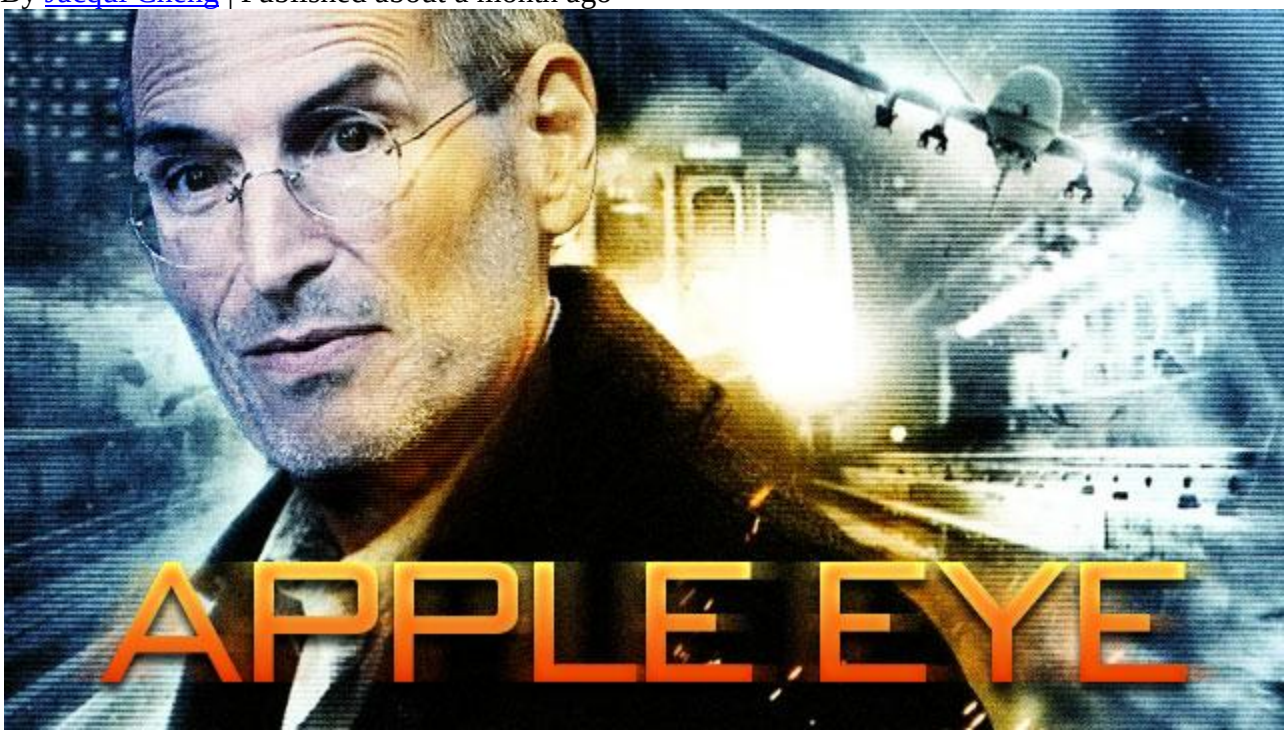
How Apple tracks your location without consent, and why it matters

By Jacqui Cheng | Published about a month ago

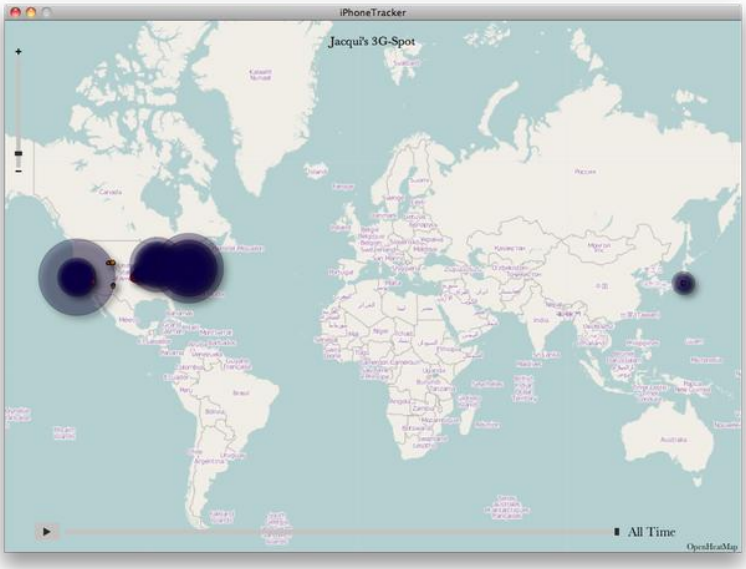


If you haven't yet enabled encrypted backups for your iPhone or iPad, now's definitely the time to start. Two security researchers have discovered a simple way to map out where you've been almost anywhere in the world—without any hacking involved. The information comes from a location cache file found within your iPhone's backups on your Mac or PC, bringing out serious privacy concerns and opening the door for a jealous spouse, thief, or even a crafty trojan to take a detailed look at your whereabouts. And it's information that no one should have access to—not even law enforcement, barring a court order.

