epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

August 19, 2025

Chair Andrew Ferguson
Commissioner Rebecca Kelly Slaughter
Commissioner Melissa Holyoak
Commissioner Mark Meador

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: *Support King, LLC (SpyFone.com)*, FTC File No. 1923003

Dear Chair Ferguson and Commissioners Slaughter, Holyoak, and Meador,

By notice published on its website on July 18, 2025,[1] the Federal Trade Commission (FTC or Commission) announced that Scott Zuckerman of Support King (a.k.a. SpyFone) filed a petition (SpyFone Petition) on June 27, 2025[2] to the FTC to vacate or modify the agency's December 20, 2021 Order (SpyFone Order).[3] The same notice announced that the FTC seeks public comment on the SpyFone Petition by August 19, 2025.

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC routinely files comments in response to proposed FTC consent orders and

[1] *FTC Seeks Comment on Petition to Vacate 2021 Order Related to Provider of Stalkerware Apps*, Fed. Trade Comm'n (July 18, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/07/ftc-seeks-comment-petition-vacate-2021-order-related-provider-stalkerware-apps.
[2] Petition to Reopen and Vacate or Modify FTC Consent Order, *In re: Support King, LLC (SpyFone.com),* FTC File No. 192-3003, OSCAR No. 613623 (filed June 27, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/1923003-PETITIONTOREOPENANDVACATEORMODIFYFTCCONSENTORDER_0.pdf [hereinafter "Zuckerman Petition"].
[3] Decision and Order, *In re: Support King, LLC (SpyFone.com),* FTC File No. 192-3003 (Dec. 20, 2021), https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfoneorder.pdf [hereinafter "SpyFone Order"].

complaints regarding business practices that violate privacy rights,[4] including in response to the FTC's 2021 SpyFone Order.[5]

Public Knowledge is a nonprofit advocacy group that promotes freedom of expression, an open internet, and access to affordable communications tools and creative works.

The Center for Democracy and Technology (CDT) is a non-profit advocacy organization working to promote democratic values online and in new, existing, and emerging technologies.

The Demand Progress Education Fund (DPEF) is a nonpartisan, nonprofit organization that educates and empowers everyday people to push back on abuses by concentrated power centers in our economy, our nation's communications infrastructure, and our democracy, to hold them accountable, and to bring them under democratic control.

Fairplay is a nonprofit committed to helping children thrive in an increasingly commercialized, screen-obsessed culture, and the only organization dedicated to ending marketing to children.

Free Press is a nonprofit media and democracy advocacy organization, founded in 2003 to advocate for equitable access to technology, diverse and independent ownership of media platforms, and a media ecosystem that holds leaders accountable and enables communities to access critical information.

For the reasons below—not the least of which are the frightening implications of diluting a unanimous FTC decision that protects consumers from the type of surveillance that is characteristic of domestic abuse—the FTC should deny this petition in its entirety. This is not a close call; per the Commission's findings, the conduct of SpyFone under Mr. Zuckerman's leadership was egregious. EPIC, Public Knowledge, CDT, DPEF, Fairplay, and Free Press submit this letter to:

- Caution the agency about weakening the deterrent effect of its consent decrees generally as well as weakening the deterrent impact of this specific Order on stalkerware and related companies;
- Remind the FTC of the vital work its staff undertook to shut down a tool which was used to facilitate stalking and other forms of domestic violence and which failed to safeguard the data it was amassing on its intended victims;
- Urge the Commission to continue to uphold its mission of protecting consumers from privacy and data security harms inflicted by the companies who have chosen to collect and retain consumer data; and
- Note that the conduct at issue in this case has potentially criminal dimensions.

---

[4] *See, e.g.*, Comments of EPIC, Demand Progress, and EFF on Proposed Consent Order, *In re X-Mode Social, Inc.*, FTC File No. 202-3038 (Feb. 20, 2024), https://epic.org/documents/comments-of-epic-demand-progress-and-eff-in-re-the-federal-trade-commissions-proposed-order-settlement-with-x-mode-social-inc/; EPIC, *EPIC Commends FTC for Including Data Minimization & Data Rights in Chegg Settlement* (Dec. 12, 2022), https://epic.org/epic-commends-ftc-for-including-data-minimization-data-rights-in-chegg-settlement/.

[5] *See* Comments of EPIC on Proposed Consent Order, *In re Support King, LLC (SpyFone.com)*, FTC File No. 192-3003 (2021), https://epic.org/wp-content/uploads/2021/10/In-re-SpyFone-Order-EPIC-comment-100821.pdf, *also available at* https://www.regulations.gov/comment/FTC-2021-0042-0008.

