARAL Pro-Choice America
National Hispanic Media Coalition
Religious Coalition for Reproductive Choice
Reproaction
Stop Online Violence Against Women Inc
The Sparrow Project
UltraViolet
Union of Concerned Scientists
V-Day/One Billion Rising
Women's March

Appendix 7



Office of the Chair

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

May 6, 2022

The Honorable Jim Jordan
Ranking Member
Committee on the Judiciary
U.S. Houses of Representatives
Washington, D.C. 20515

Dear Ranking Member Jordan:

Thank you for your May 4, 2022, letter regarding the Open Markets Institute's April 26, 2022, issuance of a statement on the proposed acquisition of Twitter by Elon Musk. I am happy to respond to the two questions posed in your letter.

1. Did you or anyone else at the FTC solicit or play any role in drafting OMI's statement?

I did not and, as far as I am aware, nor did anyone under my supervision. It would be inappropriate for FTC staff to be in contact with the Open Markets Institute regarding the drafting or solicitation of their statement.

2. Has the FTC taken any actions in response to the statement released by OMI?

The FTC has not taken any actions in response to the statement released by the Open Markets Institute. As noted in 16 C.F.R. §§ 2.2 and 2.3, anyone is welcome to file a complaint or a request for Commission action, though the Commission acts only in the public interest. The FTC's law enforcement work is driven by the Commission, conducted by the agency's staff, and confined by our statutory authorities.

Thank you again for your letter. If you have any questions, please feel free to have your staff call [REDACTED], the Director of our Office of Congressional Relations, at [REDACTED].

Sincerely,

A handwritten signature in cursive script that reads "Lina Khan".

Lina M. Khan
Chair, Federal Trade Commission

Appendix 8

**Concurring Statement of Commissioner Christine S. Wilson
and Commissioner Noah Joshua Phillips**

Twitter

Matter No. 2023062

May 25, 2022

Today's settlement with Twitter, Inc., years in the making,¹ illustrates once again that the Federal Trade Commission takes seriously both the protection of consumers' privacy and the enforcement of Commission orders. The settlement provides meaningful relief, including a \$150 million civil penalty and extensive injunctive provisions. We thank our knowledgeable and experienced career staff who investigated this case and negotiated this order – they and their colleagues work tirelessly to make the FTC the most effective privacy enforcer in the world.

In March 2011, the Commission finalized an order with Twitter (“2011 Order”), settling allegations that it deceived consumers and put their privacy at risk by failing to (1) use reasonable and appropriate security measures to protect nonpublic user data from unauthorized access, and (2) honor consumers' privacy choices.² That 2011 Order prohibited Twitter from misrepresenting the extent to which it maintains and protects the security and privacy of nonpublic data and honors users' privacy choices. As alleged in the complaint filed today, Twitter failed to live up to its obligations. Specifically, Twitter allegedly collected telephone numbers and email addresses from consumers for security purposes, but then used that information for targeted advertisements.

When consumers hand over personal information for specific security purposes, such as multi-factor authentication, account recovery, or re-authorization, they reasonably expect the information to be deployed for those purposes. When companies use those data for non-security purposes, like advertising, they undermine trust in critical security measures to the detriment of consumers and businesses alike.

The complaint alleges that this conduct violated both the 2011 Order and Section 5 of the FTC Act. The complaint also alleges that Twitter misrepresented its compliance with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, which prohibit participants from processing personal information in a way that is incompatible with the purposes for which it was originally collected.³

¹ See Twitter, Inc., Quarterly Report (Form 10-Q) (Aug. 3, 2020), <https://sec.report/Document/0001418091-20-000158/>.

² *In the matter of Twitter, Inc.*, FTC File No. 0923093 (March 2011), <https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3093-twitter-inc-corporation>.

³ This settlement demonstrates the Commission's continued commitment to take action against companies that misrepresent their compliance with Privacy Shield, any successor program, or similar agreements that protect privacy and facilitate international data transfers.

The new Twitter order employs the model that the FTC has built during two decades of vigorous privacy and data security enforcement. Observant readers will spot many injunctive remedies the Commission has employed repeatedly in its privacy and data security orders. For example, the order requires Twitter to create and implement a privacy and security program that includes privacy risk assessments, detailed privacy reviews for new or modified products, documentation, data access controls, technical measures to monitor unauthorized access, training, and certifications.

But the FTC’s enforcement model is not static; the Commission has refined and updated it to address evolving business practices and technologies. Some of the provisions in today’s order reflect recent refinements. For example, Twitter is required to use either multifactor authentication or a widely adopted mechanism that provides equivalent security.⁴ The Commission first included a requirement to use multifactor authentication in our March enforcement action against CaféPress.⁵ Today’s order also requires Twitter to design and implement both a privacy and an information security program, a dual obligation we first imposed in our 2019 enforcement action against Facebook.⁶

And, in each case, the Commission tailors its enforcement to the specific unlawful conduct and harms alleged in each case. This Twitter order includes a data use restriction tied to the core

⁴ *In the Matter of Twitter, Inc.*, C-4316, Decision and Order (May 2022) (Section IV).

⁵ See *In the Matter of CafePress*, No. 192-3209 (Mar. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Residual%20Pumpkin%20Agreement%20Containing%20Consent%20Order.pdf (Section II.E.7). This obligation builds on provisions in prior Commission orders that require encryption or other security features. See, e.g., *In the Matter of Zoom Video Communications, Inc.*, C-4731 (Feb. 2021), https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf (requiring “[p]rotections, such as encryption, tokenization, or other same or greater protections, for Covered Information collected, maintained, processed, or stored by Respondent, including in transit and at rest” (Section II.E.11)); *In the Matter of LightYear Dealer Technologies, LLC*, No. C-4687 (Sept. 2019), https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf (requiring encryption of all Social Security numbers and financial account information on Respondent’s computer networks (Section I.E.4)).

