COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

In the Matter of Support King, LLC (SpyFone.com)

FTC File No. 192 3003

October 8, 2021

By notice published on September 8, 2021, the Federal Trade Commission ("FTC") has proposed a Consent Order against Support King, LLC, formerly d/b/a SpyFone.com ("SpyFone") and its CEO Scott Zuckerman ("Zuckerman") that would settle alleged violations of federal law.[1] The FTC's Agreement Containing Consent Order[2] ("Consent Order") follows the FTC's Complaint ("Complaint"), which alleges that SpyFone, in coordination with Zuckerman, violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).[3]

The Electronic Privacy Information Center ("EPIC") submits these comments in support of the proposed Consent Order. EPIC is a public interest research center in Washington, D.C. established in 1994 to focus on public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in data protection and has played a leading role in developing the authority of the FTC to address

---

[1] Support King, LLC (SpyFone.com); Analysis of Proposed Consent Order To Aid Public Comment, 86 Fed. Reg. 50,357 (Sept. 8, 2021), https://www.federalregister.gov/documents/2021/09/08/2021-19388/support-king-llc-spyfonecom-analysis-of-proposed-consent-order-to-aid-public-comment [hereinafter Federal Register Notice].
[2] Agreement Containing Consent Order, *In the Matter of Support King, LLC (SpyFone.com) and Scott Zuckerman*, FTC File No. 192 2003 (Sept. 1, 2021), https://www.ftc.gov/system/files/documents/cases/192_3003_spyfone_agreement_and_order_without_signatures_0.pdf.
[3] Complaint, *In re Support King, LLC (SpyFone.com) and Scott Zuckerman*, FTC File No. 192 2003, (Aug. 26, 2021), https://www.ftc.gov/system/files/documents/cases/192_3003_spyfone_complaint.pdf [hereinafter Complaint].

emerging privacy issues and to safeguard the privacy rights of consumers.[4] EPIC routinely files comments in response to proposed FTC consent orders and complaints concerning business practices that violate privacy rights.[5]

EPIC's comments are divided into three sections. Section I summarizes the FTC Complaint against SpyFone. Section II commends the FTC for the proposed Consent Order and urges that it finalize the Order as is. Section III encourages the FTC to employ its authority similarly in the future to deter abusive data practices and to protect consumer privacy.

I. The FTC Complaint and Consent Order lay out deeply disturbing and unlawful data practices by SpyFone and Zuckerman.

The FTC Complaint details numerous unfair and deceptive practices engaged in by SpyFone and its CEO Scott Zuckerman, including covert surveillance of device owners and abuses of personal data.[6] SpyFone and Zuckerman licensed, marketed, and sold various surveillance products and services, "each of which allow[ed] a purchaser to monitor surreptitiously another person's activities on that person's mobile device (the 'device user')."[7] SpyFone's products were primarily marketed as tools to monitor children or employees for

[4] *See* EPIC, *What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities* (June 2021), https://epic.org/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf.
[5] *See, e.g.*, Comments of EPIC et al., *In re Zoom Video Communications, Inc*. (Dec. 14, 2020), https://epic.org/apa/comments/EPIC-FTC-Zoom-Dec2020.pdf; Complaint of EPIC, *In re Online Test Proctoring Companies* (Dec. 9, 2020), https://epic.org/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf; Complaint of EPIC, *In re Airbnb* (Feb. 26, 2020), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf; Petition of EPIC, *In re Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce* (Feb. 3, 2020), https://epic.org/privacy/ftc/ai/epic-ai-rulemaking-petition/; Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf; Comments of EPIC, *In re Unrollme, Inc*., FTC File No. 172-3139 (Sep. 19, 2019), https://epic.org/apa/comments/EPIC-FTC-Unrollme-Sept2019.pdf; Comments of EPIC, *In re Aleksandr Kogan and Alexander Nix*, FTC File Nos. 182-3106 & 182-3107 (Sep. 3, 2019), https://epic.org/apa/comments/EPIC-FTC-CambridgeAnalytica-Sept2019.pdf; EPIC, Comments on Standards for Safeguarding Customer Information (Aug. 1, 2019), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf; Complaint of EPIC, *In re Zoom Video Commc'ns, Inc*. (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf.
[6] Complaint, *supra* note 3.
[7] *Id*. at 2.

