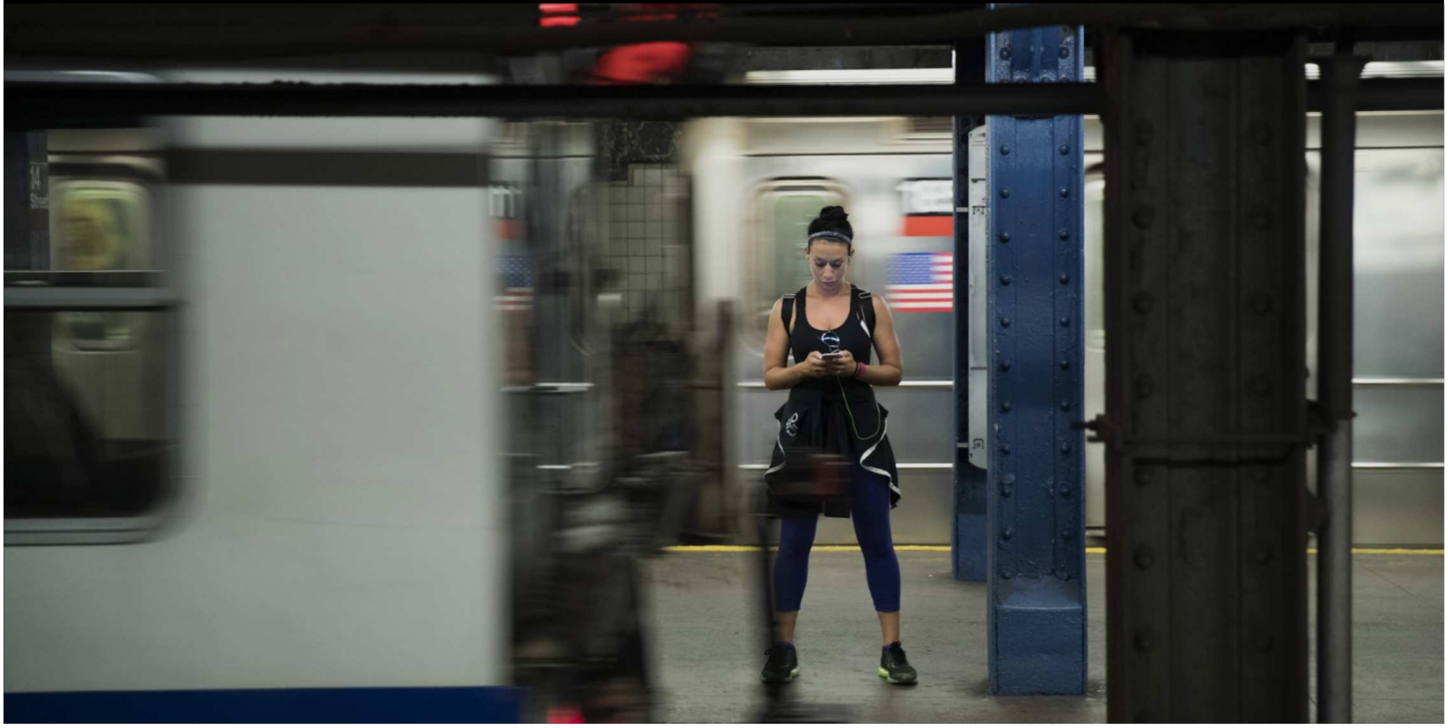
The Intercept

IPHONES SECRETLY SEND CALL HISTORY TO APPLE, SECURITY FIRM SAYS

Kim Zetter

November 17 2016, 3:00 a.m.

42



Getty Images

LEIA EM PORTUGUÊS ⟶

APPLE EMERGED AS a guardian of user privacy this year after fighting FBI demands to help crack into San Bernardino shooter Syed Rizwan Farook's iPhone. The company has gone to great lengths to secure customer data in recent years, by implementing better encryption for all phones and refusing to undermine that encryption.

But private information still escapes from Apple products under some circumstances. The latest involves the company's online syncing service iCloud.

Russian digital forensics firm Elcomsoft has found that Apple's mobile devices automatically send a user's call history to the company's servers if iCloud is enabled — but the data gets uploaded in many instances without user choice or notification.

"You only need to have iCloud itself enabled" for the data to be sent, said Vladimir Katalov, CEO of Elcomsoft.

The logs surreptitiously uploaded to Apple contain a list of all calls made and received on an iOS device, complete with phone numbers, dates and times, and duration. They also include missed and bypassed calls. Elcomsoft said Apple retains the data in a user's iCloud account for up to four months, providing a boon to law enforcement who may not be able to obtain the data either from the user's phone, if it's encrypted with an unbreakable passcode, or from the carrier. Although large carriers in the U.S. retain call logs for a year or more, this may not be the case with carrier outside the US.

