InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

Do Smartphone Sensors Present Security Risk?

By Mathew J. Schwartz

October 14, 2013

Privacy alert: Every smartphone's sensors record data in slightly different ways, and those differences are substantial enough to be measured and used to identify the device.

That warning comes via security researcher Hristo Bojinov, a computer science Ph.D. candidate at Stanford University who's been working with a team of researchers to test whether the sensors inside smartphones might pose a privacy risk, the *San Francisco Chronicle* first reported.

To date, the Stanford researchers have discovered that the accelerometers built into smartphones, which measure device acceleration and orientation -- used, for example, by the operating system to rotate displays -- don't all record reality in quite the same way.

For example, when a smartphone is resting flat on a tabletop, the reading generated by the accelerometer -- which measures acceleration along the Z-axis, which in this example would be a line rising perpendicularly from the smartphone -- should be -1 when it's lying face up, or +1 when lying face down. But in reality, a face-down device generates a Z-axis measurement that's more akin to 1.00281308281.

That result was generated via the Stanford Sensor ID Experiment website, which the researchers wrote in JavaScript to see the Z-axis measurements being returned by any given smartphone. (Anyone can use the website to test a device.) Their finding, which will be detailed in a forthcoming research paper, is that the measurements returned by any given device are unique enough to fingerprint -- or uniquely identify -- that device.

Who might want to track smartphones in this manner? As *The Verge* reported, such fingerprinting could serve as yet another tool for advertisers to identify unique devices, and by extension the identity of the person using them.

"People need to consider the whole system when they think about privacy," Stanford researcher Bojinov told the *San Francisco Chronicle*, noting that he wouldn't be surprised if advertisers had already discovered some of these tracking techniques themselves. By highlighting the fact that smartphone sensors produce data in unique ways, Bojinov said he hoped that smartphone manufacturers and software developers might be able to find ways of safeguarding such data gathering against improper use.

Furthermore, accelerometers aren't the only way that smartphones can be fingerprinted. For example, Sara M. Watson, a fellow at the Berkman Center for Internet and Society at Harvard University, recently wrote in a *Wired* opinion piece that the new M7 motion processor in the Apple 5s smartphones has been designed to continually record data from the device's accelerometer, compass and gyroscope sensors, which could be used by so-called quantified self apps that serve as personal activity trackers. But the sensor data could easily be collected by apps -- or even third parties -- without the owner's knowledge.

Of course, advertisers aren't the only potential organizations that might have their eye on this type of data, and fears over government tracking have been growing since former NSA contractor Edward Snowden began sharing confidential agency documents with select journalists this past summer. So what's the likelihood that the NSA isn't already tracking smartphones using these types of obscure -- if not hitherto unknown -- techniques?

In fact, sensor data might not even be required to create fingerprint phones. For example, one 2009 document recently released by the NSA detailed an "analytical tool" -- the name of which was redacted -- for identifying the date and time that a phone first went online, as well as the date and time that a phone last went offline. It also gets the total number of calls, and the ratio of unique contacts to calls, but not the specific numbers contacted, according Cato Institute research fellow Julian Sanchez's reading of the document.

What's the use of this type of information? "One possibility that jumps out at me -- and perhaps anyone else who's a fan of *The Wire* -- is that this is the kind of information you would want if you were trying to identify disposable prepaid 'burner' phones being used by a target who routinely cycles through cell phones as a counter-surveillance tactic," Sanchez said on the Just Security forum. "The number of unique contacts and call/contact ratio would act as a kind of rough fingerprint -- you'd assume a phone being used for dedicated clandestine purposes to be fairly consistent on that score -- while the first/last call dates help build a timeline: You're looking for a series of phones that are used for a standard amount of time, and then go dead just as the next phone goes online."

In that example, the pattern of usage -- rather than the device itself -- could be used to fingerprint a device. From a privacy and tracking standpoint, in other words, sometimes being unique has its downsides.