⁶ Part V of the Facebook order requires that it: “implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security of Covered Information. In addition to any security-related measures associated with Respondent’s Privacy Program under Part VII of this Order, the information security program must contain safeguards appropriate to Respondent’s size and complexity, the nature and scope of Respondent’s activities, and the sensitivity of the Covered Information.” Part VII of the order requires that it: “establish and implement, and thereafter maintain a comprehensive privacy program (‘Privacy Program’) that protects the privacy, confidentiality, and Integrity of the Covered Information collected, used, or shared by Respondent.” *U.S. v. Facebook*, No. 1:19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf; *In the Matter of Facebook, Inc.*, C-4365 (Apr. 2020), <https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf>, see also 2019 Order Fact Sheet (Jul. 24, 2019), https://www.ftc.gov/system/files/attachments/press-releases/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook/2019_order_fact_sheet_facebook.pdf (noting that the order requires Facebook to create a comprehensive data security program and a mandated privacy program); Statement of Chairman Joseph J. Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson Regarding the Matter of Facebook (Jul. 24, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chairman-joe-simons-commissioners-noah-joshua-phillips-christine-s-wilson-regarding-matter> (discussing the inclusion of a requirement for both a privacy and security program).

allegation of illegality in the complaint: the company may not use for advertising any phone numbers or email addresses that had been gathered for security purposes. The 2019 Facebook order contained a similar use restriction, flowing from a similar allegation of illegality.

Precisely because this order builds on established precedent and the Commission’s expertise in privacy enforcement, it provides meaningful and effective relief. The value of these types of injunctive provisions and accountability mechanisms has long been clear to us.⁷ But strikingly similar settlements in the past have been subjected to (sometimes vitriolic) criticism⁸ for alleged failings that today’s order would share. No executives are named, or obligated personally.⁹ There is no admission of liability, or disgorgement of algorithms. There is no change to Twitter’s business model.

⁷ See Statement of Chairman Joseph J. Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson, *In re Sunday Riley Modern Skincare, LLC*, (Nov. 6, 2020), https://www.ftc.gov/system/files?file=documents/cases/2020.11.6_sunday_riley_majority_statement_final.pdf (discussing the effectiveness of injunctive and other non-monetary relief); see also Statement of Chairman Joseph J. Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson Regarding the Matter of Facebook (Jul. 24, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chairman-joe-simons-commissioners-noah-joshua-phillips-christine-s-wilson-regarding-matter> (describing the breadth and scope of the non-monetary relief in the order). Commissioner Wilson also has spoken at length about the effectiveness of non-monetary relief. See, e.g., Christine S. Wilson, One Step Forward, Two Steps Back: Sound Policy on Consumer Protection, Remarks at NAD (Oct. 5, 2020), https://www.ftc.gov/system/files/documents/public_statements/1581434/wilson_remarks_at_nad_100520.pdf; Christine S. Wilson, Remarks at Global Antitrust Institute, *FTC v. Facebook* (Dec. 11, 2019), https://www.ftc.gov/system/files/documents/public_statements/1557534/commissioner_wilson_remarks_at_global_antitrust_institute_12112019.pdf.

⁸ See, e.g., Dissenting Statement of Commissioner Rohit Chopra Regarding Zoom Video Communications, Inc. (Feb. 1, 2021), https://www.ftc.gov/system/files/documents/public_statements/1586865/20210129_final_chopra_zoom_statement_0.pdf (asserting that the final order is “weak,” provides “no money” and that the injunctive relief constitutes “paperwork requirements” with no real accountability). In addition, then-Commissioner Chopra stated that the order “doesn’t fix the incentives causing these repeat privacy abuses. It doesn’t stop \$FB from engaging in surveillance or integrating platforms. There are no restrictions on data harvesting tactics — just paperwork.” Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; see also Center for Digital Democracy Press Release: Groups Join Legal Battle to Fight Ineffective FTC Privacy Decision on Facebook (Jul. 26, 2019), <https://www.democraticmedia.org/article/groups-join-legal-battle-fight-ineffective-ftc-privacy-decision-facebook> (citing several organizations that criticized and challenged the settlement). Notably, the groups stated that the settlement was “woefully insufficient,” “provides no meaningful changes to Facebook’s structure or financial incentives” and that the “fine is a mere cost of doing business,” “a parking ticket,” a “get-out-of jail free card.” *Id.*; see also Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf. See also, Dissenting Statement of Commissioner Rohit Chopra, *In the matter of Google LLC and YouTube, LLC* (Sep. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf.

⁹ See *FTC v. Google LLC and YouTube, LLC*, No. 1:19-cv-2642 (D.D.C. Sep. 4, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3083-google-llc-youtube-llc>; *In the matter of Facebook, Inc.*, No. 1:19-cv-02184, (D.D.C. Jul. 24, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter>; *U.S. v. Musical.ly* (now known as TikTok), No. 2:19-cv-1439 (C.D. Cal. Feb. 2, 2019), <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3004-musically-inc> (naming corporate entities only).

The order in the 2019 Facebook case met with condemnation from some quarters, so it is worth comparing today’s settlement to the alleged shortcomings of the Facebook order:¹⁰

Criticism of Order	Facebook Order	Twitter Order
“Mere paperwork” requirements ¹¹	Privacy risk assessments for new or modified products	Privacy risk assessments for new or modified products
“Mere paperwork” requirements ¹²	Privacy reviews and reports	Privacy reviews and reports
“Mere paperwork” requirements ¹³	Covered incident reports	Covered incident reports
Certifications only ensure that paperwork has been completed ¹⁴	Certifications by CEO and Chief Privacy Officer	Certifications by senior corporate management or senior officer (not CEO)
No accountability for executives ¹⁵	No executives named, no IH of CEO or other executives cited in statements supporting settlement	No executives named, no IH of CEO or other executives cited in statements supporting settlement

¹⁰ The Facebook order included stronger and more sweeping provisions, and a penalty measured in the billions. The differences in approach are appropriate, as there were more Section 5 and order violations alleged in Facebook.

