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

Office of Commissioner
Rohit Chopra

STATEMENT OF COMMISSIONER ROHIT CHOPRA

In the Matter of SpyFone
Commission File No. 1923003
September 1, 2021

Today, the Commission has proposed banning Support King, the operator of SpyFone, and its top executive, Scott Zuckerman, from marketing surveillance software to address severe misconduct related to their spying software scheme.

As alleged in the Commission's complaint, Support King licensed and marketed products where stalkers[1] and other users were given instructions on how to install an app on another person's mobile device, allowing users to have unfettered access to their target's location, text messages, and more. The company also employed shoddy security protocols that led to unauthorized access of sensitive personal records. To top it off, the company lied to its users about how it was handling the intrusion.

Surveillance Ban

The Commission is seeking public comment on banning Support King and Scott Zuckerman from licensing, marketing, or offering for sale surveillance products. This is a significant change from the agency's past approach. For example, in a 2019 stalkerware settlement, the Commission allowed the violators to continue developing and marketing monitoring products.[2]

In addition to the surveillance ban, affected individuals will receive notifications that someone may have been surreptitiously monitoring their mobile device, as well as information to seek help if they may be in danger.[3] The Commission welcomes public comment on these provisions.

[1] *See* Press Release, Electronic Frontier Foundation, Watch EFF Cybersecurity Director Eva Galperin's TED Talk about Stalkerware (May 28, 2020) https://www.eff.org/deeplinks/2020/05/watch-eff-cybersecurity-director-eva-galperins-ted-talk-about-stalkerware.

[2] The Commission's settlement in Retina-X Studios allowed the bad actors to continue to develop and market surveillance products, subject to certain requirements that the product would be used "legitimately." Press Release, Fed. Trade Comm'n, FTC Gives Final Approval to Settlement with Stalking Apps Developer (Mar. 27, 2020), https://www.ftc.gov/news-events/press-releases/2020/03/ftc-gives-final-approval-settlement-stalking-apps-developer. I reluctantly supported the resolution, despite my concerns about the leniency of the sanctions for illegal stalkerware behavior. The proposed ban in this matter will be easier to enforce, rather than making determinations about "legitimate" surveillance.

[3] Notice to affected individuals promotes greater accountability for bad actors and better functioning markets. Past Commissions routinely deprived these individuals of direct notice from bad actors, but we have changed course.

Criminal Law Enforcement

The FTC's proposed order in no way releases or absolves Support King or Scott Zuckerman of any potential criminal liability. 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.[4] 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.[5]

While certain applications of these laws have been concerning,[6] 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.

[4] Ideally, the Commission can also secure redress and damages for affected individuals in these matters. But monetary relief may not be sufficient to deter wrongdoing, given the structure of the market.

[5] The Computer Fraud and Abuse Act prohibits, among other things, "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" and obtaining information. 18 U.S.C. § 1030 (a)(2)(C). The Act also prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value . . . ." 18 U.S.C. § 1030 (a)(4).

[6] The indictment of Aaron Swartz for violations of the Computer Fraud and Abuse Act raised serious concerns about the application of the Act. *See e.g.* Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, WIRED (Oct. 26, 2015), https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/.