

United States Senate

WASHINGTON, DC 20510

February 7, 2019

Mr. Tim Cook
Chief Executive Officer
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014

Dear Mr. Cook:

We write concerned about reports that Facebook is collecting highly-sensitive data on teenagers, including their web browsing, phone use, communications, and locations – all to profile their behavior without adequate disclosure, consent, or oversight. These reports fit with longstanding concerns that Facebook has used its products to deeply intrude into personal privacy. Additionally, the scope of the research and the use of the Onavo Protect app raises questions about Facebook's use of personal data to engage in potentially anti-competitive behavior. As Apple is responsible for the App Store and the iOS operating systems, we request information on your policies regarding the monitoring of teens and Apple's response to the Facebook research program.

On January 29, 2019, TechCrunch reported that Facebook has run a paid research program named Project Atlas to profile consumers by monitoring their phone use. According to registration pages and advertisements run by Facebook's research partners, the program was available to individuals between the ages of 13 and 35, requiring parental consent for those younger than 18. Despite this constraint, the program appears to have specifically targeted teens, inadequately disclosed the scope of the data collection, and not properly verified parental consent. One advertisement for the program on Snapchat and Instagram found by TechCrunch shows a teen with hundred dollar bills falling from the sky, calling for "participants for a paid social media research study." According to a journalist who attempted to register as a teen, the linked registration page failed to impose meaningful checks on parental consent.¹ This recruitment and lax oversight of teen privacy flies in the face of a widespread understanding that young people require strong protections for their privacy and safety.

Facebook's monitoring under Project Atlas is particularly concerning because the data collection performed by the research app was deeply invasive. Once installed, the app added a VPN connection that would automatically route all of a participant's traffic through Facebook servers. The app also installed an SSL root certificate on the participant's phone, which would allow Facebook to intercept or modify data sent to encrypted websites. As a result, Facebook would have limitless access to monitor normally secure web traffic, even allowing Facebook to watch an individual log into their bank account or exchange pictures with their family. None of the disclosures provided at registration offer a meaningful explanation about how that sensitive

¹ Kelion, Leo. "Facebook Adviser Criticises 'lax' Child Checks." BBC News. January 31, 2019.
<https://www.bbc.com/news/technology-47071334>.

data is used, how long it is kept, or who has access to it. Facebook could have access to messages or images that teens and adults had sent believing they were private without any awareness or ability to control the use of this private information.

Lastly, Project Atlas is particularly concerning in light of Facebook's established history of using private information for potentially anti-competitive purposes. In order to monitor participants, Facebook used a version of its Onavo Protect app, a web security application that it acquired in 2013. Onavo Protect has its own history of privacy and competition concerns. According to BuzzFeed and the Wall Street Journal, Facebook has used web browsing data collected from Onavo Protect users to monitor rival products and identify emerging competitors to buy or copy. Privacy advocates have challenged that further analysis of this sensitive browsing data is not disclosed to users.² In August 2018, Apple banned Onavo Protect from the App Store for breaching its policies about transparency and limits on the data that apps are allowed to collect.

Faced with that ban, Facebook appears to have circumvented Apple's attempts to protect consumers. With Project Atlas, Facebook distributed the application to teens through an enterprise program offered by Apple meant only for Facebook's own employees. Apple has acknowledged that Facebook's use of the enterprise certificate program for installing apps on consumers' phones constituted a breach of its terms of service.

Platforms must be vigilant in light of threats to teen privacy posed by programs like Project Atlas. Facebook is not alone in engaging in commercial monitoring of teens. TechCrunch has subsequently reported that Google maintained its own measurement program called "Screenwise Meter," which raises similar concerns as Project Atlas. The Screenwise Meter app also bypassed the App Store using an enterprise certificate and installed a VPN service in order to monitor phones. Likewise, according to reports, Screenwise Meter was originally open to users as young as 13 years old, and continued to be available to the teenagers if they were registered as a part of a family group on Google Play. While Google has since removed the app, questions remain about why it had gone outside Apple's review process to run the monitoring program.³ Platforms must maintain and consistently enforce clear policies on the monitoring of teens and what constitutes meaningful parental consent, no matter who is providing an app.

Given the sensitivity and seriousness of any intrusions into the privacy of teens, we respectfully request a written response to the following questions by March 1, 2019:

1. Does the collection of browsing histories, communications content, or app usage from a user's device violate the App Store terms of service? Please explain. Why did Apple consider it important to update its terms of service in June 2018 to ban the collection of

² Comments of the Electronic Privacy Information Center, Center for Digital Democracy, Consumer Federation of America, and U.S. Public Interest Research Group to the Federal Trade Commission regarding Competition and Consumer Protection in the 21st Century Hearings. August 20, 2018. <https://epic.org/apa/comments/EPIC-FTC-CompetitionHearings-August2018.pdf>

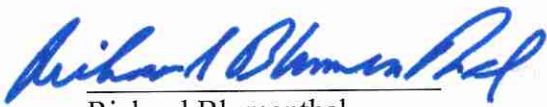
³ Whittaker, Zack, Josh Constine, and Ingrid Lunden. "Google Will Stop Peddling a Data Collector through Apple's Back Door." TechCrunch. January 30, 2019. <https://techcrunch.com/2019/01/30/googles-also-peddling-a-data-collector-through-apples-back-door/>.

data about other apps?

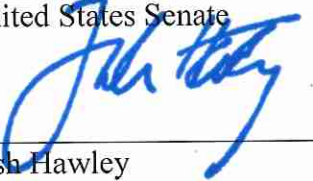
2. If Apple finds that an application has bypassed its app review process and is operating in a manner intrusive to user privacy, what remedies does it maintain to protect users, such as disabling or removing problematic apps? Will Apple pursue such any remedies with respect to the Project Atlas app?
3. When was the Project Atlas app made available to iPhone users and on how many devices was the app installed?
4. Does Apple plan to allow the Project Atlas app on its devices in the future?
5. How does Apple plan to address the Screenwise Monitor app's bypass of its app review process?
6. Has Apple conducted an assessment to determine whether Google and Facebook have bypassed the App Store approval processing using enterprise certificates for any other non-internal apps?
7. In light of recent invasions of children's and teens' privacy, including those described above, would Apple support federal legislation to create new privacy safeguards for children and teens online?

Thank you for your attention to these important issues. We look forward to your response.

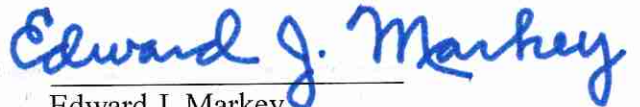
Sincerely,



Richard Blumenthal
United States Senate



Josh Hawley
United States Senate



Edward J. Markey
United States Senate