¹¹ Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹² Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹³ Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹⁴ Rohit Chopra, Twitter (Jul. 24, 2019), <https://twitter.com/chopracfpb/status/1154010756079390720?s=19>; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹⁵ Dissenting Statement of Commissioner Rebecca Kelly Slaughter, *In the matter of FTC v. Facebook* (Jul.24, 2019), https://www.system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

Penalty is a mere cost of doing business ¹⁶	\$5 billion 2018 Annual Revenues: \$55.8 billion Penalty: 9% of annual revenue	\$150 million 2021 Annual revenues: \$5.077 billion ¹⁷ Penalty: 3% of annual revenue
Company receives majority of revenue from advertising and order does nothing to change the business structure or incentives ¹⁸	Can still use data for advertising purposes; prohibited from misrepresenting the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information	Can still use data for advertising purposes; prohibited from misrepresenting the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information
Company governance unchanged ¹⁹	Board of Directors restructured to include Privacy Committee with oversight authority	No governance changes
No meaningful restrictions on ability to collect, share, and use personal information ²⁰	Use restriction for phone numbers; requirement to identify material risks to privacy of covered information and prepare privacy review statements documenting efforts to control for the risk	Use restriction for phone numbers; requirement to identify material risks to privacy of covered information and prepare privacy review statements documenting efforts to control for the risk

We support this order, which is a strong one. The Facebook order included more stringent obligations and greater relief because more egregious conduct was alleged. We reject the view that the provisions in orders like these constitute “mere paperwork” that provide no meaningful restrictions or accountability. And we reject the characterization of substantial penalties as “a slap on the wrist.” Penalties matter, then and now. And so do the privacy programs and

¹⁶ Nancy Scola and Steven Overly, “FTC strikes \$5B Facebook settlement against fierce Democratic objections,” POLITICO (July 24, 2019), <https://www.politico.com/story/2019/07/24/ftc-facebook-settlement-1428432> (quoting Representation Cicilline as stating that the \$5B fine is “disappointing” and Senator Blumenthal as stating that the penalty is “[a] tap on the wrist, not even a slap”); *see also* Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹⁷ *See Twitter Revenue 2011-2022* TWTR, Macrotrends, <https://www.macrotrends.net/stocks/charts/TWTR/twitter/revenue>.

¹⁸ Dissenting Statement of Commissioner Rebecca Kelly Slaughter *In the matter of FTC v. Facebook* (Jul. 24, 2019), https://www.system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

¹⁹ Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

²⁰ Dissenting Statement of Commissioner Rebecca Kelly Slaughter, *In the matter of FTC v. Facebook* (Jul. 24, 2019), https://www.system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf; Dissenting Statement of Commissioner Rohit Chopra, *In re Facebook, Inc.* (Jul. 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

assessments that orders like today's command. Both orders also create processes that require the companies to consider the risks to the privacy and security of the information they collect, evaluate the safeguards they have in place, and adjust procedures to address those risks. Both orders require assessments by third-party experts, approved by the FTC, to evaluate the companies' privacy programs and issue reports evaluating compliance with the mandated program. Both orders require executives in the company to certify to compliance. These processes force companies under order to consider privacy, account for privacy, and be accountable for failing to protect it.

The Commission recognizes that its orders are not perfect. For this reason, we approach each new order with care, fine-tuning provisions and considering alternative ways to address violations.²¹ We hope that the bipartisan approval of this order, one very much in line with prior orders, signals the beginning of a more constructive dialogue about how to continue refining our enforcement program. If this case can close the door on unfounded and gratuitous attacks on the FTC's privacy enforcement program, that closure would serve consumers, provide clarity to stakeholders, and advance the mission of the agency.

The resolution of this matter also demonstrates the general deterrent effect of Commission orders. In our July 2019 complaint and order against Facebook,²² the Commission for the first time found it unlawful for companies to collect consumer information for security purposes and then use it to target advertising. Shortly after the Facebook order was announced, in October 2019, Twitter disclosed its similar misuse of consumers' email addresses and phone numbers.²³ This timeline suggests that Twitter was paying attention to the FTC's actions and underscores the value of sending signals to the marketplace through orders like these.

A side note. In August 2020, Twitter publicly disclosed that the FTC was investigating it for potential order violations, taking an accounting reserve to pay a \$150 million fine.²⁴ Nearly two full years have passed, and Twitter now is paying the anticipated fine. An observer might ask what took so long, and why now. Despite (and because of) the coincidence in timing with

²¹ See, e.g., Statement of the Federal Trade Commission *Regarding Unixiz, Inc. d/b/a i-Dressup.com and Zhijun Liu and Xichen Zhang individually & James V. Grago, Jr. d/b/a ClixSense.com* (Apr. 2019), https://www.ftc.gov/system/files/documents/cases/2019-03-19_idressupclixsense_statement_final.pdf (announcing new requirements that go beyond requirements from previous data security orders); see also *In the Matter of LightYear Dealer Technologies, LLC*, No. C-4687 (Sept. 2019), [https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf_\(including_additional_data_security_requirements_such_as_encryption_of_all_Social_Security_numbers_and_financial_account_information_on_Respondent's_computer_networks\)](https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf_(including_additional_data_security_requirements_such_as_encryption_of_all_Social_Security_numbers_and_financial_account_information_on_Respondent's_computer_networks)).

²² FTC Press Release, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, July 24, 2019, <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>.

²³ Twitter Support (@TwitterSupport), TWITTER (Oct. 8, 2019, 4:02 PM), https://twitter.com/twittersupport/status/1181661080033955840?ref_src=.

²⁴ See Kate Conger, *F.T.C. Investigating Twitter for Potential Privacy Violations*, N.Y. TIMES (Aug. 3, 2020), <https://www.nytimes.com/2020/08/03/technology/ftc-twitter-privacy-violations.html>.

unrelated headlines concerning Twitter,²⁵ it is important to be clear that this settlement has nothing to do with Twitter's potential sale or new ownership, the company's content moderation policies, or anything other than the facts alleged in the Complaint.

This settlement is about ensuring that Twitter safeguards consumer privacy and vindicates the Commission's authority through zealous enforcement of its orders. It is an excellent settlement. We commend staff on their stellar work.