I. Modifying the SpyFone Order per the SpyFone Petition would undermine the FTC as a consumer protection agency and embolden other purveyors of stalkerware.

Consent decrees serve several important functions, including remediating harms to consumers, permitting companies to avoid litigation by binding themselves to settlement terms, and putting the industry on notice that certain illegal practices will not be tolerated. A contract-like instrument such as a consent decree is less impactful when it is insinuated that one party can escape from their obligations. Both SpyFone and Mr. Zuckerman agreed to the terms of the 2021 SpyFone Order in lieu of further administrative and civil proceedings. Allowing the parties to this contract-like instrument to escape from obligations they explicitly agreed to without significant changes in the factual circumstances would imply that the FTC does not intend to hold companies or their executives accountable for their actions.

Moreover, especially where data security issues are concerned,[6] the FTC has often taken the approach of regulating an industry by indicating legal obligations through a pattern of consistent enforcement actions. This ability to shift industries in the right direction without rulemaking would be threatened by modifying the SpyFone Order, muddying what were supposed to be clear regulatory parameters.

Particularly in the aftermath of the Supreme Court's decision in *AMG Capital Management*,[7] the FTC's ability to secure redress for unlawful business practices is more limited when there is not an existing operative consent decree. In other words: if the agency were to grant Mr. Zuckerman's petition and he were to reoffend, the Commission might find it more difficult to effectively respond.[8] This would not only undermine the authority of the agency but also create an environment of uncertainty for the rest of the marketplace, leaving good actors to wonder what the rules of the road are and giving bad actors leeway to erode industry standards. This is especially concerning where the product or service at issue relates to consumer surveillance that very foreseeably could be—and in this instance apparently was—used to facilitate domestic violence.

a. A consent decree should only be modified in narrow circumstances not present here.

A consent decree should only be modified where the factual circumstances have changed so significantly that the initial order has been rendered unenforceable, or that continuing to enforce the order has demonstrably created a severe injustice, "nothing less than a clear showing of grievous

---

[6] *See, e.g.*, Comments of EPIC, *FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security*, 182 n.833-34 (Nov. 2022), available at https://epic.org/documents/disrupting-data-abuse-protecting-consumers-from-commercial-surveillance-in-the-online-ecosystem/ [hereinafter "Disrupting Data Abuse"].
[7] *See AMG Cap. Mgmt., LLC* v. *FTC,* 141 S. Ct. 1341 (2021).
[8] *See, e.g.*, Trade Rule on Impersonation of Government and Businesses, 89 Fed. Reg. 15,072 at 15,076, §V(A)(1) (proposed Mar. 1, 2024) (discussing the implications of the Supreme Court decision in *AMG*); *id.* at n.83 (noting differences between violations of existing rules and violations of existing cease and desist orders).

wrong evoked by new and unforeseen conditions."[9] A respondent who merely suggests that the settlement terms they agreed to earlier in order to avoid litigation are burdensome falls woefully short of this standard.

In this matter, the FTC notably approved both the initial Complaint[10] and the SpyFone Order unanimously.[11] Then-Commissioner Chopra considered this misconduct so egregious that after joining the 5-0 decision on the SpyFone Complaint (but before leaving the FTC prior to its 4-0 decision on the SpyFone Order), he published a statement noting his position was in favor of enforcement and even of referring the matter for criminal prosecution.[12]

The terms Mr. Zuckerman agreed to in the SpyFone Order are not burdensome; indeed, they were both proportional and likely to be effective. The SpyFone Order requires annual or biannual reporting (more frequent reporting in the event of a covered incident—e.g., a data breach—or in response to an affirmative request for compliance from the FTC). These terms are commensurate with the data security requirements the Commission has issued in other data breach actions.[13] These compliance measures are important because they ensure the respondent does not reoffend, both by creating friction to prevent further offenses and by making it harder to misrepresent one's compliance with the terms of the consent decree through mandatory reporting and certifications. To the extent these measures represent an affirmative penalty and not merely a harm reduction measure, that too serves an important deterrent function, warning away others who might engage in similar misconduct as Mr. Zuckerman and SpyFone.

EPIC previously applauded the Commission for holding not only SpyFone but also Mr. Zuckerman responsible for this dangerous misconduct.[14] The other arguments presented in this letter are adequate justification to deny the petition on their own, but coupled with the egregiousness of the conduct at issue, it would be a crushing abdication of the FTC's consumer protection duties to allow Mr. Zuckerman to escape the consequences of his actions. The FTC's Complaint outlines how Mr.

