Before the
FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue NW
Washington, DC 20580

Petition to Reopen, Set Aside, or in the Alternative, Modify Order	)	FTC Docket No. C-4316 Twitter, Inc.

COMMENT OF THE CALIFORNIA BUSINESS & CONSUMER SERVICES AGENCY

The California Business & Consumer Services Agency writes to outline its opposition to the petition to terminate the Federal Trade Commission's (FTC or Commission) order regarding X (formerly known as Twitter). This submission outlines why the petition fails to meet the Commission's standard for setting aside the order. Moreover, if the FTC terminates the order, this raises the appearance of another politically motivated pardon for individuals and firms connected to the Trump Administration.

Social Media Privacy and Data Security is Critical for Consumers

Safeguarding personal data is critical for protecting consumers and securing critical systems in our economy. When sensitive data is compromised, this can create conditions for fraud and scams. For example, when a bad actor exfiltrates personal information, this makes it easier to engage in phishing, social engineering campaigns, and tech-enabled scams. In addition, when sensitive personal information falls into the wrong hands, this also creates the risk of intrusions into critical systems that affect our everyday lives.

Many social media platforms retain large quantities of information about individual users. Consumers reasonably expect that this information is kept secure. When it is not, it can lead to a host of harms.

Like other states, California consumers have suffered significant losses from identity theft and scams. Older adults and members of the military face particular risks when it comes to identity theft. In addition, access to sensitive information, like social media messages, can even heighten the risk of stalking and other abuse.

Many users on social media platforms like X participate anonymously. They may not wish to reveal which accounts they follow or consume content from. But, according to media reports, in

April 2025, personal information on 200 million X users was allegedly circulating online.[1] The information could apparently be used to link user e-mail addresses with usernames. When someone knows an individual's e-mail address, it becomes much easier to determine their actual identity. In the case of this alleged leak, individuals who did not wish to reveal their personal identities may have had information compromised. Sophisticated hackers and scammers can often combine information obtained from multiple breaches that can leave consumers more vulnerable.

Background on California's New Consumer Agency

On July 1, 2026, Governor Gavin Newsom launched the Business & Consumer Services Agency. The Agency oversees dozens of departments, boards, and bureaus that protect consumers and competition.

The Agency has a strong interest in the work of the Federal Trade Commission. For example, California law dictates that the Agency's Department of Consumer Affairs accepts complaints from the public on "unfair methods of competition" and "unfair or deceptive acts or practices."[2] This mirrors the prohibitions outlined in the Federal Trade Commission Act.[3] Other departments within the Agency also enforce certain data security and privacy requirements.

The 2010 and the 2022 Law Enforcement Orders

In 2010, Twitter entered into a settlement with the FTC.[4] The FTC charged Twitter with making material misrepresentations about its privacy and security. Despite Twitter's representations about its privacy and security, the FTC identified serious lapses in the company's data security which allowed hackers to infiltrate Twitter, including access to non-public user information, tweets that consumers had designated private, and the ability to send out phony tweets from any account including those belonging to then-President-elect Barack Obama and Fox News, among others.

While Twitter paid no monetary penalty, it willingly agreed to take certain corrective measures, including retaining an independent assessor to ensure it maintained appropriate privacy and security controls. Importantly, Twitter agreed to be bound by an order that would trigger penalties if it made any misrepresentations regarding its privacy and security. The settlement was approved by the FTC by a 5-0 vote.

In 2022, the FTC and the Department of Justice charged Twitter with violating the previous order.[5] Specifically, it found that Twitter baited users to provide personal phone numbers for the purpose of two-factor authentication. 140 million users provided a phone number or e-mail to participate in the enhanced security protocols. In reality, Twitter used the phone numbers to feed

---

1 https://mashable.com/article/elon-musk-x-twitter-breach-data-leak-breachforums
2 Cal. Bus. & Prof. Code, § 325
3 15 U.S.C. § 45
4 https://www.ftc.gov/news-events/news/press-releases/2010/06/twitter-settles-charges-it-failed-protect-consumers-personal-information-company-will-establish
5 https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads

its advertising targeting and monetization. The FTC also noted that Twitter's conduct violated international privacy agreements with the European Union and Switzerland.