²⁵ See, e.g., Cara Lombardo, Meghan Bobrowsky & Georgia Wells, *Twitter Accepts Elon Musk's Offer to Buy Company in \$44 Billion Deal*, WALL ST. J. (Apr. 25, 2022, 5:48PM), <https://www.wsj.com/articles/twitter-and-elon-musk-strike-deal-for-takeover-11650912837>.

Appendix 9

**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, 2021), <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 Twitter⁸

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.

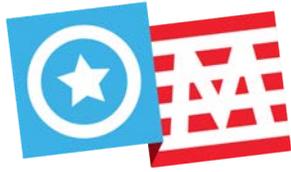
Third, Twitter must pay \$150 million in civil penalties for its alleged recidivism. Civil penalties are key for deterring law violations, and we believe the FTC must approach civil penalties with an eye to complete deterrence. We are confident that in this matter the civil penalty amount obtained ensures 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).

Appendix 10



OPEN MARKETS

LIBERTY ★ DEMOCRACY ★ PROSPERITY

FOR IMMEDIATE RELEASE: Tuesday, Apr. 26, 2022

CONTACT: Roberto Hylton, roberto@npagency.com

OMI STATEMENT ON ELON MUSK AND TWITTER

WASHINGTON - *In response to Elon Musk buying Twitter Open Markets Institute Director Barry Lynn issues the following statement:*

Yesterday Twitter's board agreed to sell the corporation to Elon Musk, the owner of Tesla and SpaceX. The Open Markets Institute believes the deal poses a number of immediate and direct threats to American democracy and free speech. Open Markets also believes the deal violates existing law, and that the Federal Communications Commission (FCC), the Department of Justice (DOJ), and the Federal Trade Commission (FTC) have ample authority to block it.

The most obvious problem is that the deal would give to a single man – one who already wields immense political and economic power – direct control over one of world's most important platforms for public communications and debate. As has been true from the Founding, the American people have an absolute right to ensure the full openness and neutrality of all essential public infrastructure. Specific to communications, we see this in Article I, Section 8 of the Constitution, in the Telegraph acts of 1860 and 1866, the Mann-Elkins Act of 1910, the Communications Act of 1934, and many other federal and state laws. Americans have also repeatedly used our antitrust laws to prevent concentrations of power over communications, speech, debate, and news.

Yesterday's deal also violates the law at a more technical level. Mr. Musk already controls one of the most important internet platforms in the world – in the form of the satellite communications system Starlink. Since the late 19th Century, the U.S. government has routinely acted to prevent mergers between existing essential platforms. Most recently, the DOJ in 2017 attempted to block AT&T's takeover of Time-Warner (an effort which failed because the DOJ filed a poor case, as OMI made clear at the time). This means that just as we would now expect the U.S. government to block a takeover of Twitter by Google, Facebook, Comcast, or Verizon, the same rules apply to the owners of Starlink.

Let's be clear. Elon Musk's effort to buy Twitter is not the only threat to free communications and debate in the United States. The size, scope, and business models of Facebook, Google, and Amazon also pose a wide variety of often extreme threats to American democracy and the basic rights of citizens. That's why law enforcers and Congress should view this deal as an opportunity to firmly reestablish clear bans on any manipulation of communications by essential platforms, and to eliminate all business models that rely on such manipulation.

Finally, as Open Markets made clear in [this article](#) in the Washington Monthly, it's past time for the FCC to get serious about regulating Starlink to ensure that this vital and increasingly important Internet platform serves the public interest only.

Appendix 11



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

Office of the Chair

June 24, 2022

The Honorable Jim Jordan
Ranking Member
Committee on the Judiciary
U.S. Houses of Representatives
Washington, D.C. 20515

Dear Ranking Member Jordan:

Thank you for your May 24, 2022, letter regarding the proposed acquisition of Twitter by Elon Musk. Generally speaking, the goal of every FTC merger review is to determine whether the transaction violates the antitrust laws.

Below are the responses to the three informational requests presented in your letter:

1. ***All documents and communication between or among the Federal Trade Commission and any third-party organizations referring or relating to Mr. Musk's purchase of Twitter.***

The only responsive document to this request is enclosed.

2. ***All documents and communication between or among the Federal Trade Commission and members and staff of the White House Competition Council referring or relating to Mr. Musk's purchase of Twitter.***

Inter-governmental discussions generally are protected under various exemptions, including the deliberative-process privilege, attorney-client privilege, and attorney work product privilege. In addition, the Commission's longstanding policy is that if the agency receives a legally binding request that may require the disclosure of information protected by executive privilege, the FTC will inform the White House so that the President can decide whether to invoke executive privilege.

3. ***All documents and communications, including all plans, proposals, or other communications, referring, or relating to the FTC's purpose in making inquiries related to Mr. Musk's purchase of Twitter that deviate from typical reviews.***

There are no such documents or communications.

Thank you again for your letter. If you have any questions, please feel free to have your staff call [REDACTED] the Director of our Office of Congressional Relations, at [REDACTED] [REDACTED]

Sincerely,



Lina M. Khan
Chair, Federal Trade Commission

Enclosure



COMPUTER INFORMATION ALLIANCE FOUNDATION
400 NORTH TAMPA ST, 15TH FL, TAMPA, Floor, 33602
9544447408
cio-alves@minixel.com
<https://oneye.us>

Federal Trade Commission. Bureau of Competition
Office of Policy and Coordination, Room CC-5422
Bureau of Competition, 600 Pennsylvania Ave., NW
Washington, DC 20580, Telephone: (202) 326-3300

April 26, 2022

Dear Federal Trade Commission,

As we all know, the mission of the FTC, as defined by Congress, is “*to protect consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity.*” With the above statement in mind is that I am writing to you to respectfully demand that Citizen Elon Musk be stopped from buying and taking private the so far public company called Twitter, INC.