---

[9] *United States v. Swift & Co*., 286 U.S. 106, 119 (1932) (finding that even the decade-long transformation of the meat-packing industry caused by the rise of the grocery business was not a sufficiently significant change or sufficiently severe burden to merit modification of antitrust consent decree); *see also U. S. v. ITT Cont'l Baking Co.*, 420 U.S. 223, 237 (1975) (noting in context of FTC antitrust consent decree that consent decrees are treated as contracts for some purposes but not others, as they have attributes of both contracts and of administrative orders).

[10] *See FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data*, Fed. Trade Comm'n (Sept. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data.

[11] *See FTC Finalizes Order Banning Stalkerware Provider from Spyware Business*, Fed. Trade Comm'n (Dec. 21, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/12/ftc-finalizes-order-banning-stalkerware-provider-spyware-business.

[12] *See* Statement of Comm'r Rohit Chopra, *In re: SpyFone*, FTC File No. 192-3003 (Sept. 1, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-commissioner-rohit-chopra-matter-spyfone.

[13] *See, e.g.*, Section III(a) *infra*; *see also* Decision, *In re Global Tel*Link d/b/a GTL, d/b/a Via Path Technologies, et al.*, FTC File No. 212-3012 (Feb. 23, 2024); Decision, *In re Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC,* FTC File No. 192-3022 (Dec. 20, 2024).

[14] *See* Comments of EPIC on Proposed Consent Order *supra* note 5.

Zuckerman lied to consumers about an investigation and cooperation with law enforcement.[15] Articles published after the fact suggest that Mr. Zuckerman even ignored the ban he agreed to.[16] In his petition to modify the SpyFone Order, Mr. Zuckerman unconvincingly attempts to distance himself[17] from the actions of the company of which he was the CEO, founder, and resident agent; and on behalf of which he created websites, hired service providers, and signed contracts.[18] It is remarkable that Mr. Zuckerman claims "no consumer harm" resulted from a product that, on its face, facilitates domestic abuse.[19] The terms of the SpyFone Order are as much about preventing further harm caused by the mastermind of the company as it is about preventing harm caused by the company and its offerings.

b. Modifying the SpyFone Order would embolden other purveyors of stalkerware.

Companies look to the actions of regulators, such as the FTC, to inform their conduct—evaluating what is likely to result in liability and measuring this against the profit potential of the ethically dubious conduct they are considering (e.g., selling data to third parties, failing to implement fundamental cybersecurity protections, and peddling stalkerware). Industry guidance is awash with reporting on the FTC's enforcement actions and what they portend for every other actor in the

---

[15] *See* Complaint at ¶¶ 19-21, *In re: Support King, LLC (SpyFone.com) and Scott Zuckerman*, FTC File No. 192-3003 (Dec. 20, 2021), https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfonecomplaint_0.pdf [hereinafter "SpyFone Complaint"].

[16] *See, e.g.*, Zach Whittaker, *Support King, banned by FTC, linked to new phone spying operation*, TechCrunch (Dec. 17, 2022), https://techcrunch.com/2022/12/17/support-king-ftc-spytrac/ (noting that according to LinkedIn profiles and other work portfolios, the technical lead and other SpyFone developers also worked on SpyTrac and worked with Zuckerman on GovAssist). GovAssist was not mentioned in Zuckerman's petition, likely because the FTC clarified that that was outside the scope of the SpyFone Order. *See* Letter to Commenter Parental Values at 2, *In re: Support King, LLC (SpyFone.com)*, FTC File No. 192-3003, FTC Dkt. No. C-4756 (Dec. 20, 2021), https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfonelettercommenterparentalvalues.pdf [hereinafter "FTC Letter to Parental Values"].

[17] *See, e.g.*, Zuckerman Petition, *supra* note 2, at 3.

[18] See, e.g., SpyFone Complaint, *supra* note 15, at ¶ 2.

