Facebook tricks teens into installing VPN that spies on them more than they realize

Josh Constine@joshconstine /

Desperate for data on its competitors, Facebook has been secretly paying people to install a "Facebook Research" VPN that lets the company suck in all of a user's phone and web activity, similar to Facebook's Onavo Protect app that Apple banned in June and that was removed in August. Facebook sidesteps the App Store and rewards teenagers and adults to download the Research app and give it root access to network traffic in what may be a violation of Apple policy so the social network can decrypt and analyze their phone activity, a TechCrunch investigation confirms.

Facebook admitted to TechCrunch it was running the Research program to gather data on usage habits, and it has no plans to stop.

Since 2016, Facebook has been paying users ages 13 to 35 up to $20 per month plus referral fees to sell their privacy by installing the iOS or Android "Facebook Research" app. Facebook even asked users to screenshot their Amazon order history page. The program is administered through beta testing services Applause, BetaBound and uTest to cloak Facebook's involvement, and is referred to in some documentation as "Project Atlas" — a fitting name for Facebook's effort to map new trends and rivals around the globe.

Facebook's Research app requires users to 'Trust' it with extensive access to their data

We asked Guardian Mobile Firewall's security expert Will Strafach to dig into the Facebook Research app, and he told us that "If Facebook makes full use of the level of access they are given by asking users to install the Certificate, they will have the ability to continuously collect the following types of data: private messages in social media apps, chats from in instant messaging apps – including photos/videos sent to others, emails, web searches, web browsing activity, and even ongoing location information by tapping into the feeds of any location tracking apps you may have installed." It's unclear exactly what data Facebook is concerned with, but it gets nearly limitless access to a user's device once they install the app.

The strategy shows how far Facebook is willing to go and how much it's willing to pay to protect its dominance — even at the risk of breaking the rules of Apple's iOS platform on which it depends. Apple could seek to block Facebook from continuing to distribute its Research app, or even revoke it permission to offer employee-only apps, and the situation could further chill relations between the tech giants. Apple's Tim Cook has repeatedly criticized Facebook's data collection practices. Facebook disobeying iOS policies to slurp up more information could become a new talking point. TechCrunch has spoken to Apple and it's aware of the issue, but the company did not provide a statement before press time.

Facebook's Research program is referred to as Project Atlas on sign-up sites that don't mention Facebook's involvement

"The fairly technical sounding 'install our Root Certificate' step is appalling," Strafach tells us. "This hands Facebook continuous access to the most sensitive data about you, and most users are going to be unable to reasonably consent to this regardless of any agreement they sign, because there is no good way to articulate just how much power is handed to Facebook when you do this."

Facebook's surveillance app

Facebook first got into the data-sniffing business when it acquired Onavo for around $120 million in 2014. The VPN app helped users track and minimize their mobile data plan usage, but also gave Facebook deep analytics about what other apps they were using. Internal documents acquired by Charlie Warzel and Ryan Mac of BuzzFeed News reveal that Facebook was able to leverage Onavo to learn that WhatsApp was sending more than twice as many messages per day as Facebook Messenger. Onavo allowed Facebook to spot WhatsApp's meteoric rise and justify paying $19 billion to buy the chat startup in 2014. WhatsApp has since tripled its user base, demonstrating the power of Onavo's foresight.

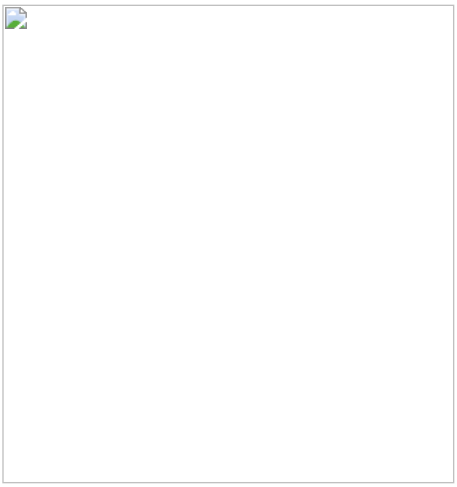
Over the years since, Onavo clued Facebook in to what apps to copy, features to build and flops to avoid. By 2018, Facebook was promoting the Onavo app in a Protect bookmark of the main Facebook app in hopes of scoring more users to snoop on. Facebook also launched the Onavo Bolt app that let you lock apps behind a passcode or fingerprint while it surveils you, but Facebook shut down the app the day it was discovered following privacy criticism. Onavo's main app remains available on Google Play and has been installed more than 10 million times.