Twitter agreed to pay $150 million and agreed to a modified order through 2042. The FTC approved this by a 4-0 vote.

The May 2026 Request for Pardon

On May 15, 2026, X, a corporation that operates X.com and ultimately controlled by Elon Musk, submitted a petition[6] that seeks to terminate a law enforcement order otherwise set to expire in 2042.

The pardon request is pursuant to Section 5(b) of the Federal Trade Commission Act, 15 U.S.C. § 45(b), and Section 2.51 of the Federal Trade Commission Rules of Practice, 16 C.F.R. § 2.51. The request "shall contain a satisfactory showing that changed conditions of law or fact… or that the public interest so requires."

The petition offers a series of reasons why the Commission should pardon X, including claims about how the remedial purposes of the order have been fully addressed.

The Commission Should Deny the Petition

The California Business & Consumer Services Agency has reviewed the Federal Trade Commission's use of the petition process to terminate orders. Termination of an order, particularly a relatively recent order, is unprecedented, particularly for repeat offenders.

In general, the Commission has modified orders to ensure that the order's requirements do not disrupt the remedial purpose of the order. In this case, the Commission put in place certain safeguards – which, again, the company willingly agreed to – in order to prevent further violations of law related to privacy and security.

In the docket, the Commission published a summary of the petition's arguments.[7] This submission briefly addresses each of these arguments described in the summary.

First, X claims that the company "no longer exists." While it is true that Twitter was the subject of a takeover by Elon Musk, it is standard practice to ensure that law enforcement orders can't simply disappear by virtue of a change in ownership. The petition also claims that all of the employees previously involved with the company are gone. However, the law enforcement action did not claim that the wrongdoing was due to an individual wrongdoer. Instead, the law violations occurred because the company failed to put in place basic controls to protect consumer privacy and the company engaged in bait-and-switch tactics when it collected personal phone numbers. The company *twice* agreed that the company would be subject to the order's restrictions.

[6] https://downloads.regulations.gov/FTC-2026-0727-0002/content.pdf
[7] https://www.regulations.gov/document/FTC-2026-0727-0001

As mentioned above, last year's reports about the circulation of the personal information of 200 million users reinforce the need for ongoing vigilance into X's data security practices.

Second, X claims that the order addresses "obligations and protections already required by domestic and international privacy regimes and industry-recognized frameworks that X Corp. follows."[8] This argument is quite unusual. If X is already adhering to international rules, why is it unwilling to hold itself to the same standard in the United States of America?

Notably, while X complains about costs to adhere to the law enforcement order, the company does not proffer a more efficient solution to prove to the Commission that it will not compromise privacy and security again. Rather, it simply asks that the Commission destroy the order, which would eliminate the possibility of the Commission seeking penalties for wrongdoing.

Third, X asserts that the pardon would be consistent with the First Amendment. X asserts that the FTC previously sought information about whether X inappropriately shared users' personal information with third parties, such as journalists. Putting aside whether or not the petition accurately characterizes the facts, the company is not seeking targeted modifications to safeguard speech protected by the U.S. Constitution. Instead, it uses this argument pretextually as cover to obtain a full release from all obligations it agreed to under the order.

Finally, X notes that terminating the order supports American leadership in artificial intelligence. This argument is particularly weak. The most substantive requirement of the order is a prohibition on misrepresentations to users about privacy and security of their data. The petition raises a troubling question: does X believe that it must deceive the public to make advances to Grok?

Conclusion

As digital technologies continue to permeate all aspects of our society, it is critical that government agencies work together to ensure robust levels of privacy and data security. This can prevent financial losses and guard against a range of other harms to consumers.

In addition, corruption is deeply corrosive to competitive markets. The Federal Trade Commission should not be picking winners and losers based on political contributions or personal enrichment to the President.

The pardon request filed by X clearly fails to meet the standard outlined in the Commission's Rules of Practice. If the Commission grants the request, it raises the appearance of political favoritism toward Elon Musk.

In closing, we urge the Commission to deny the request to terminate the 2022 law enforcement order. We also request that the Commission disclose in the docket all communications between the Commission and representatives of Elon Musk and any of his affiliated companies, as well as any directives from the White House on this matter.

[8] https://www.regulations.gov/document/FTC-2026-0727-0001