[19] Zuckerman Petition *supra* note 2, at 1. *See, e.g.*, Aaron Thomas, *The Abuser in Your Pocket How Stalkerware Threatens Women's Privacy*, Operation Safe Escape (Apr. 6, 2025), https://safeescape.org/stalkerware-threatens-womens-privacy/ ("The people who end up with this software on their phones can become victims of physical abuse and physical stalking. They get beaten. They can be killed. Their children can be kidnapped. It's the small end of a very large, terrifying wedge."); Andy Greenberg, *Hacker Eva Galperin Has a Plan to Eradicate Stalkerware*, Wired (Apr. 3, 2019), https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/; Press Release, *Attorney General James Secures $410,000 from Tech Companies for Illegally Promoting Spyware and Violating New Yorkers' Privacy*, New York State Attorney General (Feb. 2, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-secures-410000-tech-companies-illegally-promoting-spyware (noting stalkerware puts New Yorkers at risk of stalking and domestic abuse).

marketplace.[20] In response to public comments on the SpyFone Order, the Commission itself stated that:

> The relief in this proposed Order, in particular banning SpyFone from selling monitoring products or services in the future, demonstrates the Commission's commitment to protecting consumers from the very serious harms that can come from these types of privacy and security violations.[21]

By walking back its SpyFone Order, the Commission would inversely demonstrate a weaker commitment to protecting consumers from the types of surveillance that facilitate domestic violence.

II. The SpyFone Order shut down a tool used to facilitate stalking and other forms of domestic violence and reinforced the FTC's long-running efforts to strengthen cybersecurity.

Companies have a responsibility to consider the foreseeable misuses of their products and to incorporate guardrails to prevent such harms.[22] Cybersecurity practices to prevent data breaches are only one example of this, but where the company's offering facilitates surveillance, it is entirely foreseeable that misuse could entail stalking or other forms of domestic violence.[23] Because this implicates threats to personal safety, companies offering products and services facilitating surreptitious surveillance—to the extent that they are permitted to offer such products and services at all—should be held to a higher standard of protecting the privacy and security of consumer data.

a. Personal surveillance "features" inherent to offerings like stalkerware are inherently hazardous to consumers.

Companies should not be permitted to deliberately facilitate stalking and should be required to take precautions to prevent misuse of their products and services that could foreseeably result in stalking or other domestic violence-related harms.

---

[20] *See, e.g.*, Kirk J. Nahra, et al., *Recent Enforcement Actions Signal FTC Focus on Protecting Location Data*, WilmerHale (Feb. 9, 2024), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240209-recent-enforcement-actions-signal-ftc-focus-on-protecting-location-data (analyzing enforcement actions as indicative of focus on protecting location data). This includes reporting on industry takeaways from the SpyFone enforcement action specifically. *See, e.g.*, Natasha G. Kohne and Joseph Hold, *FTC on Data Breach: Complying with Breach Notification Laws Might Not Be Enough*, Akin (June 1, 2022), https://www.akingump.com/en/insights/blogs/ag-data-dive/ftc-on-data-breach-complying-with-breach-notification-laws-might-not-be-enough (noting misleading statements about investigating and cooperating with law enforcement); Dakota M. Coates, *Increasingly Active FTC Pursues Steep Penalties for Data Security and Privacy Practices*, Ice Miller (Dec. 16, 2022), https://www.icemiller.com/thought-leadership/increasingly-active-ftc-pursues-steep-penalties-for-data-security-and-privacy-practices (footnote about similar misrepresentations).

[21] FTC Letter to Parental Values, *supra* note 15, at 1.

[22] *See, e.g.*, *FTC v. Neovi*, 604 F.3d 1150, 1156 (9th Cir. 2010) ("Courts have long held that consumers are injured for purposes of the [FTC] Act not solely through the machinations of those with ill intentions, but also through the actions of those whose practices facilitate, or contribute to, ill intentioned schemes if the injury was a predictable consequence of those actions.") (internal citations omitted).

[23] *See, e.g.*, *Hughes et al v. Apple, Inc*, 723 F.Supp.3d 693, 696 (N.D. Cal. 2024), ("From the beginning, it was obvious that the AirTag would be an especially useful tool for stalkers.").

The Commission rightly alleged that it is an unfair business practice to "sell or have sold monitoring products and services that operate surreptitiously on mobile devices without taking reasonable steps to ensure that the purchasers use the monitoring products and services only for legitimate and lawful purposes."[24] Indeed, the very premise of SpyFone inherently violates privacy and facilitates domestic violence by revealing intimate details about the surveilled consumer to abusers in real time.[25] Cybersecurity best practices require exploitable products to have safeguards.[26] But SpyFone wasn't even created or marketed pretextually for a benign purpose that could be exploited: its premise was the exploitation itself.