Android devices.[8] SpyFone customers were able to install the company's software on devices they could physically access.[9]

Notably, "purchasers of SpyFone Android products that require installation [were required to] take steps to bypass numerous restrictions implemented by the operating system or the mobile device manufacturer on the monitored mobile device."[10] Purchasers could enable certain capabilities of SpyFone products after gaining administrative privileges to the device, which "exposes a mobile device to various security vulnerabilities, and can invalidate warranties that a mobile device manufacturer or carrier provides."[11] SpyFone did not appear as an application on the user's device, and SpyFone provided purchasers with instructions to hide the product to prevent detection.[12] After installation, the purchaser did not need to have physical access to the user's device and could conduct remote monitoring. SpyFone did nothing to regulate the purposes for which its customers could use SpyFone products.[13]

SpyFone's products collected personal information including photos, text messages, web histories, and GPS locations.[14] SpyFone's terms of use stated that it would "take all reasonable precautions to safeguard customer information" and that "Spyfone uses its database to store your encrypted personal information."[15] Despite these claims, SpyFone and Zuckerman failed to implement reasonable security measures for the data it collected, failed to address security vulnerabilities, and failed to encrypt personal information.[16] In August 2018, a hacker infiltrated SpyFone's server and gained access to approximately 2,200 users' personal information. In

[8] *Id*. at 2–3.
[9] *Id*. at 3.
[10] *Id*. at 3.
[11] *Id*. at 3.
[12] *Id*. at 3.
[13] *Id*. at 3–4.
[14] *Id*. at 4.
[15] *Id*. at 4.
[16] *Id*. at 4–5.

response, SpyFone and Zuckerman told purchasers that they had "partner[ed] with leading data security firms to assist in our investigation" and that they would "coordinate with law enforcement authorities[.]" In reality, SpyFone and Zuckerman did not partner with any data security firms and did not coordinate with law enforcement regarding the breach.

The Complaint identifies several substantial injuries resulting from SpyFone and Zuckerman's practices. SpyFone's products allowed stalkers and abusers to surreptitiously monitor victims' personal information, physical movements, and online activities, which can in turn "cause mental and emotional abuse, financial and social harm, and physical harm, including death."[17] SpyFone's surveillance products also injured device users by weakening their device security—a risk "compounded by the fact that, in most circumstances, the device user [was] unaware that security features [had] been compromised, and thus [did] not know that he or she should implement heightened safeguards to protect the security of his or her mobile device."[18]

The Complaint lays out three counts arising from SpyFone and Zuckerman's unfair and deceptive business practices. Count I concerns the unfair sale and deployment of surreptitious monitoring tools that device users could not reasonably avoid.[19] Count II concerns SpyFone's data security misrepresentations.[20] Count III concerns SpyFone's data breach response misrepresentations.[21]

[17] *Id*. at 5.
[18] *Id*. at 6.
[19] *Id*. at 6.
[20] *Id*. at 6.
[21] *Id*. at 7.

II. The FTC should finalize the Consent Order, which requires notification, deletion of illegally collected data, and a ban on surveillance activities.