It's not just regular call logs that get sent to Apple's servers. FaceTime, which is used to make audio and video calls on iOS devices, also syncs call history to iCloud automatically, according to Elcomsoft. The company believes syncing of both regular calls and FaceTime call logs goes back to at least iOS 8.2, which Apple released in March 2015.

And beginning with Apple's latest operating system, iOS 10, incoming missed calls that are made through third-party VoIP applications like Skype, WhatsApp, and Viber, and that use Apple CallKit to make the calls, also get logged to the cloud, Katalov said.

Because Apple possesses the keys to unlock iCloud accounts, U.S. law enforcement agencies can obtain direct access to the logs with a court order. But they still need a tool to extract and parse it.

Elcomsoft said it's releasing an update to its Phone Breaker software tool today that can be used to extract the call histories from iCloud accounts, using the account holder's credentials. Elcomsoft's forensic tools are used by law enforcement, corporate security departments, and even consumers. The company also leases some of its extraction code to Cellebrite, the Israeli firm the FBI regularly uses to get into seized phones and iCloud data.

In some cases, Elcomsoft's tool can help customers access iCloud even without account credentials, if they can obtain an authentication token for the account from the account holder's computer, allowing them to get iCloud data without Apple's help. The use of authentication tokens also bypasses two-factor authentication if the account holder has set this up to prevent a hacker from getting into their account, Elcomsoft notes on its website.

Apple's collection of call logs potentially puts sensitive information at the disposal of people other than law enforcement and other Elcomsoft customers. Anyone else who might be able to obtain the user's iCloud credentials, like hackers, could potentially get at it too. In 2014, more than 100 celebrities fell victim to a phishing attack that allowed a hacker to obtain their iCloud credentials and steal nude photos of them from their iCloud accounts. The perpetrator reportedly used Elcomsoft's software to harvest the celebrity photos once the accounts were unlocked.

Generally, if someone were to attempt to download data in an iCloud account, the system would email a notification to the account owner. But Katalov said no notification occurs when someone downloads synced call logs from iCloud.

Apple acknowledged that the call logs are being synced and said it's intentional.

"We offer call history syncing as a convenience to our customers so that they can return calls from any of their devices," an Apple spokesperson said in an email. "Device data is encrypted with a user's passcode, and access to iCloud data including backups requires the user's Apple ID and password. Apple recommends all customers select strong passwords and use two-factor authentication."

The syncing of iCloud call logs would not be the first time Apple has been found collecting data secretly. A few months ago, The Intercept reported about similar activity occurring with iMessage logs.

Chris Soghoian, chief technologist for the American Civil Liberties Union, said he's not surprised that Apple is collecting the information.

"It's arguably not even the worst thing about iCloud," he told The Intercept. "The fact that iCloud backs up what would otherwise be end-to-end encrypted iMessages is far worse in my mind. There are other ways the government can obtain [call logs]. But without the backup of iMessages, there may be no other way for them to get those messages."

Still, he said it's further proof that "iCloud really is the Achilles heel of the privacy of the iPhone platform. The two biggest privacy problems associated with iCloud don't have check boxes [for users to opt out], nor do they require that you opt in either."

Jonathan Zdziarski, an iOS forensics expert and security researcher, said he doesn't think Apple is doing anything nefarious in syncing the call logs. But he said that Apple needs to be clear to users that the data is being collected and stored in the cloud.

Authorized and Unauthorized iCloud Collection

iCloud is Apple's cloud service that allows users to sync data across multiple Apple devices, including iPhones, iPads, iPods, and Macs. The iPhone menu corresponding to the service gives users the option of syncing mail, contacts, calendars, reminders, browser history, and notes and wallet data. But even though call logs are automatically getting synced as well, the menu does not list them among the items users can choose to sync. Because there's no way to opt in to sync call logs, there is also no way to opt out – other than turning off iCloud completely, but this can cause other issues, like preventing apps from storing documents and data (such as WhatsApp backups) in the cloud.

"You can only disable uploading/syncing notes, contacts, calendars, and web history, but the calls are always there," Katalov said. One way call logs will disappear from the cloud is if a user deletes a particular call record from the log on their device; then it will also get deleted from their iCloud account during the next automatic synchronization.

Katalov said they're still researching the issue but it appears that in some cases the call logs sync almost instantly to iCloud, while other times it happens only after a few hours.