The backlash heated up after security expert Strafach detailed in March how Onavo Protect was reporting to Facebook when a user's screen was on or off, and its Wi-Fi and cellular data usage in bytes even when the VPN was turned off. In June, Apple updated its developer policies to ban collecting data about usage of other apps or data that's not necessary for an app to function. Apple proceeded to inform Facebook in August that Onavo Protect violated those data collection policies and that the social network needed to remove it from the App Store, which it did, Deepa Seetharaman of the WSJ reported.

But that didn't stop Facebook's data collection.

Project Atlas

TechCrunch recently received a tip that despite Onavo Protect being banished by Apple, Facebook was paying users to sideload a similar VPN app under the Facebook Research moniker from outside of the App Store. We investigated, and learned Facebook was working with three app beta testing services to distribute the Facebook Research app: BetaBound, uTest and Applause. Facebook began distributing the Research VPN app in 2016. It has been referred to as Project Atlas since at least mid-2018, around when backlash to Onavo Protect magnified and Apple instituted its new rules that prohibited Onavo. Facebook didn't want to stop collecting data on people's phone usage and so the Research program continued, in disregard for Apple banning Onavo Protect.



Facebook's Research App on iOS

Ads (shown below) for the program run by uTest on Instagram and Snapchat sought teens 13-17 years old for a "paid social media research study." The sign-up page for the Facebook Research program administered by Applause doesn't mention Facebook, but seeks users "Age: 13-35 (parental consent required for ages 13-17)." If minors try to sign-up, they're asked to get their parents' permission with a form that reveal's Facebook's involvement and says "There are no known risks associated with the project, however you acknowledge that the inherent nature of the project involves the tracking of personal information via your child's use of apps. You will be compensated by Applause for your child's participation." For kids short on cash, the payments could coerce them to sell their privacy to Facebook.

The Applause site explains what data could be collected by the Facebook Research app (emphasis mine):

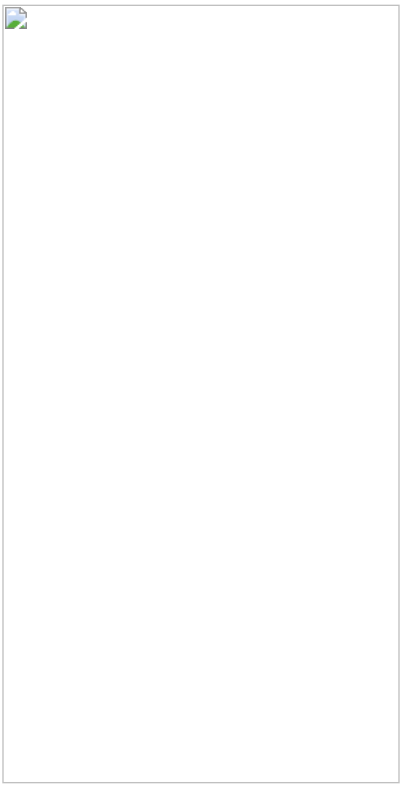
"By installing the software, you're giving our client permission to collect data from your phone that will help them understand how you browse the internet, and how you use the features in the apps you've installed . . . This means you're ***letting our client collect information such as which apps are on your phone, how and when you use them****, data about your activities and content within those apps, as well as how other people interact with you or your content within those apps. You are also* ***letting our client collect information about your internet browsing activity*** *(including the websites you visit and data*

that is exchanged between your device and those websites) and your use of other online services. There are some instances when ***our client will collect this information even where the app uses encryption****, or from within secure browser sessions."*

Meanwhile, the BetaBound sign-up page with a URL ending in "Atlas" explains that "For $20 per month (via e-gift cards), you will install an app on your phone and let it run in the background." It also offers $20 per friend you refer. That site also doesn't initially mention Facebook, but the instruction manual for installing Facebook Research reveals the company's involvement.

Facebook's intermediary uTest ran ads on Snapchat and Instagram, luring teens to the Research program with the promise of money

Facebook seems to have purposefully avoided TestFlight, Apple's official beta testing system, which requires apps to be reviewed by Apple and is limited to 10,000 participants. Instead, the instruction manual reveals that users download the app from r.facebook-program.com and are told to install an Enterprise Developer Certificate and VPN and "Trust" Facebook with root access to the data their phone transmits. Apple requires that developers agree to only use this certificate system for distributing internal corporate apps to their own employees. Randomly recruiting testers and paying them a monthly fee appears to violate the spirit of that rule.



Security expert Will Strafach found Facebook's Research app contains lots of code from Onavo Protect, the Facebook-owned app Apple banned last year

Once installed, users just had to keep the VPN running and sending data to Facebook to get paid. The Applause-administered program requested that users screenshot their Amazon orders page. This data could potentially help Facebook tie browsing habits and usage of other apps with purchase preferences and behavior. That information could be harnessed to pinpoint ad targeting and understand which types of users buy what.