As the FTC found, this stalking and surveillance causes mental and emotional abuse, financial and social harm, and physical harm—including death.[27] Indeed, stalkerware-style surveillance can facilitate other abuse-related practices such as coerced debt and identity theft[28] and can be effectuated

---

[24] SpyFone Complaint, *supra* note 15, at ¶ 29. *See also* Shannon Vavra, *'Rare' stalkerware emerges with targets around the world*, CyberScoop (Mar. 17, 2020), https://cyberscoop.com/monitorminor-stalkerware-kaspersky-research/ ("'The conceptual difference between parental control software and stalkerware is that they function in a different manner,' [Kaspersky researcher Viktor] Chebyshev told CyberScoop. 'Parental controls or services that truly have that legitimate focus would never hide its activity, and would notify a user that his or her data has been requested by a third party. Stalkerware has mechanisms that allow the app to remain hidden on the phone, making it hard to notice. This includes hiding the icon of the stalkerware app in the phone menu and even deleting its own logs and cleaning any traces it has made.'"); Internet of Things Advisory Board, Internet of Things (IoT) Advisory Board (IoTAB) Report 30 (Oct. 2024), https://www.nist.gov/system/files/documents/2024/10/21/The%20IoT%20of%20Things%20Oct%202024%20508%20FINAL_1.pdf (recommending a location tracking notice); *id*. at 95 (same).

[25] *See, e.g.*, Alvaro Puig, *SpyFone barred from selling stalking apps that secretly monitor phone activity*, FTC Consumer Blog (Sept. 2021), https://consumer.ftc.gov/consumer-alerts/2021/09/spyfone-barred-selling-stalking-apps-secretly-monitor-phone-activity.

[26] *See, e.g.*, Cybersecurity and Infrastructure Sec. Agency, *Protecting Against Malicious Use of Remote Monitoring and Management Software*, Cybersecurity Advisory: Alert Code AA23-025A (Jan. 26, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a; Rahul Chatterjee, et al., *The Spyware Used in Intimate Partner Violence*, 2018 IEEE Symposium on Sec. & Priv., SP 2018 (July 23, 2018), *available at* https://nixdell.com/papers/spyware.pdf (discussing the risks in dual-use apps); Comment of the Clinic to End Tech Abuse and Madison Tech Clinic at the University of Wisconsin-Madison to Fed. Commc'ns Comm'n at 4, *In re: Supporting Survivors of Domestic and Sexual Violence*, WC Docket No. 22-238 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/105241552112348 (discussing "physical proximity overrides" and "exclusive control" as anti-abusable design).

[27] *See* SpyFone complaint, *supra* note 15, at ¶ 22.

[28] *See, e.g.*, EPIC, *Letter Comment Supporting Petition for Rulemaking to Amend Identity Theft Definitions in the Fair Credit Reporting Act (Reg. V)*, CFPB-2024-0037-0001 (Oct. 4, 2024), *available at* https://epic.org/documents/letter-comment-supporting-petition-for-rulemaking-to-amend-identity-theft-definitions-in-the-fair-credit-reporting-act-regulation-v/. The National Consumer Law Center has a model law that outlines some of the contours of the coerced debt issue. *See* Andrea Bopp Stark, Carla Sanchez-Adams, National Consumer Law Center, *Model State Coerced Debt Law* (May 1, 2024), https://www.nclc.org/resources/model-state-coerced-debt-law/.

through a variety of products and services.[29] Shelters have reported stalkerware to be a pervasive problem.[30] Stalkerware has long been a prevalent threat.[31]

Regulators and the courts increasingly consider how best to prevent tech-facilitated abuse, such as that enabled by stalkerware like SpyFone. This includes the FTC,[32] the Federal Communications

---

[29] *See, e.g.*, Reply Comment of EPIC to Fed. Commc'ns Comm'n, *In re: Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 (May 24, 2024), *available at* https://epic.org/documents/reply-comment-in-cybersecurity-labeling-for-internet-of-things-fnprm/ (noting that devices in an intended victim's home, vehicle, or on their person may be used to attempt to surveil, control, or re-victimize them) (internal citations omitted); Comment of EPIC and Public Knowledge to Fed. Commc'ns Comm'n, *In re: Supporting Survivors of Domestic and Sexual Violence* Further Notice of Proposed Rulemaking (FNPRM), WC Dkt. No. 22-238 (May 23, 2024), *available at* https://epic.org/documents/in-re-supporting-survivors-of-domestic-and-sexual-violence-fnprm/ (citing Kaspersky survey in which 87% of participants indicated automakers should delete user data upon request, and 71% indicated considering buying an older car or one with less tech to protect their privacy and security but noting that "connected cars make up a growing share of the available inventory"). The Internet of Things Advisory Board has emphasized the importance of privacy-specific disclosures, noting that exposure of location data in particular can put certain populations at elevated risk. *See* IoTAB Committee, *Meeting Minutes, May 16 & 17, 2023*, at 23-24 (May 17, 2023), *available at* https://www.nist.gov/system/files/documents/2023/07/14/May_2023_IoTAB_ Day_1_and_2_Minutes_2023-06-27_v4%20Final.pdf.