Your duty as a Federal Agency, is, above all, to protect the American economy from predatory actors and preclude fraud by establishing rules that make it hard to create havoc in the life of millions of investors. It happens that this operation will doom the company, and it will cause a hole of \$US 43 BN in banks, pensions funds, mutual funds, etc., but in the end, the money will be lost to the American people. How do I know this? Citizen Musk is NOT buying the company outright, with his own money, he is borrowing some \$US 43 BN, and the interest alone to service this loan is estimated to be \$US 2.5 BN/year, more than double the available Twitter’s revenue after direct operating expenses. The Commission may verify these figures against the public filings and also it may request details of the transaction from Citizen Musk. This is an absolutely unacceptable model, and the FTC must step in and forbid the actors to commit what constitutes a fraud against the American people. Furthermore, being a private company, the new Twitter, INC, will not be able to sell shares in the public market to raise capital and cover temporary operating losses. Private banks will never lend money to a business that is unable to service its existing debt. This is a Kamikaze operation and it must be stopped.

Yours truly
Federico Alves
President, CIAF

Appendix 12

Open Markets Institute Statement in response to Elon Musk Buying Twitter

October 27, 2022 - Press Releases, Public Comments - Open Markets



FOR IMMEDIATE RELEASE: October 27, 2022

CONTACT: Ashly Woolhiser woolhiser@openmarketsinstitute.org

In response to Elon Musk buying Twitter Open Markets Institute Director Barry Lynn issues the following statement:

WASHINGTON- "The Open Markets Institute believes Elon Musk's deal to buy Twitter poses a number of immediate and direct threats to American democracy, free speech, and national security. Open Markets believes the deal violates existing law and that the Department of Justice (DOJ), Federal Communications Commission (FCC), and the Federal Trade Commission (FTC) each have ample authority to block it. We also believe the Securities and Exchange Commission (SEC), Department of Defense (DOD), and the Committee on Foreign Investment in the U.S. (CFIUS) each have a duty to vet this takeover closely.

The most obvious problem is that the deal would give to one man – who already wields enormous economic and political power – direct control over one of world's most important platforms for public communications and debate. As has been true from the Founding, the American people have both an absolute right and responsibility to regulate all essential public communications infrastructure to ensure its full openness and neutrality, and freedom from foreign influence.

And let's be clear, Elon Musk is no run-of-the-mill billionaire. In recent months he has repeatedly meddled in delicate foreign policy issues in ways that demonstrate a seeming disregard for the security of the United States and its closest allies in a time of war and economic conflict. This includes shutting down his Starlink satellite system in certain parts of Ukraine, in ways that appear to support Russian and Chinese interests and demands. And it includes undermining U.S. policy on Taiwan at a moment when China is threatening to invade or blockade that island. In reporting these actions, the New York Times this week described Musk as a "geopolitical chaos agent."

Then there's the fact that Musk has exploited Twitter and other communications platforms to engage in fraudulent misrepresentations of his own businesses, as he admitted in 2018 in a settlement with the SEC. And just this week Reuters reported that the DOJ is investigating Tesla for fraudulent statements about its autopilot system.

Specific to domestic communications, Musk's statements on Twitter's regulation of its own platform show a basic misunderstanding of how the United States protects freedom of expression. In addition to using our antimonopoly laws to prevent concentrations of power over communications, speech, debate, and news, Americans also use both private and public regulation to ensure platforms are not used to promote violence or spread dangerous disinformation, as Donald Trump used Twitter to do.

One way law enforcers can move swiftly to block Musk's takeover of Twitter is to focus on his existing ownership of Starlink. As its use in Ukraine demonstrates, Starlink has become one the most important communications platforms in the world. Since the late 19th Century, the U.S. government has routinely acted to ensure the separation of essential platforms. This includes the 1913 order to AT&T to spin off Western Union, the 1956 consent decree with AT&T that blocked a move into publishing, and most recently, the DOJ's 2017 attempt to block AT&T's takeover of Time-Warner (an effort which failed only because the DOJ filed a poor case, as OMI made clear at the time). Just as we would now expect law enforcers to block a takeover of Twitter by Google, Facebook, Comcast, or Verizon, the same rules apply to the owners of Starlink.

Elon Musk's effort to buy Twitter is not the only threat to free communications and debate in the United States. The size, scope, and business models of Google, Amazon, and Facebook also pose a wide variety of threats to American democracy and the basic rights of citizens. That's why law enforcers and Congress should also view this deal as a big step towards eliminating all business models that rely on the manipulation of communications, commerce, and debate."

Lynn also commented in April on Musk's initial plans to purchase the social media site, outlining why the deal would both pose risks to democracy and free speech and violate existing antitrust law. Since then Musk's reckless engagement in national security matters has made it even more clear why the public must block his effort to capture control over this essential public communications platform

###

The Open Markets Institute is a team of journalists, researchers, lawyers, economists, and advocates working together to expose and reverse the stranglehold that corporate monopolies have on our country.

Appendix 13

November 16, 2022

To: Jonathan Kanter
Assistant Attorney General, Department of Justice Antitrust Division

Jessica Rosenworcel
Chair, Federal Communications Commission

Lina Khan
Chair, Federal Trade Commission

The Open Markets Institute respectfully calls on your offices to fully investigate Elon Musk’s takeover of the communications platform Twitter. The deal raises many fundamental questions about the independence and integrity of essential communications services in America.

No democracy can survive if its citizens allow one or few private individuals to seize control over the public square or public marketplace, or any platform or network essential to the ability of citizens to speak with and do business with one another. Citizens of democracies therefore have an absolute right and duty to protect the independence, neutrality, and economic wellbeing of every communications and commercial platform and network.

It is vital to move swiftly. The Twitter platform long ago proved it serves a unique and irreplaceable role in enabling citizens to communicate and to debate key issues of the day.¹ Twitter’s character as a utility is even more clear when we look at how the platform has been used during emergencies such as Hurricane Ian in Florida, earthquakes in Mexico and Japan, floods in Pakistan, and fires in Australia. In the company’s own words, “Over the years, Twitter has become a critical communication tool for responding to natural disasters.”² One way it does so is by creating a “centralized source of credible information.”³

Yet now, people in the United States and around the world are watching a single man radically alter this essential communications platform to favor his own personal interests and political views. And indeed, since Mr. Musk took control of Twitter on October 27, there are many well-documented reports that he or people working for him have interfered directly in public debate on that platform.⁴ Similarly, people across the United States and around the world are watching Mr. Musk potentially destroy – out of greed, recklessness, or incompetence – a service that has proven critical to their safety, and around which they have institutionalized entire systems of emergency response.