TechCrunch commissioned Strafach to analyze the Facebook Research app and find out where it was sending data. He confirmed that data is routed to "vpn-sjc1.v.facebook-program.com" that is associated with Onavo's IP address, and that the facebook-program.com domain is registered to Facebook, according to MarkMonitor. The app can update itself without interacting with the App Store, and is linked to the email address PeopleJourney@fb.com. He also discovered that the

Enterprise Certificate indicates Facebook renewed it on June 27th, 2018 — weeks after Apple announced its new rules that prohibited the similar Onavo Protect app.

“It is tricky to know what data Facebook is actually saving (without access to their servers). The only information that is knowable here is what access Facebook is capable of based on the code in the app. And it paints a very worrisome picture,” Strafach explains. “They might respond and claim to only actually retain/save very specific limited data, and that could be true, it really boils down to how much you trust Facebook’s word on it. The most charitable narrative of this situation would be that Facebook did not think too hard about the level of access they were granting to themselves . . . which is a startling level of carelessness in itself if that is the case.”

“Flagrant defiance of Apple’s rules”

In response to TechCrunch’s inquiry, a Facebook spokesperson confirmed it’s running the program to learn how people use their phones and other services. The spokesperson told us “Like many companies, we invite people to participate in research that helps us identify things we can be doing better. Since this research is aimed at helping Facebook understand how people use their mobile devices, we’ve provided extensive information about the type of data we collect and how they can participate. We don’t share this information with others and people can stop participating at any time.”

Facebook’s Research app requires Root Certificate access, which Facebook gather almost any piece transmitted by your phone

Facebook’s spokesperson claimed that the Facebook Research app was in line with Apple’s Enterprise Certificate program, but didn’t explain how in the face of evidence to the contrary. They said Facebook first launched its Research app program in 2016. They tried to liken the program to a focus group and said Nielsen and comScore run similar programs, yet neither of those ask people to install a VPN or provide root access to the network. The spokesperson confirmed the Facebook Research program does recruit teens but also other age groups from around the world. They claimed that Onavo and Facebook Research are separate programs, but admitted the same team supports both as an explanation for why their code was so similar.

Facebook's Research program requested users screenshot their Amazon order history to provide it with purchase data

However, Facebook claim that it doesn't violate Apple's Enterprise Certificate policy is directly contradicted by the terms of that policy. Those include that developers "Distribute Provisioning Profiles only to Your Employees and only in conjunction with Your Internal Use Applications for the purpose of developing and testing". The policy also states that "You may not use, distribute or otherwise make Your Internal Use Applications available to Your Customers" unless under direct supervision of employees or on company premises. Given Facebook's customers are using the Enterprise Certificate-powered app without supervision, it appears Facebook is in violation.

Facebook disobeying Apple so directly could hurt their relationship. "The code in this iOS app strongly indicates that it is simply a poorly re-branded build of the banned Onavo app, now using an Enterprise Certificate owned by Facebook in direct violation of Apple's rules, allowing Facebook to distribute this app without Apple review to as many users as they want," Strafach tells us. ONV prefixes and mentions of graph.onavo.com, "onavoApp://" and "onavoProtect://" custom URL schemes litter the app. "This is an egregious violation on many fronts, and I hope that Apple will act expeditiously in revoking the signing certificate to render the app inoperable."

Facebook is particularly interested in what teens do on their phones as the demographic has increasingly abandoned the social network in favor of Snapchat, YouTube and Facebook's acquisition Instagram. Insights into how popular with teens is Chinese video music app TikTok and meme sharing led Facebook to launch a clone called Lasso and begin developing a meme-browsing feature called LOL, TechCrunch first reported. But Facebook's desire for data about teens riles critics at a time when the company has been battered in the press. Analysts on tomorrow's Facebook earnings call should inquire about what other ways the company has to collect competitive intelligence.

Last year when Tim Cook was asked what he'd do in Mark Zuckerberg's position in the wake of the Cambridge Analytica scandal, he said "I wouldn't be in this situation . . . The truth is we could make a ton of money if we monetized our customer, if our customer was our product. We've elected not to do that." Zuckerberg told Ezra Klein that he felt Cook's comment was "extremely glib."

Now it's clear that even after Apple's warnings and the removal of Onavo Protect, Facebook is still aggressively collecting data on its competitors via Apple's iOS platform. "I have never seen such open and flagrant defiance of Apple's rules by an App Store developer," Strafach concluded. If Apple shuts the Research program down, Facebook will either have to invent new ways to surveil our behavior amidst a climate of privacy scrutiny, or be left in the dark.

Additional reporting by Zack Whittaker.