In addition to syncing data among their devices, users can also configure their iCloud account to automatically back up and store their data. Katalov said that call logs get sent to the cloud with these backups as well, but this is separate from the trafficking his company discovered: Even if users disable the backups, their call logs will still get synced to Apple's servers.

"I would suggest Apple to add a simple option to disable call log syncing, as they do that for calendars and other things," Katalov told The Intercept, though he acknowledges this would likely take some re-architecting on Apple's part. Nonetheless, he says, "They should allow people to disable that if they want to."

Even as Apple has increased the security of its mobile devices in recent years, the company has been moving more and more data to the cloud, where it is less protected. Although iCloud data is encrypted on Apple's server, Apple retains the encryption keys in almost every instance and can therefore unlock the accounts and access data for its own purposes or for law enforcement.

"All of your [iCloud] data is encrypted with keys that are controlled by Apple, but the average user isn't going to understand that," Zdziarski said. "You and I are well aware that Apple can read any of your iCloud data when they want to."

A report in the Financial Times nine months ago indicated Apple plans to re-architect iCloud to resolve this issue and better protect customer data, but that has yet to occur.

Apple discusses the privacy implications of iCloud collection on its website and does say that implementing backups will send to iCloud "nearly all data and settings stored on your device." A 63-page white paper on the site discloses more clearly that call logs get uploaded to Apple servers when iCloud backups are enabled. But neither document mentions that the logs still get uploaded even if backups aren't enabled.

Even in an online document about handling legal requests from law enforcement, Apple never mentions that call logs are available through iCloud. It says that it possesses subscriber information that customers provide, including name, physical address, email address, and telephone number. It also says it retains IP connection logs (for up to 30 days), email metadata (for up to 60 days), and content that the user chooses to upload, such as photos, email, documents, contacts, calendars, and bookmarks. The law enforcement document also says that Apple's servers have iOS device backups, which may include photos and videos in the user's camera roll, device settings, application data, iMessages, SMS and MMS messages, and voicemail.

The only time it mentions call logs is to say that iCloud stores call histories associated with FaceTime, but it says it maintains only FaceTime call invitation logs, which indicate when a subscriber has sent an invitation to someone to participate in a FaceTime call. Apple says the logs "do not indicate that any communication between users actually took place." It also says it only retains these logs for "up to 30 days."

But Elcomsoft said this is not true. Katalov said the FaceTime logs contain full information about the call, including the identification of both parties to the call and the call duration. He said his researchers also found that the FaceTime call logs were retained for as long as four months.

Early Clues From Frustrated Apple Customers

Some users are aware that their call logs are being synced to Apple's servers, because a byproduct of the automatic syncing means that if they have the same Apple ID as someone with a different device — for example, spouses who have different phones but use the same Apple ID — they will see calls from one device getting synced automatically to the device of the other person who is using the same ID.

"It's very irritating," one user complained in a forum about the issue. "My wife and I both have iPhones, we are both on the same apple ID. When she gets a call my phone doesn't ring but when she misses that call my phone shows a missed call icon on the phone app and when I go to the phone app it's pretty clearly someone who wasn't calling my phone. Any way to fix this so it stops?"

Another user expressed frustration at not knowing how to stop the syncing. "I use my phone for business and we have noticed in the last few days that all of the calls I make and receive are appearing in my wife's iPhone recent call history? I have hunted high and low in settings on both phones but with no joy."

There's no indication, however, that these customers realized the full implications of their logs being synced — that the same data is being sent to and stored on Apple's servers for months.

Apple isn't the only company syncing call logs to the cloud. Android phones do it as well, and Windows 10 mobile devices also sync call logs by default with other Windows 10 devices that use the same Microsoft account. Katalov said there are too many Android smartphone versions to test, but his company's research indicates that call log syncing occurs only with Android 6.x and newer versions. As with Apple devices, the only way for a user to disable the call history syncing is to disable syncing completely.

"In 'pure' [stock versions of] Android such as one installed on Nexus and Pixel devices, there is no way to select categories to sync," Katalov said. "For some reason, that is only able on some third-party Android versions running on Sony, HTC, Samsung, etc." The company already produces a tool for harvesting call logs associated with Android devices.

There's little that subscribers can do to prevent law enforcement from obtaining their iCloud call logs. But to protect against hackers who might obtain their Apple ID from doing the same, they can use two-factor authentication. But Zdziarski said there's another solution.

"The takeaway really is don't ever use iCloud. I won't use it myself until I can be in control of the encryption keys," he said.

Correction: Nov. 17, 2016

An earlier version of this story quoted the director of a university computer forensics program, who is also a former FBI supervisory agent, stating that telecom providers generally only retain call logs for 30 or 60 days. It has been updated to clarify that U.S. providers retain such information for a year or more.