A second reason to move immediately is that Mr. Musk controls the satellite-based Internet service provider Starlink. Although as yet unfinished, Starlink in recent months has proven to be a highly effective technology, one that is of critical importance to the security of the United States, its citizens, and to allies such as the Ukraine and Taiwan.⁵ Over this same period,

however, Mr. Musk has repeatedly interfered in the normal operations of Starlink in ways that appear to promote his personal economic and political interests.⁶ It is therefore anything but inconceivable that Mr. Musk will manage Starlink in ways that disrupt Twitter, or vice versa.

We fully understand that this deal does not fit easily into some of the categories your agencies have relied on in recent years to determine when and how to investigate takeovers or certain corporate actions. But we are very confident that each of your agencies has ample authority to fully review this takeover, and if necessary to unwind or restructure the deal and/or regulate the actions of the combined corporations. The Department of Justice played exactly such a role with America's main telephone corporation, AT&T, in 1913, 1956, and 1982.⁷ The American people created the Federal Communications Commission precisely to guarantee the independence and integrity of our communications platforms and news and entertainment media⁸ (including, in 2018, Starlink).⁹ And the Federal Trade Commission has routinely acted to ensure that industries vital to democracy are protected from the concentration and misuse of private power.¹⁰ Over the years this includes newspapers, book publishing, and online communications platforms (including, in 2011, Twitter).¹¹

Indeed, the FTC's statement on November 10, 2022 that it intends to use the original text of the Federal Trade Act of 1914 to guide enforcement of the "federal ban on unfair methods of competition" provides an excellent model for all three agencies to adopt in assessing the nature of the threats posed by Mr. Musk's takeover of Twitter, and for cataloging the many authorities available to address those threats.¹²

Ultimately, your responsibility derives from the Constitution itself. As Supreme Court Justice Anthony M. Kennedy wrote in 1994, "The First Amendment's command that government not impede the freedom of speech does not disable the government from taking steps to ensure that private interests not restrict, through physical control of the critical pathway of communication, the free flow of information and ideas."¹³

You are not alone in having a duty to review this combination and to act to protect our democracy and security. At least six other departments, agencies, and offices have a responsibility to work with you on a thorough investigation of Mr. Musk's takeover and management of Twitter, and his management of Starlink: the Committee on Investment in the United States (CFIUS), the Securities and Exchange Commission (SEC), the Consumer Financial Protection Bureau (CFPB), the Department of Defense, the Department of Treasury, and the Federal Reserve.

That said, only your agencies have the ability to lead and coordinate this investigation. Your offices and staffs are uniquely equipped to: 1) identify threats to freedom of expression and freedom of the press posed by dangerous forms of vertical integration and arbitrary and discriminatory provision of services; 2) wield a wide and sophisticated range of regulatory tools to address such threats; 3) help other departments and agencies understand such threats and how to use their own authorities to protect democracy and the public interest; and 4) establish rules that empower citizens to safely benefit from the full promise of new technologies.

We believe the following goals should guide your work and that of the other offices in the U.S. government with whom you partner:

- Ensuring the complete independence of Twitter and Starlink from foreign interests.
- Ensuring the complete Independence of Twitter and Starlink from other business interests.
- Protecting all communications and political debates on Twitter and Starlink from any interference by Twitter and Starlink executives, board members, and employees.
- Ensuring both Twitter and Starlink establish clear terms of service for all users, and enforce those terms without prejudice or discrimination, in a completely transparent fashion.
- Ensuring that present management of Twitter and Starlink does not pose any avoidable threat to the stability and viability of Twitter Starlink.
- Protecting the interests and properties of Twitter users, who are the people who built that platform into an essential communications network.
- Protecting the privacy of every Twitter and Starlink user.
- Protecting small and medium-scale investors in Twitter, SpaceX/Starlink, and Tesla.
- Preventing any use of the Twitter and Starlink platforms to sidestep financial and monetary regulatory regimes, or to promote dangerous speculation.
- Preventing any leveraging of the monopoly nature of the Twitter and Starlink platforms to concentrate power over other businesses and markets.

There is no reasonable excuse for delay. On its own, an investigation by CFIUS into ownership of Twitter is not sufficient.¹⁴ The same is true for FTC enforcement of its consent decree with Twitter on privacy.¹⁵ The same is true The public has a right to know that the U.S. government is investigating *every* potentially troublesome aspect of this deal, and using *every* existing authority to ensure that the managers of Twitter and Starlink neither misuse nor destroy either platform.

It is important to state that our aim in writing you is not to target Mr. Musk personally. No matter who controlled Starlink and Twitter, we would call for the same close review of any deal involving these two entities.

In ending, it's worth remembering Justice Hugo Black's assurance in 1945 that enforcement of antimonopoly law against powerful communications platforms does not, in any respect, constitute regulation of speech or of the press. On the contrary, as Justice Black said, "it would be strange indeed... if the grave concern for freedom of the press which prompted adoption of the First Amendment should be read as a command that the government was without power to protect that freedom."¹⁶

Thank you.

The Open Markets Institute.

¹ As Lydia Polgreen of the *New York Times* put it, "Musk is right that the world needs a digital public square; unfortunately, he seems to have little idea that creating one involves balancing free speech against abuse, misinformation and government overreach. Twitter had just barely managed to get the hang of that difficult, important work in the past couple of years. Musk has left little doubt that rather than continue that work, he'd rather burn it all down." *If You Want to Understand How Dangerous Musk Is, Look Outside America*, NEW YORK TIMES (Nov. 14, 2022).

² *When Natural Disasters Happen, Twitter Can Be Used to Help. Here's How*, TWITTER (Oct. 13, 2022), https://blog.twitter.com/en_us/topics/company/2022/when-natural-disasters-happen-twitter-can-help-heres-how.

