

SIMON TAYLOR
777 South Flagler Drive
Suite 800 West Tower
West Palm Beach, Florida 33401
(561) 818-0170

November 7, 2019

Mayor and Town Council of Palm Beach
360 South County Road
Palm Beach, Florida 33480

Subject: Concerns about Parking and Mobile Phone Apps

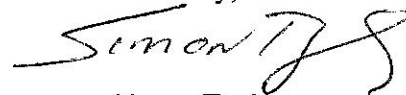
Honorable Mayor and Council Members:

It appears that proposals to install parking meters or kiosks in Palm Beach may be heard at the Town Council meeting on November 12. The Council voted at its August meeting to defer the matter to November after hearing objections from residents.

I understand the concerns voiced by resident Warren Belmar at the August meeting. In addition, I want to repeat comments I made to the Council at the time, focused on the inadvisability of limiting parking meters or kiosks to technology that can only be used with a mobile phone app. My concerns then and now include the obvious: Many people may not have, or may not choose to download, install and use, apps on their mobile phones for parking or other commercial purposes. Also of grave concern are the privacy and security risks that would come from forcing residents and others to install and use apps on their phones, including the danger and likelihood of the following: access through the phone to personal data, tracking of calls and other uses of the phone, mining and sale of data, targeting of unwanted ads, continual tracking of the locations of the user, hacking of the phone by bad actors and other harms and privacy and security violations. To provide just a few real world examples of these dangers, I am sending to you copies of an August 30, 2019 BBC News article describing the "enormous amounts of data" accessed in a hacking attack on iPhones and a May 28, 2019 Washington Post article detailing the numerous incursions and exploitations of mobile phones through mobile apps.

Individuals may choose to ignore the privacy, security and personal hazards of using mobile apps too readily, but the Town Council and Palm Beach should not force people to suffer those risks and harms by insisting that any paid parking will only be possible with mobile phone apps. If meters or kiosks are used in Town, they can allow payment with lesser risks using credit cards and payment with much less privacy and data security risk by permitting use of coins.

Sincerely,

A handwritten signature in black ink, appearing to read "Simon Taylor", with a stylized flourish at the end.

Simon Taylor

[Home](#) [News](#) [Sport](#) [Reel](#) [Worklife](#) [Travel](#) [Future](#)

IV

[Home](#) [Video](#) [World](#) [US & Canada](#) [UK](#) [Business](#) [Tech](#) [Science](#)

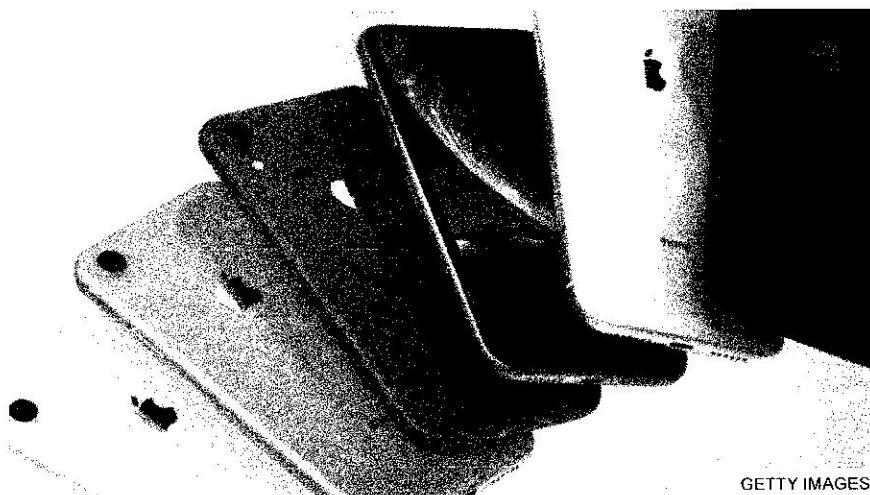
Technology

Google finds 'indiscriminate iPhone attack lasting years'

By Dave Lee

North America technology reporter

30 August 2019



Security researchers at Google have found evidence of a “sustained effort” to hack iPhones over a period of at least two years.

The attack was said to be carried out using websites which would discreetly implant malicious software to gather contacts, images and other data.

Google’s analysis suggested the booby-trapped websites were said to have been visited thousands of times per week.

Apple told the BBC it did not wish to comment.

The attack was shared in great detail in a series of technical posts written by British cybersecurity expert Ian Beer, a member of Project Zero, Google’s taskforce for finding new security vulnerabilities, known as zero days.