[30] *See, e.g.*, Aarti Shahani, *Smartphones Are Used to Stalk, Control Domestic Abuse Victims*, NPR (Sept. 15, 2014), https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims (noting 85% shelters surveyed worked directly with victims tracked by GPS, 75% worked with victims whose conversations were surveilled remotely using hidden mobile apps). Dual-use apps also pose enhanced risk to survivors, and often tech clinics cannot readily support survivors with them absent further regulatory action. *See, e.g.*, Reply Comment of EPIC et al. to Fed. Commc'ns Comm'n at 5-8, *In re Lifeline and Link Up Reform and Modernization, Affordable Connectivity Program,* Supporting Survivors of Domestic *and Sexual Violence*, WC Dkt. Nos. 11-42, 21-450, 22-238 (May 12, 2023)*, available at* https://epic.org/documents/reply-comments-in-re-supporting-survivors-of-domestic-and-sexual-violence-nprm/#a-the-commission-should-investigate-family-tracker-apps-and-similar-apps.

[31] *See, e.g.*, *What is stalkerware?*, Kaspersky, https://www.kaspersky.com/resource-center/definitions/what-is-stalkerware (last visited Aug. 18, 2025) (citing 2023 report revealing tens of thousands of mobile users worldwide subject to stalkerware, noting that "the number of new people being targeted by this form of digital stalking has remained fairly constant on a monthly and annual basis now since 2021, suggesting that the issue isn't going away anytime soon"); *Stalkerware*, Malwarebytes, https://www.malwarebytes.com/stalkerware (last visited Aug. 18, 2025) (noting 565% increase in stalkerware-type app detections in 2020).

[32] *See, e.g.*, *FTC Brings First Case Against Developers of "Stalking" Apps*, Fed. Trade Comm'n (Oct. 22, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps; *Stalkerware: What To Know*, FTC Consumer Advice, https://consumer.ftc.gov/articles/stalkerware-what-know (Nov. 2023).

Commission,[33] Congress,[34] and the New York State Attorney General.[35] Consumer advocates likewise raise the alarm over such unfair and deceptive abuse and exploitation.[36] This Commission should continue be a leader in this regard.

The FTC should not reverse course on this important issue—a move that would jeopardize the personal safety of vulnerable Americans—on the word of one executive complaining about the comparatively mild consequences of his own actions.

b. The risk of sensitive data from sources like stalkerware being breached demands enhanced safeguards.

Any data breach can result in consumer harms, even absent any downstream consequences.[37] However, where especially sensitive data, such as private communications and continuous location data, is collected surreptitiously, these risks are amplified, meriting greater precautions to prevent such a breach.

In this instance, consumers weren't even aware that data was being collected about them and so had no way of preventing that data from being exposed when SpyFone's patently deficient security practices resulted in a data breach. This type of breach—data that the consumer didn't even know had

---

[33] *See, e.g.*, Fed. Commc'ns Comm'n, Further Notice of Proposed Rulemaking, *in re: Supporting Survivors of Domestic and Sexual Violence*, WC Docket No. 22-238, FCC 24-38, https://www.fcc.gov/document/fcc-proposes-rules-protect-survivors-using-connected-cars.

[34] *See, e.g.*, Safe Connections Act of 2022, H.R. 7132, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/7132/text, implemented by the FCC. *See, e.g.*, *in re Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform Modernization, Affordable Connectivity Program*, Report and Order, WC Dkt. Nos. 22-238, 11-42, 21-450 at ¶ 4 (Rel. Nov. 16, 2023), https://www.fcc.gov/document/fcc-approves-rules-safeguard-domestic-violence-survivors-0 (quoting Congress's findings in the Safe Connections Act §§ 3(3), 3(4), including that "perpetrators of violence and abuse . . . increasingly use technological and communications tools to exercise control over, monitor, and abuse their victims," and that "[c]ommunications law can play a public interest role in the promotion of safety, life, and property.").