To settle the allegations in the FTC's Complaint, SpyFone and Zuckerman agreed to an FTC consent order (subject to final approval) on September 8, 2021.[22] Part I requires that SpyFone immediately end the collection of data through any monitoring software and disable all access to information collected through a monitored user device.[23] Part II requires that SpyFone and Zuckerman delete all consumer data collected within 30 days of the entry of the proposed order.[24] Part III requires that SpyFone and Zuckerman provide notice to all purchasers and device users that SpyFone collected information from the user's phone and that the phone may not be secure.[25] Part IV bans SpyFone and Zuckerman "from licensing, advertising, marketing, promoting, distributing, selling, or assisting in any of the former, any monitoring product or service to consumers."[26] Part V prohibits SpyFone and Zuckerman "from making any misrepresentations about the extent to which Respondents work with privacy or security firms, or the extent to which Respondents maintain and protect the privacy, security, confidentiality, and integrity of personal information."[27] Part VI prohibits SpyFone from transferring, selling, collecting, maintaining, or storing personal information until it implements and maintains a comprehensive data security program.[28] Part VII requires SpyFone and Zuckerman to submit to data security assessments for twenty years.[29] Part VIII prohibits SpyFone and Zuckerman from misrepresenting any material fact to the assessments and requires them to disclose all material facts to the assessor. Part IX requires that SpyFone and Zuckerman certify annually that they

[22] Federal Register Notice, *supra* note 1.
[23] Federal Register Notice, *supra* note 1, at 3.
[24] *Id*.
[25] *Id*.
[26] *Id*.
[27] *Id*.
[28] *Id*.
[29] *Id*.

have implemented and complied with the requirements of the Proposed Order.[30] Part X requires SpyFone and Zuckerman to report to the FTC following the discovery of any covered incident.[31] Parts XI through XIV explain SpyFone and Zuckerman's reporting and compliance obligations, including recordkeeping provisions and requirements to provide information to the FTC to monitor compliance.[32]

EPIC urges the Commission approve and finalize the Proposed Order as is. This is the first stalkerware case in which the FTC has secured a ban against participating in the surveillance business.[33] This ban, along with the Proposed Order's requirements to delete any illegally collected information and to notify affected device owners, are crucial measures to end and remediate SpyFone's abusive data practices. SpyFone's business model "made it easy for stalkers and abusers to monitor their potential targets and steal sensitive information about their physical movements, phone use, and online activities."[34] Given the severity of SpyFone's misconduct and the injuries suffered by affected device users, the remedies imposed by the Commission are necessary and appropriate.

III. The FTC should make fuller use of its statutory authority to prevent data abuse in the future, including bans.

In addition to approving the proposed Consent Order against SpyFone, EPIC urges the Commission to employ similar bans in future data protection enforcement actions. The FTC must require meaningful changes to a company's business practices—up to and including permanent exclusion from a particular line of business—when a company violates privacy rights and injures

[30] *Id*.
[31] *Id*.
[32] *Id*.
[33] Press Release, Fed. Trade Comm'n, FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data (Sept. 1, 2021), https://www.ftc.gov/news-events/press-releases/2021/09/ftc-bans-spyfone-and-ceo-from-surveillance-business.
[34] *Id*.

consumers. As evidenced by the proposed settlement, the FTC has the authority to enact permanent bans in particularly serious cases. The Commission should use this authority more frequently.

Further, as Commissioner Chopra noted in a separate statement,[35] the FTC's proposed settlement does not release Zuckerman or Support King, LLC of any potential criminal liability. Commissioner Chopra encouraged federal and state law enforcement agencies to "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."[36] EPIC supports this statement and urges the FTC to improve coordination with other agencies in the future to protect consumers from privacy harms.[37]

IV. Conclusion

EPIC urges the Commission to finalize the Proposed Order as is and encourages the FTC to make greater of its authority in the future—including bans—to fulfill its mandate to protect consumers from data abuse.

Sincerely,

/s/ John Davisson
EPIC Senior Counsel

/s/ Sara Geoghegan
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW

[35] Statement of Commissioner Rohit Chopra, *In the Matter of SpyFone*, FTC File No. 192 2003 (Sept. 1, 2021), https://www.ftc.gov/system/files/documents/public_statements/1595161/updated_date_final_chopra_statement_on_spyfone_.pdf.
[36] *Id*.
[37] *See* EPIC, *supra* note 4, at 19.

Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)