United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Prepared Remarks of Commissioner Rebecca K. Slaughter
Retina-X Studios, LLC Press Call
October 22, 2019

Good afternoon. I am pleased to join this conference, because the case we are discussing represents an important milestone in the FTC's efforts to protect consumers. It is our first case against "stalkerware," apps that allow surreptitious monitoring of consumers. These apps are not just creepy, they can put victims of stalking and domestic violence at profound risk.

In 2014, a survey by National Public Radio of 72 domestic violence shelters in the US discovered that 85 percent had assisted victims whose abusers had tracked them through GPS. Cybersecurity company Kaspersky Labs recently reported that from January through August 2019, there were over 500,000 cases where their antivirus software detected either the presence of stalkerware on users' devices or detected an attempt to install it. Stalking apps like the ones offered by Retina-X can be extremely dangerous; today's action makes clear that they are also illegal.

Today's announcement sends three key messages. The first message is for businesses considering developing monitoring products: you have an additional responsibility to ensure your products are used legitimately; you cannot turn a blind eye and you certainly cannot tacitly wink at the use of your software to monitor adults without their consent. Require written certifications as to how the app will be used. Save those certifications in case law enforcement has questions. If you suspect someone wants to use your product for illegitimate purposes, don't sell the subscription. Do not rely on buried terms of service to tell people they can only use the app for specified purposes.

The second message is one for all businesses: you have an obligation to safeguard information you collect. When businesses collect intimate details about people's whereabouts, communications, and contacts, not only must they make sure that people understand exactly what is being collected and who has access to it—they must safeguard that information. These obligations are especially important when we are talking about personal information collected from children. Most of Retina-X's information security deficiencies were well known and, in fact, have been identified in our business guidance. For example, the company did not have written security standards in place, did not conduct security testing for known vulnerabilities, and failed to take appropriate steps to monitor its own service providers—including those that managed its servers, handled its payment processing, and provided marketing and customer support services.

But most critically, Retina-X almost certainly collected information about adults who had not consented to that collection and did not even know it was occurring, which brings me to our final message, for the public: stalking apps can pose serious dangers to consumers. It only takes an abuser a few minutes to install a stalking app on a victim's phone, and from an online dashboard, watch not only almost everything the victim does on the phone but also everywhere she goes in the world.

If you think someone might have installed a stalking app on your smartphone, we have put together resources for you at consumer.ftc.gov. We have a blogpost there that outlines steps you may take to check if your device has been compromised. For example, you can use a "Root checker" app to identify if your smartphone has been rooted or jailbroken, which might then signal that a stalking app has been installed on your phone. If your phone is rooted or jailbroken, or otherwise could be compromised, you might also consider whether to get a new smartphone with an account that the abuser does not have access to, or consider factory resetting your smartphone and reinstalling the manufacturer's operating system. An additional step could be to contact law enforcement and domestic violence advocates as resources to assist in identifying tech misuse and creating a safety plan. If you reach out to these resources, consider contacting them from a different device than the one that might have the stalking app.

I would also like to thank the National Network to End Domestic Violence for being such a comprehensive resource for domestic abuse survivors and an important partner to us at the Commission, as we strive to educate more consumers about the risks certain technologies can introduce to our daily lives, especially at the intersection of technology and intimate partner abuse. Now I will turn things over to Cindy Southworth and Erica Olsen of the NNEDV, who will share some examples of why products like those at the heart of today's settlement are so dangerous for victims of domestic violence and stalking, and provide more information and advice for consumers about resources that can help.