



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

June 5, 2015

The Honorable Al Franken
United States Senate
Washington, DC 20510

Dear Senator Franken:

Thank you for your letter regarding mSpy, a maker of spying software for computers and mobile devices. Your letter expresses concerns about the legality of the company's products and about a recent data breach that may have exposed sensitive information belonging to more than 400,000 individuals, including children and stalking victims. I share your concerns about surreptitious monitoring software and data breaches that result in unauthorized access to consumer location data or other personal information. Further, I appreciate your strong support for consumer privacy and data security generally and your continued efforts to strengthen federal protections for the privacy of consumers' location information.

The Federal Trade Commission is committed to using its civil law enforcement authority against companies that use spyware unlawfully and access or expose consumers' personal information. For example, in a series of settlements with national rent-to-own retailer Aarons and seven of its franchisees, we alleged the unlawful use of spyware to monitor consumers who had rented computers.¹ In particular, we alleged that the defendants used spyware installed on rented computers to capture screenshots of confidential and personal information, log computer keystrokes, track consumers' locations, and in some cases take webcam pictures of people in

¹ *Aaron's, Inc.*, No. C-4442 (F.T.C. Mar. 10, 2014) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3256/aarons-inc-matter>; *Aspen Way Enterprises, Inc.*, No. C-4392 (F.T.C. April 11, 2013) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/aspen-way-enterprises-inc-matter>; *Watershed Development Corp.*, No. C-4398 (F.T.C. April 11, 2013) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/watershed-development-corp-matter>; *Showplace, Inc.*, No. C-4397 (F.T.C. April 11, 2013) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/showplace-inc-matter>; *J.A.G. Rents, LLC*, No. C-4395 (F.T.C. April 11, 2013) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/jag-rents-llc-also-dba-colorzyme-matter>; *Red Zone Investment Group, Inc.*, No. C-4396 (F.T.C. April 11, 2013) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/red-zone-investment-group-inc-matter>; *B. Stamper Enterprises, Inc.*, No. C-4393 (F.T.C. April 11, 2013) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/b-stamper-enterprises-inc-matter>; *C.A.L.M. Ventures, Inc.*, No. C-4394 (F.T.C. April 11, 2013) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/calm-ventures-inc-matter>.

their homes, all without notice to, or consent from, affected consumers. We also alleged law violations by the software design firm that offered the spyware to these rental companies.² Among other things, these settlements bar the companies from further illegal spying and from activating location-tracking software without notice to, and consent from, computer renters. As you know, we also took action in an earlier suit against CyberSpy Software, LLC, and its owner,³ alleging they violated the law by advertising a keylogger software program as a “100% undetectable” way to “Spy on Anyone. From Anywhere.” Among other things, the final order in that case bars the defendants from providing purchasers with the means to disguise the product as an innocent file or e-mail attachment. The order also requires them to inform buyers that improper use of the software may violate the law and to take measures to reduce the risk that their product is misused.

In addition to our cases against companies that offer or use surreptitious spyware, we have highlighted the potential sensitivity of precise geolocation information,⁴ and we have taken action when companies unlawfully collect this information. Absent specific laws that protect geolocation information, the FTC has used its core consumer protection authority – Section 5 of the FTC Act⁵ – to target unfair or deceptive practices related to this information. For example, in our case against the developers of the mobile app Snapchat,⁶ we alleged, among other things, that the company had collected users’ geolocation information, contrary to its statements to consumers. In another case against a mobile app developer, we alleged that developers of a mobile flashlight app unlawfully collected user data – including precise geolocation information – and transmitted it to third-party ad networks, despite purporting to allow users to avoid the collection of such information.⁷ More recently, we settled charges that Nomi Technologies, a company whose technology allows retailers to track consumers’ movement through retail stores, misled consumers with promises that it would provide them with an in-store mechanism to opt out of tracking and that they would be informed when locations were using Nomi’s tracking services.⁸

The protection of consumers’ privacy is central to our mission. In addition to confronting illegal spyware and unlawful location tracking, we continue to focus our enforcement efforts on ensuring that consumers’ personal information – and the products that transmit such information

² *DesignerWare, LLC*, No. C-4390 (F.T.C. April 11, 2013) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter>.

³ See *FTC v. CyberSpy*, No. 6:08-cv-1872-ORL-31GLK (M.D. Fla. 2010) (stipulated final order), available at <http://www.ftc.gov/enforcement/cases-proceedings/082-3160/cyberspy-software-llc-trace-r-spence>.

⁴ See Federal Trade Commission, *Protecting Consumers in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), available at <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

⁵ 15 U.S.C. § 45(a). In addition, the Commission enforces the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. § 6501(8)(b), and its implementing rule, 16 C.F.R. Part 312, which includes “geolocation information” in the definition of “personal information” that child-directed websites and online services, as well as those with actual knowledge they are dealing with a child, may only collect with parental consent.

⁶ *Snapchat, Inc.*, No. C-4501 (Dec. 23, 2014) (consent order), available at <https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf>.

⁷ *Goldenshores Technologies, LLC*, No. C-4446 (F.T.C. Mar. 31, 2014) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter>.

⁸ *Nomi Technologies, Inc.*, No. 1323251 (F.T.C. April 23, 2015) (proposed consent order) available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter>.

– are secure. To date, we have settled 53 actions alleging that companies failed to maintain reasonable security to protect consumers’ personal information or to protect access to their personal, connected devices. We also have sought to educate consumers about location tracking technologies and spyware, and the steps they can take to detect and defend against malware.⁹

In determining whether to take enforcement or other action in any particular situation, the Commission may consider a number of factors, including the type of violation alleged; the nature and amount of consumer injury at issue and the number of consumers affected; and the likelihood of preventing future unlawful conduct and securing redress or other relief. I can assure you that the FTC staff will carefully consider the information you provided in determining whether enforcement or other action is appropriate.

Thank you again for sharing your concerns with us and for your support on issues relating to privacy and data security. If you or your staff has any additional questions or comments, please contact me or Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2946.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Edith Ramirez', is positioned above the printed name.

Edith Ramirez
Chairwoman

⁹ See, e.g., “Technology Tips for Domestic Violence and Stalking Victims,” FTC Consumer Article (Feb. 2015), available at <http://www.consumer.ftc.gov/blog/technology-tips-domestic-violence-and-stalking-victims>; “Understanding Mobile Apps,” FTC Consumer Article (Sept. 2011) (describing how mobile apps access personal information, including location data, and how privacy settings can affect such access), available at <http://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps>; see also “Malware,” FTC Consumer Article (Feb. 2014) (providing tips on detecting and defending against computer malware), available at <http://www.consumer.ftc.gov/articles/0011-malware>.