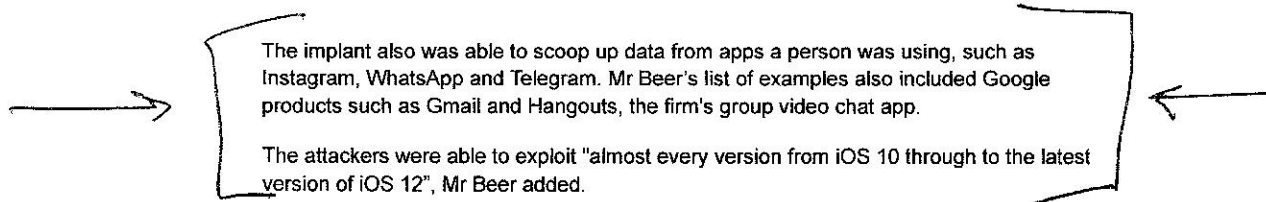
“There was no target discrimination,” Mr Beer wrote.

“Simply visiting the hacked site was enough for the exploit server to attack your device, and if it was successful, install a monitoring implant.”

Mr Beer and his team said they discovered attackers were using 12 separate security flaws in order to compromise devices. Most were bugs within Safari, the default web browser on Apple products.

'Sustained effort'

Once on a person’s iPhone, the implant could access an enormous amount of data, including (though not limited to) contacts, images and GPS location data. It would relay this information back to an external server every 60 seconds, Mr Beer noted.



"This indicated a group making a sustained effort to hack the users of iPhones in certain communities over a period of at least two years."

Are you protected?

Apple issued a software fix to address the flaw back in February.

If you are an iPhone user, you should make sure your device is running the latest version of iOS, to make sure you are protected.

To do this, go to Settings and tap General. Under 'Software Update' you should be running iOS 12.4.1.

If you are not running iOS 12.4.1 you will be given the opportunity to update your device.

Apple's fix

Google's team notified Apple of the vulnerabilities on 1 February this year. **A patch was subsequently released** six days later to close the vulnerability. Apple's patch notes refer to fixing an issue whereby "an application may be able to gain elevated privileges" and "an application may be able to execute arbitrary code with kernel privileges".

iPhone users should update their device to the latest software to make sure they are adequately protected.

Unlike some security disclosures, which offer merely theoretical uses of vulnerabilities, Google discovered this attack "in the wild" - in other words, it was in use by cybercriminals.

Mr Beer's analysis did not speculate on who may be behind the attack, nor how lucrative the tool may have been on the black market. Some "zero day" attacks can be sold for several millions dollars - until they're discovered and fixed.

Follow Dave Lee on Twitter @DaveLeeBBC

Do you have more information about this or any other technology story? You can reach Dave directly and securely through encrypted messaging app Signal on: +1 (628) 400-7370

Related Topics

[iPhones](#) [Google](#) [Apple](#) [Computer hacking](#)

Share this story About sharing

More on this story

Apple Watch bug allowed iPhone eavesdropping

11 July 2019

It's the middle of the night. Do you know who your iPhone is talking to?

Apple says, "What happens on your iPhone stays on your iPhone." Our privacy experiment showed 5,400 hidden app trackers guzzled our data — in a single week.

While you're sleeping, your iPhone stays busy. (Washington Post Illustration; iStock/The Washington Post)



By
Geoffrey A. Fowler
Technology columnist
May 28, 2019 at 8:00 a.m. EDT

It's 3 a.m. Do you know what your iPhone is doing?

Mine has been alarmingly busy. Even though the screen is off and I'm snoring, apps are beaming out lots of information about me to companies I've never heard of. Your iPhone probably is doing the same — and Apple could be doing more to stop it.

On a recent Monday night, a dozen marketing companies, research firms and other personal data guzzlers got reports from my iPhone. At 11:43 p.m., a company called Amplitude learned my phone number, email and exact location. At 3:58 a.m., another called Appboy got a digital fingerprint of my phone. At 6:25 a.m., a tracker called Demdex received a way to identify my phone and sent back a list of other trackers to pair up with.

And all night long, there was some startling behavior by a household name: Yelp. It was receiving a message that included my IP address — once every five minutes.

AD

What you can do to limit app tracking: 5 privacy tips

Our data has a secret life in many of the devices we use every day, from talking Alexa speakers to smart TVs. But we've got a giant blind spot when it comes to the data companies probing our phones.