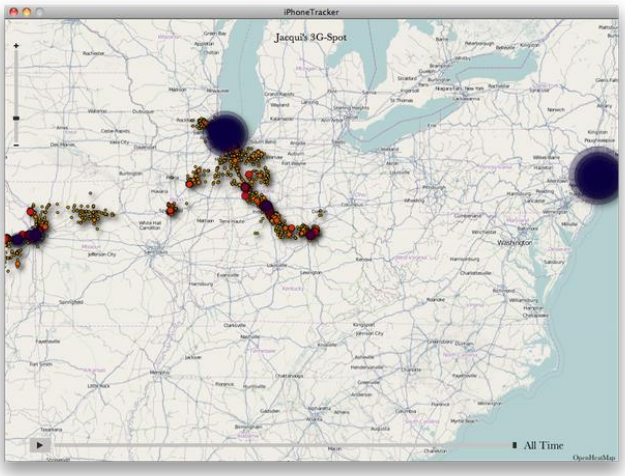
Researchers Alasdair Allan and Pete Warden revealed their findings on Wednesday ahead of their presentation at the Where 2.0 conference taking place in San Francisco. The two discovered that the iPhone or 3G iPad—anything with 3G data access, so no iPod touch—are logging location data to a file called consolidated.db with latitude and longitude coodinates and a timestamp. The data collection appears to be associated with the launch of iOS 4 last June, meaning that many users (us at Ars included) have nearly a year's worth of stalking data collected.

In order to drive the point home, the two developed an open source application called iPhone Tracker that lets anyone with access to your computer see where you've been. For example, my log appears to start on June 23, 2010 (one day before the launch of the iPhone 4) and shows nearly every trip I've ever taken since then and when. You can see that I seem to spend most of my time in Chicago and occasionally the suburbs, with road trips down to Indianapolis,

Cincinnati, Springfield, and Wichita. I also fly to New York City and San Francisco, and I have a few dots at the Tokyo Narita airport when I traveled through there in October.



Where in the world is Jacqui Cheng?



What's *not* shown is a week-long trip I took to Hong Kong in October. Why? Because I left my iPhone's cellular and data connections turned off and only used GPS with WiFi while I was there. But if I know I used GPS in Hong Kong in order to make geotagged tweets and photos, shouldn't it show up in this log file? The answer is no, and the reason behind it should scare you.

Court order required—or not

From the end-user point of view, Apple only does one kind of location tracking, and it happens via GPS. The company makes sure to notify you on your iPhone or iPad every time you use an app that will grab your GPS location so that you're always informed of when you're being tracked. However, that's not all that's going on behind the scenes. Apple also triangulates your

location from cell phone towers and logs that information in order to help get a faster GPS lock (or to find your location without GPS if you're getting bad GPS signal).

Allan and Warden point out in their iPhone Tracker FAQ that this is indeed the method Apple is using in the consolidated.db file, and this is also the reason users might see strange iPhone Tracker dots in places they haven't been.

"As far as we can tell, the location is determined by triangulating against the nearest cell-phone towers. This isn't as accurate as GPS, but presumably takes less power," they wrote. "In some cases it can get very confused and temporarily think you're several miles from your actual location, but these tend to be intermittent glitches."

Users don't get to decide whether their locations are tracked via cell towers or not—unlike GPS, there is no setting that lets users turn it off, there's no explicit consent every time it happens, and there's no way to block the logging. (Nitpickers will point out that you do give your consent to iTunes when you download and install iOS 4, but this is not treated the same way as the consent given to the iPhone every time an app wants to use GPS.) So, whether or not you're using GPS, if you're using your iPhone as a cell phone, you are being tracked and logged constantly without your knowledge. This is why my trip to Hong Kong wasn't logged (because I had all cell connections turned off while GPS was on), but my stop-over in Tokyo Narita on the same trip *was* logged (I had turned on my phone to make a quick call, but did not use GPS).

