United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

May 19, 2015

The Honorable Loretta E. Lynch
Attorney General
Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Attorney General Lynch and Chairwoman Ramirez:

I am writing to draw your attention to recent reports concerning mSpy, a maker of spying software for computers and mobile devices. The company's product offering is deeply troubling, and a recent data breach may have exposed personal and sensitive information belonging to more than 400,000 individuals, including children and stalking victims. I urge your agencies to apply your respective authorities to examine the legality of mSpy and to hold those behind the product accountable for the sale of the software and for any mishandling of individuals' sensitive information.

I believe every American has a fundamental right to privacy, which includes the right to control whether and with whom personal, sensitive information—including location data—is being shared. In recent years we have seen a proliferation of so-called "stalking apps"—pieces of software that allow domestic abusers or stalkers to continuously and secretly spy on victims' electronic communications, movements, and whereabouts through their mobile devices. Such apps not only operate in clear violation of fundamental privacy principles, but the serious danger they pose is well-documented.[1]

In October 2011, I and eight of my colleagues on the Senate Judiciary Committee wrote to your agencies about the dangers of stalking apps. We asked your agencies to examine your existing authorities to investigate and prosecute developers and distributors of stalking apps.[2] Last year, the Justice Department successfully pursued Hammad Akbar, the CEO of the company that made the mobile app known as StealthGenie. Mr. Akbar pleaded guilty to advertising and selling spyware that amounted to illegal wiretapping equipment.

---

[1] *See, e.g.*, Aarti Shahani, *Smartphones Are Used To Stalk, Control Domestic Abuse Victims*, NPR (Sept. 15, 2014), http://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

[2] Letter to Attorney General Holder and Chair Liebowitz (Oct. 26, 2011), https://www.franken.senate.gov/?p=hot_topic&id=1815.

I hope the Justice Department will continue this important work and investigate whether other companies, such as mSpy, are likewise engaged in unlawful conduct. I hope you will also continue to lend your support as I work to ensure that our federal laws fully address the threat of stalking apps. I believe that there must be explicit laws to outlaw the development and sale of stalking apps. I have a bill—the Location Privacy Protection Act—that would finally put an end to these appalling apps that allow abusers to secretly track their victims, and would give consumers more control over their very sensitive location data. The time has come for Congress to enact these important protections.

mSpy describes itself as "monitoring software [that] runs invisibly on the target device to track all activity including call log history, GPS location, calendar updates, text messages, emails, web history, and much more!"[3] The company boasts that, when installed on a smartphone or other mobile device, "mSpy is inconspicuous and runs in a discreet operating mode," without notifying the user.[4] It records the device's location and activities, and uploads all of the data to an online account, where the purchaser of the software can review it. According to the company's website, that data may include real-time location information; photographs and videos on the device; incoming and outgoing text messages and emails; instant messages exchanged on Snapchat, Facebook, and other social networks; calendar activities and contacts; and browsing history and keystrokes. mSpy also enables certain remote controls of the target device—for example, allowing the software purchaser to block calls to the target device from predefined numbers.

In the hands of a stalker or abusive intimate partner, mSpy software is nothing short of terrifying. And the product—as well as its marketing, with its emphasis on the software's invisibility—seems carefully designed to appeal to such potential buyers. While the company acknowledges that there are legal prohibitions on surreptitious monitoring, the website expressly disavows any responsibility for informing device users that they are being monitored.[5] Instead, mSpy's website repeatedly assures its customers that the application is "discreet" and will operate without detection.[6]

On its Frequently Asked Questions (FAQ) page, mSpy's website acknowledges that individuals may wish to know how to detect the presence of mSpy on a device or how to uninstall the software. The website does not answer these questions, however, insisting that such information is confidential.[7] The website does make sure to explain that installation of the software can be completed quickly, requiring only a few minutes with the target device. Indeed, the website explains that in some cases, physical access to the target device is not even necessary to enable certain of mSpy's monitoring features.[8]

---

[3] mSpy, Features, http://www.mspy.com/features.html.
[4] mSpy, FAQ, Question # 5, http://www.mspy.com/faq.html.
[5] *Id.* at Questions #1, #2, #6.
[6] *Id.* at Questions #2, #5, #20; mSpy, Features, http://www.mspy.com/features.html.
[7] mSpy, FAQ, Question #22, http://www.mspy.com/faq.html.
[8] *Id.* at Questions #7, #8.

Unfortunately, my concerns about mSpy are not limited to questions about the current legality or illegality of its software. On May 15, security expert Brian Krebs reported that mSpy had suffered a massive data breach. According to Krebs, "a huge trove of data"—several hundred gigabytes worth of emails, text messages, photos, location tracking data, Apple IDs and passwords, and payment data—was "apparently stolen from the company's servers" and "posted on the Deep Web."[9] Krebs explained that a "message left by the unknown hackers who've claimed responsibility for this intrusion suggests that the data dump includes information on more than 400,000 [individuals]."[10]

Krebs has reported that mSpy recently claimed that approximately 40% of the company's subscribers are parents interested in monitoring their children.[11] If this is true, a significant portion of the sensitive information now exposed may pertain to minors, which is particularly worrisome. (And of course, mSpy's accounting still means that the majority of the company's subscribers are "discreetly" monitoring adults, which speaks to my concerns about surreptitious spying and stalking.) In any event, no matter whose information has been hacked, the reported breach raises serious questions about mSpy's data security practices. I urge the Federal Trade Commission to examine whether the company misled consumers by failing to maintain adequate security controls for sensitive personal information, or otherwise engaged in unfair or deceptive acts or practices in or affecting commerce.

According to press reports, mSpy has thus far declined to comment on the breach. The company must be held accountable, and, to this end, I hope that your agencies will use your existing authorities to the fullest extent possible. As the Ranking Member on the Senate Judiciary Committee's Subcommittee on Privacy, Technology, and the Law, I am keenly aware that Americans constantly face the threat of their personal information being hacked, as reportedly happened here. At this time, federal law does not establish explicit, applicable minimum requirements for commercial data security and breach notification. For this reason, I'm a co-sponsor of the Consumer Privacy Protection Act, a legislative proposal to require companies to protect consumers' personal information, defend against cyberattacks, and prevent data breaches ahead of time. That legislation would have required mSpy to inform the federal government and its customers about the breach soon after it happened, and would give your agencies stronger enforcement tools.

I believe that we need to take a comprehensive approach to protecting the sensitive information of consumers in Minnesota and all across the country. That means we need to update our laws to make sure that stalking apps cannot continue to operate in any form, and we need to make sure that we are doing everything possible to address the ever-increasing threat of data breaches. I will continue to press my colleagues in Congress to act, and I encourage your agencies to do everything in your power to protect the American people.

---

[9] Brian Krebs, *Mobile Spy Software Maker mSpy Hacked, Customer Data Leaked*, KrebsOnSecurity (May 15, 2015), https://krebsonsecurity.com/2015/05/mobile-spy-software-maker-mspy-hacked-customer-data-leaked/.
[10] *Id.*
[11] *Id.*

Thank you for your attention to this matter, and please do not hesitate to contact me, or Samantha Chaifetz on my staff, at (202) 224-5641.

Sincerely,

Al Franken
Ranking Member, Subcommittee on Privacy,
Technology, and the Law