You might assume you can count on Apple to sweat all the privacy details. After all, it touted in a recent ad, "What happens on your iPhone stays on your iPhone." My investigation suggests otherwise.

iPhone apps I discovered tracking me by passing information to third parties — just while I was asleep — include Microsoft OneDrive, Intuit's Mint, Nike, Spotify, The Washington Post and IBM's the Weather Channel. One app, the crime-alert service Citizen, shared personally identifiable information in violation of its published privacy policy.

And your iPhone doesn't only feed data trackers while you sleep. In a single week, I encountered over 5,400 trackers, mostly in apps, not including the incessant Yelp traffic. According to

privacy firm Disconnect, which helped test my iPhone, those unwanted trackers would have spewed out 1.5 gigabytes of data over the span of a month. That's half of an entire basic wireless service plan from AT&T.

AD

Don't use default privacy settings on sites and devices

The Post's Geoffrey A. Fowler explains all the things companies can get if you use their default privacy settings. How to change them: wapo.st/SayNoToDefaults (Jhaan Elker, David Jorgenson, Geoffrey Fowler/The Washington Post)

"This is your data. Why should it even leave your phone? Why should it be collected by someone when you don't know what they're going to do with it?" says Patrick Jackson, a former National Security Agency researcher who is chief technology officer for Disconnect. He hooked my iPhone into special software so we could examine the traffic. "I know the value of data, and I don't want mine in any hands where it doesn't need to be," he told me.

In a world of data brokers, Jackson is the data breaker. He developed an app called Privacy Pro that identifies and blocks many trackers. If you're a little bit techie, I recommend trying the free iOS version to glimpse the secret life of your iPhone.

Yes, trackers are a problem on phones running Google's Android, too. Google won't even let Disconnect's tracker-protection software into its Play Store. (Google's rules prohibit apps that might interfere with another app displaying ads.)

AD

Help Desk: Ask our tech columnist a question

Part of Jackson's objection to trackers is that many feed the personal data economy, used to target us for marketing and political messaging. Facebook's fiascos have made us all more aware of how our data can be passed along, stolen and misused — but Cambridge Analytica was just the beginning.

Jackson's biggest concern is transparency: If we don't know where our data is going, how can we ever hope to keep it private?



Patrick Jackson, chief technology officer for Disconnect, hooked columnist Geoffrey A. Fowler's iPhone into software so they could examine the personal data flowing out of the phone. (James Pace-Cornsilk/The Washington Post)

The app gap

App trackers are like the cookies on websites that slow load times, waste battery life and cause creepy ads to follow you around the Internet. Except in apps, there's little notice trackers are lurking and you can't choose a different browser to block them.

Why do trackers activate in the middle of the night? Some app makers have them call home at times the phone is plugged in, or think they won't interfere with other functions. These late-night encounters happen on the iPhone if you have allowed "background app refresh," which is Apple's default.

AD

With Yelp, the company says the behavior I uncovered wasn't a tracker but rather an "unintended issue" that's been acting like a tracker. Yelp thinks my discovery affects 1 percent of its iOS users, particularly those who've made reservations through Apple Maps. At best, it is shoddy software that sent Yelp data it didn't need. At worst, Yelp was amassing a data trove that could be used to map people's travels, even when they weren't using its app.

A more typical example is DoorDash, the food-delivery service. Launch that app, and you're sending data to nine third-party trackers — though you'd have no way to know it.

App makers often use trackers because they're shortcuts to research or revenue. They run the gamut from innocuous to insidious. Some are like consultants that app makers pay to analyze what people tap on and look at. Other trackers pay the app makers, squeezing value out of our data to target ads.

AD

Hands off my data! 15 default privacy settings you should change right now.

In the case of DoorDash, one tracker called Sift Science gets a fingerprint of your phone (device name, model, ad identifier and memory size) and even accelerometer motion data to help identify fraud. Three more trackers help DoorDash monitor app performance — including one called Segment that routes onward data including your delivery address, name, email and cell carrier.

DoorDash's other five trackers, including Facebook and Google Ad Services, help it understand the effectiveness of its marketing. Their presence means Facebook and Google know every time you open DoorDash.

The delivery company tells me it doesn't allow trackers to sell or share our data, which is great. But its privacy policy throws its hands up in the air: "DoorDash is not responsible for the privacy practices of these entities," it says.