[35] *See* New York State Attorney General, *supra* note 19 (noting stalkerware puts New Yorkers at risk of stalking and domestic abuse, emphasizing monitoring users without their awareness).

[36] *See, e.g.*, Order on Motion to Dismiss, *Hughes et al v. Apple, Inc*, *supra* note 23 at 696 ("From the beginning, it was obvious that the AirTag would be an especially useful tool for stalkers."). *But see* Order on Motion to Dismiss*, Hughes et al v. Apple, Inc*, N.D. Cal. 3:22-cv-07668-VC Dkt. 74 at 4 n 3 (Mar. 15, 2024) (noting that state consumer protection law likely would not afford stalked victims statutory standing as they were not a "consumer" in the AirTag transaction); *see also* Order on Motion to Dismiss, *Ireland-Gordy et al v. Tile, Inc. et al*, N.D. Cal. 3:23-cv-04119-RFL Dkt. 105 at 3 (Aug. 6, 2025) (acknowledging that while such facts were not adequately alleged in that case, there may certainly be circumstances that raise an inference of ongoing stalking to trigger the continuing violation doctrine).

[37] *See, e.g.*, Danielle Keats Citron and Daniel J. Solove, *Privacy Harms* 102 B.U. L. Rev. 793 (2022) [hereinafter "Privacy Harms"]; Jessica Guynn, *Anxiety, Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes*, USA Today (Feb. 24, 2020), https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips- mental-health-toll-depression-anxiety/4763823002/; Eleanor Dallaway, *#ISC2Congress: Cybercrime Victims Left Depressed and Traumatized*, Info. Sec. (Sep. 12, 2016), https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/.

been collected about them—exacerbates the harm that breaches cause to consumer autonomy,[38] as the consumer has lost control over how information about them is being collected and used. Moreover, this case implicated particularly sensitive datasets. The breached SpyFone data included records of thousands of consumers collected from their mobile devices, including photos.[39]

In encouraging companies to implement data security practices commensurate with the size and sensitivity of their datasets,[40] the Commission should raise the bar, rather than lower it. SpyFone and Mr. Zuckerman presided over a company that recklessly collected highly sensitive data without the knowledge of the device owner, failed to secure that data, and then mislead investigators after the fact of the breach. These three facts together make it abundantly clear that the FTC must strengthen its data security recommendations to ensure that industry standards move in the right direction. This is true in the case of SpyFone and Mr. Zuckerman, and would be true in any other case in which sensitive information is collected or in which any consumer information is collected surreptitiously. [41]

III. The FTC should not abandon its congressional mandate to protect the privacy and security of consumers.

Companies that collect and retain data about consumers have a responsibility to secure that data and to restrict their use of it to what is lawful, responsible, and consistent with the expectations of consumers. The Commission's record of data security and privacy enforcement reflects these fundamental tenets of data protection. Granting the relief Mr. Zuckerman seeks would upend that record and do irreparable harm to the FTC's mission.

Companies that choose to collect and retain data about consumers have a responsibility to safeguard that data. If they cannot protect it, they should not collect it.[42] The Commission has been exceedingly consistent when it comes to addressing cybersecurity issues, developing a reliable corpus for reference on these matters through its case-by-case enforcement actions. The FTC has taken on a great many cybersecurity cases, which together establish poor data security as a deceptive[43] and

---

[38] *See, e.g.*, *Privacy Harms*, *supra* note 37, at 845-55.
[39] *See* SpyFone Complaint, *supra* note 15, at ¶ 18.
[40] Disrupting Data Abuse, *supra* note 6, at 206 (citing to William McGeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1179 (2018)).
[41] While this applies more broadly than stalkerware, even just within the realm of stalkerware the FTC should consider actions against other, similar vendors. *See, e.g.*, Pieter Arntz, *Millions of stalkerware users exposed again*, MalwarebytesLabs (Feb. 28, 2025), https://www.malwarebytes.com/blog/news/2025/02/millions-of-stalkerware-users-exposed-again; Zach Whittaker, *A massive 'stalkerware' leak puts the phone data of thousands at risk*, TechCrunch (Oct. 19, 2021), https://techcrunch.com/2021/10/19/stalkerware-security-phone-data-thousands/; Shannon Vavra, *Stalkers using surveillance software on partners are exposing their own data, research finds*, CyberScoop (May 18, 2021), https://cyberscoop.com/stalkerware-app-spying-abuse-eset/ (not only intended victims but also would-be perpetrators can be at risk in stalkerware data breaches).
[42] John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too*, EPIC (June 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/ ("The relationship between data security and data minimization is perhaps best summarized by the maxim 'You don't have to protect what you don't collect.'")
[43] Disrupting Data Abuse, *supra* note 6, at 194.