Of course, the fact that this data exists somewhere is nothing new. Cell companies have been tracking this triangulation information for their own purposes for years. In the US, however, regular people cannot access that data—law enforcement must obtain a court order before they can get it for an investigation, and your jealous spouse can't get it from the wireless company at all.

What the cellco has on you is now basically being mirrored in a file on your iPhone or iPad without any kind of encryption, and is also being copied to your computer. (Allan and Warden say that, according to their research, no other phones log triangulated cell locations in this way, including Android phones.) And, if you leave iTunes on the default syncing settings, your iPhone backups aren't being encrypted on the computer either, making tools like iPhone Tracker possible.

Who has access now?

So your iPhone—and probably your computer—now both have a file that mirrors data that was previously limited to law enforcement, which itself was only able to obtain it from a court order. Without encrypted backups, someone who has access to your computer can see your whereabouts. "By passively logging your location without your permission, Apple have made it possible for anyone from a jealous spouse to a private investigator to get a detailed picture of your movements," the team wrote.

But even if you check the box to encrypt your iPhone backups on the computer, the file is still unencrypted on your iPhone, and it wouldn't be hard for someone with ill intentions to access it.

"Anyone with a good jailbreaking tool could get it off the phone too. And of course my forensics tools," iPhone hacker and forensics expert Jonathan Zdziarski told Ars. "In fact even the old SSH worms (which are still effective on a large number of handsets) could be modified to collect this. It's part of the Core Location cache on the phone. So, it's not a covert, evil, Big Brother secret invisible file, but Apple has been administratively lazy in their programming, which is the root cause of most data leaks on the iPhone."

Security expert and repeat Pwn2Own champion Charlie Miller was slightly less pessimistic about who can access the file, but agreed that it wouldn't be trivial for an experienced iPhone tinkerer.

"This file is only readable by root. That means that a rogue App Store app won't be able to read it. Even a bad guy who hacks into your browser won't be able to read it," Miller told Ars. However, remote hackers can make use of two separate exploits—a code execution exploit and a privilege escalation exploit—which Miller points out have been available before in the form of jailbreakme.com (a tool that allowed users to jailbreak their devices through a Web page on the Internet).

Although Apple makes an effort to patch security holes as they come up, the jailbreak community is constantly working on new ways to gain access to previously forbidden files—if something like Jailbreakme existed before, it could exist again.

"It is bad for privacy this file exists, especially when it doesn't seem to be linked to any particular feature that provides any benefit," Miller said. "[T]here is no easy way to wipe the data from it."

Implications for Apple

Zdziarski says the iPhone has actually been logging this location data for longer than a year, but it wasn't so easily accessible before the launch of iOS 4 in mid-2010.

"The iPhone has been keeping caches of user location data for quite some time now. iOS 4 made it a little easier to get to, but law enforcement has been using data like this since around 2009 to build evidence against criminals using the iPhone," Zdziarski told Ars. "Similar data has been cached in different files prior to iOS 4. [The cache revealed today] is a bit more aggressive and centralized, making it easier to access by normal folks."

Apple did not respond to our questions about how long it has been logging the location data, but it's clear that the reason the issue is coming to light now is because of this easy access. Zdziarski added that the iPhone in general "leaks like a sieve," and warned that consumers should consider the possible implications to their personal privacy with today's discovery.

Privacy advocates are taking things a step further by calling out Apple for abusing user trust. "Apple has some explaining to do. iPhone owners place a great deal of trust in Apple, and Apple has a responsibility not to abuse that trust," Princeton University Center for Information Technology Policy researcher and regular Ars contributor Timothy B. Lee said.

"This incident raises questions about whether Apple is serious about user privacy," Lee continued. "If this was an accident, Apple needs to fix the problem and put in place procedures to make sure it doesn't happen again. If the data is being collected deliberately, perhaps in preparation for a future product, Apple should have clearly notified users and given them an opportunity to opt out."

Apple told Congress last July that all location data collected by the iPhone remains private. According to Apple lead counsel Bruce Sewell, Apple does collect anonymous location data from iPhones in an effort to improve its own database of cell tower and WiFi hotspot locations, but that it only does this with user consent. The discovery made by Allan and Warden clearly shows that this is happening constantly *without* explicit consent like Apple treats GPS, however, and it sure isn't anonymous when it's accessible directly from the user's device.

So, is there anywhere you've been in the last year that you don't want anyone to know about?

http://arstechnica.com/apple/news/2011/04/how-apple-tracks-your-location-without-your-consent-and-why-it-matters.ars