AD

All but one of DoorDash's nine trackers made Jackson's naughty list for Disconnect, which also powers the Firefox browser's private browsing mode. To him, any third party that collects and retains our data is suspect unless it also has pro-consumer privacy policies like limiting data retention time and anonymizing data.

Microsoft, Nike and the Weather Channel told me they were using the trackers I uncovered to improve performance. Mint, owned by Intuit, said it uses an Adobe marketing tracker to help figure out how to advertise to Mint users. The Post said its trackers were used to make sure ads work. Spotify pointed me to its privacy policy.

Privacy policies don't necessarily provide protection. Citizen, the app for location-based crime reports, published that it wouldn't share "your name or other personally identifying information." Yet when I ran my test, I found it repeatedly sent my phone number, email and exact GPS coordinates to the tracker Amplitude.

AD

After I contacted Citizen, it updated its app and removed the Amplitude tracker. (Amplitude, for its part, says data it collects for clients is kept private and not sold.)

"We will do a better job of making sure our privacy policy is clear about the specific types of data we share with providers like these," Citizen spokesman J. Peter Donald said. "We do not sell user data. We never have and never will."

The problem is, the more places personal data flies, the harder it becomes to hold companies accountable for bad behavior — including inevitable breaches.

As Jackson kept reminding me: "This is your data."

Las Vegas. (David Becker/Getty Images)

The letdown

What disappoints me is that the data free-for-all I discovered is happening on an iPhone. Isn't Apple supposed to be better at privacy?

"At Apple we do a great deal to help users keep their data private," the company says in a statement. "Apple hardware and software are designed to provide advanced security and privacy at every level of the system."

AD

In some areas, Apple is ahead. Most of Apple's own apps and services take care to either encrypt data or, even better, to not collect it in the first place. Apple offers a privacy setting called "Limit Ad Tracking" (sadly off by default) which makes it a little bit harder for companies to track you across apps, by way of a unique identifier for every iPhone.

And with iOS 12, Apple took shots at the data economy by improving the "intelligent tracking prevention" in its Safari web browser.

Alexa has been eavesdropping on you this whole time

Yet these days, we spend more time in apps. Apple is strict about requiring apps to get permission to access certain parts of the iPhone, including your camera, microphone, location, health information, photos and contacts. (You can check and change those permissions under privacy settings.) But Apple turns more of a blind eye to what apps do with data we provide them or they generate about us — witness the sorts of tracking I found by looking under the covers for a few days.

"For the data and services that apps create on their own, our App Store Guidelines require developers to have clearly posted privacy policies and to ask users for permission to collect data before doing so. When we learn that apps have not followed our Guidelines in these areas, we either make apps change their practice or keep those apps from being on the store," Apple says.

Yet very few apps I found using third-party trackers disclosed the names of those companies or how they protect my data. And what good is burying this information in privacy policies, anyway? What we need is accountability.

Getting more deeply involved in app data practices is complicated for Apple. Today's technology frequently is built on third-party services, so Apple couldn't simply ban all connections to outside servers. And some companies are so big they don't even need the help of outsiders to track us.

The result shouldn't be to increase Apple's power. "I would like to make sure they're not stifling innovation," says Andrés Arrieta, the director of consumer privacy engineering at the Electronic Frontier Foundation. If Apple becomes the Internet's privacy police, it could shut down rivals.

Jackson suggests Apple could also add controls into iOS like the ones built into Privacy Pro to give everyone more visibility.

Or perhaps Apple could require apps to label when they're using third-party trackers. If I opened the DoorDash app and saw nine tracker notices, it might make me think twice about using it.

Read more tech advice and analysis from Geoffrey A. Fowler:

[When tax prep is free, you may be paying with your privacy](#)

[Not all iPhones are the same. These cost less and are better for the Earth.](#)

[Rock this way: AirPods, Beats and Bose wireless ear buds take the headbang test](#)

Dig Deeper: Personal tech + Privacy

Want to learn about how to keep your personal information private? Check out our curated list of stories below.

[Get smart about stopping spam calls](#)

Americans receive more than 5.2 billion automated calls in a month. But there are new apps to help stem the deluge.

[Understanding what your phone tracks for marketers](#)

As tech columnist Geoffrey Fowler slept, a dozen marketing companies used his iPhone to learn his number, email, location and IP address.

[Say no to your default privacy settings](#)

Changing privacy default settings means you'll get less personalization from some services, but it can slow down the number of eerie on-the-nose ads driven by data siphoned by major companies.

[Home](#)

Share