³ *Id.*

⁴ Barbara Ortutay, *Musk's Partisan Tweets Call Twitter Neutrality into Question*, AP NEWS (Nov. 7, 2022), <https://apnews.com/article/elon-musk-twitter-inc-technology-cbd873f1>.

⁵ See Alex Marquardt, *Musk's SpaceX Says It Can No Longer Pay For Critical Satellite Services in Ukraine, Asks Pentagon to Pick Up the Tab*, CNN (Oct. 14, 2022), <https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine>; see also Karina Tsui, *Taiwan, Looking to Ukraine, Pursues Internet Backup*, WASH. POST (Oct. 6, 2022), <https://www.washingtonpost.com/world/2022/10/06/taiwan-ukraine-satellite-interent-china-russia/>.

⁶ Mehul Srivastava et al., *Ukrainian Forces Report Starlink Outages During Push Against Russia*, FIN. TIMES (Oct. 7, 2022), <https://www.ft.com/content/9a7b922b-2435-4ac7-acdb-0ec9a6dc8397>.

⁷ See Daniel A. Hanley et al., *Financing Free Speech: A Typology of Government Competition Policies in Information, Communication, and Media Markets*, CTR. FOR JOURNALISM & LIBERTY 5-6, 10-11 (Sept. 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4089870.

⁸ Daniel A. Hanley, *Administrative Antimonopoly*, OPEN MARKETS INST. 7 (Feb. 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4044077.

⁹ *Why Are We Letting Monopolists Corner Space?* Luke Goldstein, Washington Monthly, Nov./Dec. 2021.

¹⁰ See generally Sandeep Vaheesan, *Resurrecting "A Comprehensive Charter of Economic Liberty": The Latent Power of the Federal Trade Commission*, 19 U. PA. J. BUS. L. 645 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830702.

¹¹ American citizens have used their state and federal governments to guarantee the neutrality and financial stability of electronic communications systems since passing the first laws regulating telegraph services in the mid-19th century. See RICHARD R. JOHN, NETWORK NATION: INVENTING AMERICAN TELECOMMUNICATIONS (2010); see, e.g., Act of July 1, 1862, § 15, 12 Stat. 489 (1862).

¹² *FTC Restores Rigorous Enforcement of Law Banning Unfair Methods of Competition*, FTC, Nov. 10, 2022.

¹³ *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 657 (1994).

¹⁴ *Musk's Foreign Investors in Twitter Are "Worthy" of Review*, Biden Says, Rebecca Kern, Politico, Nov. 9, 2022.

¹⁵ *In the Matter of Twitter, Inc.*, 151 F.T.C. 162 (2011).

¹⁶ *Associated Press v. United States*, 326 U.S. 1 (1945)

Appendix 14

PRESS STATEMENT DEC 21, 2022

STATEMENT: The FTC, Congress, and Advertisers Must Hold Elon Musk and Twitter Accountable, Say Progressive Groups

CONTACT



Julia Cusick

[Restoring Social Trust in Democracy](#)



Washington, D.C. — In his latest erratic behavior since buying Twitter, Elon Musk suspended several journalists, then abruptly reinstated some. In response, 14 groups issued the following statement:

As organizations deeply attached to democracy, to our freedom of expression, and to our fundamental rights, we cannot remain silent about Elon Musk's reckless decision to suspend numerous journalists' Twitter accounts. The reversal of some of these suspensions over the weekend does not diminish this attempt to silence journalists for simply doing their jobs.

Journalism is the cornerstone of free speech, and any attack on journalism is an assault on one of our fundamental pillars. While pretending to give power back to the people, Elon Musk is actually turning Twitter into an autocratic system where neo-Nazi accounts are restored while journalists' accounts are suspended. This is a dangerous turn that raises deep concerns. Journalists doing fact-based reporting have been a critical part of Twitter's success, and Elon Musk's apparent disdain for journalism and fundamental rights must be rebutted with clear shows of support from throughout civil society.

If Elon Musk is as committed to freedom of expression and democracy as he states, then it is not enough to reverse his incorrect decision; he also must guarantee appropriate safeguards to protect journalists and voices of interrogation and dissent on his platform, even and especially when he is the one they may be holding accountable.

While Musk may own Twitter, we all have a role to play in ensuring accountability on the platform:

1 All advertisers should take notice of these dangerous actions and ensure Elon Musk does not profit from dismantling one of the world's most influential communications platforms.

2 The Federal Trade Commission (FTC) should determine if any of Musk's actions since taking over Twitter—including broken public promises around the site's terms of service and efforts to protect users' privacy and safety—violate the company's existing consent decree or any other laws enforced by the commission. The commission should share those findings with the public.

3 Congress should move quickly to hold hearings on this incident and the potential for a privately held forum for national dialogue to endanger journalism and U.S. democracy. It should also explore potential remedies.

The undersigned,

Accountable Tech
AFL-CIO
American Federation of Teachers
Center for American Progress
Common Cause
Indivisible
GLAAD
Media Matters for America
MoveOn
National Education Association
National Women's Law Center
Public Citizen
Public Knowledge
SEIU

Appendix 15

United States Senate
WASHINGTON, DC 20510

November 17, 2022

The Honorable Lina Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chair Khan,

We write regarding Twitter’s serious, willful disregard for the safety and security of its users, and encourage the Federal Trade Commission (FTC) to investigate any breach of Twitter’s consent decree or other violations of our consumer protection laws.