unfair[44] trade practice. The remedies for the deficiencies outlined in these enforcement actions are very similar to requirements established across multiple cybersecurity regulations.[45] Companies have ample information to build cost-effective cybersecurity programs that protect consumers.[46]

Companies that choose to collect and retain data about consumers also have a responsibility to use that data responsibly.[47] Secret, unaccountable processing of personal data offers no plausible benefit to consumers or competition[48]—one reason why products or services that allow one person's purchases to surreptitiously surveil another person are so legally and ethically suspect.[49]

Mr. Zuckerman should not be granted a retroactive exemption from these industry-wide tenets of data security and privacy, which would undercut the FTC's important work as the nation's primary data protection regulator.

IV. The SpyFone case may have criminal implications.

To underscore the gravity of the conduct for which Mr. Zuckerman now seeks an administrative reprieve, we note that the Commission could well have chosen to refer this matter to the Department of Justice for criminal investigation. As Commissioner Chopra noted in September 2021:

> While this action was worthwhile, I am concerned that the FTC will be unable to meaningfully crack down on the underworld of stalking apps using our civil enforcement authorities. I hope that federal and state enforcers examine the applicability of criminal laws, including the Computer Fraud and Abuse Act, the Wiretap Act, and other criminal laws, to combat illegal surveillance, including the use of stalkerware.

---

[44] *Id*. at 191.
[45] *Id*. at 194-197; *see also* Comments of EPIC to the Office of the National Cyber Director at Appendix 1, *In re Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations (RFI)*, ONCD-2023-0001 (Oct. 2023), *https://epic.org/documents/in-re-opportunities-for-and-obstacles-to-harmonizing-cybersecurity-regulations-rfi/*.
[46] *See, e.g.*, FINRA, *Report on Cybersecurity Practices* (Feb 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf; Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; CISA, *Cross-Sector Cybersecurity Performance Goals* (2022), https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf.
[47] Disrupting Data Abuse, *supra* note 6, at 153 ("companies that exercise control over our personal data must demonstrate that they have carefully evaluated the risks of the processing they undertake and that such processing is justified in light of those risks. An individual must also have a straightforward mechanism to learn what personal data a company collects and retains from them, which in turn enables the consumer to demand its correction or deletion.")
[48] *Id.*
[49] Indeed, this may be why no "consumer" could have complained to Zuckerman about SpyFone, as the consumers of Zuckerman's offerings were the stalkers, not the stalked.

> While certain applications of these laws have been concerning, I believe it would be appropriate for enforcers to use these laws to seek criminal sanctions against individuals and firms that facilitate human endangerment through surveillance and stalkerware.[50]

For example, under 18 U.S.C. § 2512, it is a crime to intentionally distribute or advertise devices that are "primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications."[51]

In any event, the Commission should reject Mr. Zuckerman's invitation to eliminate the reasonable curative measures he agreed to in the SpyFone Consent Decree. Where, as here, an individual is responsible for masterminding the creation and distribution of a product used for surreptitious interception of communications, that individual bears personal responsibility and should not be excused merely because their corporate entity was held to account.[52]

V. Conclusion

EPIC, Public Knowledge, CDT, DPEF, Fairplay, and Free Press urge the Commission to reject the SpyFone Petition in its entirety. To do otherwise would send a dreadful signal about this Commission's commitment to the privacy and security of consumers and give a green light to purveyors of stalkerware to continue marketing products and services that facilitate domestic abuse. If there are any questions, please contact Chris Frascella at frascella@epic.org.

/s/ *John Davisson*
EPIC Director of Litigation &
Senior Counsel

/s/ *Chris Frascella*
EPIC Counsel

/s/ *Maria Villegas Bravo*
EPIC Law Fellow

---

[50] Statement of Comm'r Rohit Chopra, *supra* note 12, at 2 (internal citations omitted).
[51] 18 U.S.C. § 2512. We note that the statute of limitations is likely five years, assuming no tolling. *See* "Length of Limitations Period", Criminal Resource Manual, U.S. Dep't of Justice Archives, https://www.justice.gov/archives/jm/criminal-resource-manual-650-length-limitations-period (last visited Aug. 18, 2025).
[52] Notably in this instance, there was no financial penalty to SpyFone apart from the compliance costs which Mr. Zuckerman has provided estimates for in his petition.