iPhone secretly records location of users

Bryan Dyne, Andre Damon
28 April 2011

Mobile phones and tablets made by Apple Computer have been secretly recording every place that their owner has been since June 2010, according to research findings presented April 20. There is no way to disable the recording without voiding the devices' warranty, and the devices continue to track their location even if "location services" are disabled.

The revelation set off a firestorm of commentary over privacy rights as subsequent media reports announced that both of Apple's major competitors, Google and Microsoft, similarly track users' locations.

Starting with the latest release of Apple's mobile operating system, iOS 4, iPhone mobile phones and 3G-enabled iPad tablets have stored a record of their location histories in a secret file called 'consolidated.db'. The list of locations is gathered by triangulating clusters of nearby cellular towers and wireless networks to find the position of the phone, then dumped into the file one after another.

Steve Jobs, the company's chief executive, replied to the allegations in a personal email to a user Monday, saying, "We don't track anyone. The info circulating around is false." The company followed up the letter with an official statement on the matter, saying, "Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so."

Earlier this week, the *Wall Street Journal* said its research showed phones using both Apple's and Google's operating systems sent location information back to the respective companies on a regular basis. The revelation contradicts the claims by both companies that they do not track the locations of phones running their software.

Apple said in its Wednesday statement that the location data it received from phones consisted of anonymous, encrypted records of nearby wireless networks and cell towers, which were pooled together, processed, and sent back to individual phones to allow them to determine their location more quickly.

Apple said that the most troubling aspects of its location policy—the fact that locations are stored for months and never deleted, and the fact that the data is stored even when the user requests that location tracking be disabled—were oversights and will be fixed in an upcoming software update. It also said that the software update, to be released in the "next few weeks" will add encryption to the locations database.

Two iPhone customers sued Apple for privacy invasion and computer fraud Monday in response to the revelations.

Senator Al Franken of Minnesota summoned Apple and Google before a Senate Judiciary Committee hearing on mobile device privacy set for May 10. Earlier, Franken sent a letter to Apple asking why the company was "secretly compiling its customers location data … sometimes logging their precise geo-location up to 100 times a day."

The House Energy and Commerce Committee separately sent letters to the heads of six mobile phone operating system makers, including Steve Jobs, asking for clarification on their user tracking policies.

The data secretly gathered by Apple and Google is worth billions of dollars in advertising revenue. The total market value of location-based smartphone services is currently $2.9 billion and is expected to rise to $8.4 billion, according to research from Gartner, Inc. As both companies near the point where they saturate the market for their products, location-driven advertising is becoming a major avenue for expanding their profitability.

The locations database on Apple devices is not normally accessible to users. But if a user syncs his phone with a computer—to transfer music, for example—the file containing months of location data is transferred and stored unencrypted on the user's machine.

It is possible to make the location file more secure by encrypting phone backups, but the setting is not enabled by default. However a properly-equipped user who is able to physically access a phone or tablet will be able to get data from it in as little as two minutes, even if the device is password-protected.

Law enforcement agents in some states are already equipped to surreptitiously copy these location records, along with other data, and have not refuted charges that they are copying mobile phone data in routine searches.

Earlier this month, the American Civil Liberties Union (ACLU) said it had "credible information" that the mobile data extraction devices "were being used during routine stops without a warrant" by the Michigan State Police.

The ACLU said in an open letter dated April 13 that in 2006, the Michigan State Police purchased devices capable of completely copying the contents of mobile phones in under 90 seconds. The ACLU repeatedly filed Freedom of Information Act requests to the Michigan State Police over the course of three years to find out how the devices were being used, but has not had its requests granted.

The Michigan State Police did not deny the existence of the devices, but said that assembling the documents necessary to explain their use would cost $544,680, of which the ACLU would have to pay $272,340 up front.

Police Inspector Greg Zarotney told the State house of Representatives' Oversight, Reform and Ethics Committee that the devices "are not being used in routine traffic stops," and that "We're confident we're using them within the confines of the law."

CelleBrite, the manufacturer of the devices, says that its products can "insure that a suspect's phone can be examined before the individual has a chance to destroy or erase data."

The manufacturer added that the device "allows you to extract a wide variety of data types from the handset: Phonebook; Text messages; Call History… Deleted Text Messages ..; Audio Recordings; Video; Pictures and Images; Ringtones... Complete File System Memory Dump on selected handsets."

The ACLU said it was concerned that the devices would be used to copy sensitive information during routine traffic stops without consent. "A device that allows immediate, surreptitious intrusion into private data creates enormous risks that troopers will ignore these requirements to the detriment of the constitutional rights of persons whose cell phones are searched," the ACLU said in its letter to the department.