In recent weeks, Twitter’s new Chief Executive Officer, Elon Musk, has taken alarming steps that have undermined the integrity and safety of the platform, and announced new features despite clear warnings those changes would be abused for fraud, scams, and dangerous impersonation. According to media reports, in prioritizing increasing profits and cutting costs, Twitter’s executives have dismissed key staff, scaled back internal privacy reviews, and forced engineers to take on legal liability for new changes — preventing managers and staff tasked with overseeing safety and legal compliance from reviewing the product updates.¹ Moreover, key Twitter executives responsible for the platform’s privacy, cybersecurity, and integrity resigned last week, further calling into question whether personal data is adequately protected from misuse or breach while the company explores new products and monetization strategies.²

Users are already facing the serious repercussions of this growth-at-all-costs strategy. Since the launch of the verification feature over a decade ago, Twitter users have come to rely on the blue checkmark as an assurance that prominent users are who they claim to be — the most clear sign that an account is trustworthy. When Mr. Musk announced plans to open Twitter’s verification services to all paying users, experts warned the change would exacerbate the

¹ “Two Weeks of Chaos: Inside Elon Musk’s Takeover of Twitter.” New York Times.
<https://www.nytimes.com/2022/11/11/technology/elon-musk-twitter-takeover.html>

² “Twitter’s Security And Privacy Leaders Quit Amidst Musk’s Chaotic Takeover.” Forbes.
<https://www.forbes.com/sites/thomasbrewster/2022/11/10/twitter-security-privacy-compliance-leads-quit-elon-musk-takeover/>

platform's already rampant problems with financial scams, foreign disinformation, and public safety threats.³ These misguided changes come at a time when Twitter is facing coordinated campaigns of racist, misogynistic, and antisemitic harassment, attempting to exploit the change in ownership to spread hate and vitriol.⁴

Despite these warnings, Mr. Musk pressed ahead and launched the feature, resulting in fake accounts impersonating President Biden, Senators, athletes, companies, and others.⁵ Of particular concern, these fake accounts included scammers impersonating companies and celebrities for cryptocurrency schemes, identity theft, and other financial crimes.⁶ Twitter knew in advance that there was high likelihood the Twitter Blue product could be used for fraud, and still it took no action to prevent consumers from being harmed until this rampant impersonation became a public relations crisis.⁷

We are concerned that the actions taken by Mr. Musk and others in Twitter management could already represent a violation of the FTC's consent decree, which prohibits misrepresentation and requires that Twitter maintain a comprehensive information security program. The FTC was already on notice, even prior to Mr. Musk's acquisition, about Twitter's recent inadequate security practices based on whistleblower disclosures by Twitter's former Security Lead Peiter "Mudge" Zatkó.⁸ Earlier this year, Twitter agreed to pay \$150 million to settle allegations by the FTC and the Department of Justice that Twitter violated the Federal Trade Commission Act and its 2011 consent decree with the FTC by deceiving users about the company's privacy and security practices.⁹ We fear that Mr. Musk's reported changes to internal reviews and data security practices further put consumers at risk and could directly violate the

³ "Elon Musk wants Twitter users to pay to be verified. It could create a new set of headaches for the company." CNN. <https://www.cnn.com/2022/11/03/tech/elon-musk-twitter-verification-plans>

⁴ "Antisemitic campaign tries to capitalize on Elon Musk's Twitter takeover." New York Times. <https://www.nytimes.com/2022/10/28/technology/musk-twitter-antisemitism.html>

⁵ Letter from Senator Markey to Twitter Chief Executive Officer Elon Musk. <https://www.markey.senate.gov/news/press-releases/senator-markey-demands-answers-from-twitter-on-disinformation-and-fake-accounts>

For \$8, Twitter Blue users create a wave of checkmarked imposter accounts. Ars Technica. <https://arstechnica.com/gaming/2022/11/twitter-scammers-use-musks-paid-checkmarks-to-spread-official-looking-fake-news/>

⁶ "Elon Musk's Twitter Is a Scammer's Paradise." Wired. <https://www.wired.com/story/twitter-blue-check-verification-buy-scams/>

⁷ "Elon Musk wants Twitter users to pay for their blue checks. What could possibly go wrong?" NBC News. <https://www.nbcnews.com/think/opinion/elon-musk-just-changed-meaning-twiters-coveted-blue-check-rcna55121>

⁸ Letter from Senator Blumenthal to the Federal Trade Commission. <https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-calls-on-ftc-to-investigate-twitter-whistleblower-claims>

⁹ "Twitter to pay \$150 million penalty for allegedly breaking its privacy promises – again." Federal Trade Commission. <https://www.ftc.gov/business-guidance/blog/2022/05/twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again>

"Twitter Agrees with DOJ and FTC to Pay \$150 Million Civil Penalty and to Implement Comprehensive Compliance Program to Resolve Alleged Data Privacy Violations." Department of Justice. <https://www.justice.gov/opa/pr/twitter-agrees-doj-and-ftc-pay-150-million-civil-penalty-and-implement-comprehensive>.

requirements of the consent decree. One Twitter lawyer was concerned enough about potential legal violations and management’s attitude toward the consent decree that they advised colleagues to seek legal counsel.¹⁰

We urge the Commission to vigorously oversee its consent decree with Twitter and to bring enforcement actions against any breaches or business practices that are unfair or deceptive, including bringing civil penalties and imposing liability on individual Twitter executives where appropriate. As you recently noted in Senate testimony, “no CEO or company is above the law, and companies must follow our consent decrees.”¹¹

Thank you for your attention to this important matter.

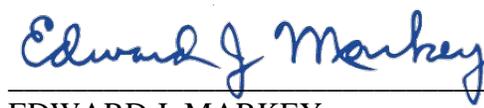
Sincerely,

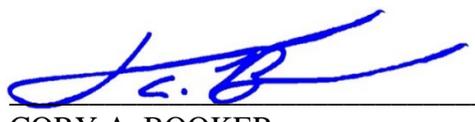

RICHARD BLUMENTHAL
United States Senate


DIANNE FEINSTEIN
United States Senate


BEN RAY LUJÁN
United States Senate


ELIZABETH WARREN
United States Senate


EDWARD J. MARKEY
United States Senate


CORY A. BOOKER
United States Senate


ROBERT MENENDEZ
United States Senate

¹⁰ “Elon Musk is putting Twitter at risk of billions in fines, warns company lawyer.” The Verge.

<https://www.theverge.com/2022/11/10/23451198/twitter-ftc-elon-musk-lawyer-changes-fine-warning>

¹¹ FTC Chair Lina M. Khan Testifies Before Senate Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights. Federal Trade Commission. <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-chair-lina-m-khan-testifies-senate-judiciary-subcommittee-antitrust-competition-policy-consumer-rights>