the Atlantic

Print | Close

What Does Your Phone Know About You? More Than You Think

By Alexis Madrigal

Figuring that I've got nothing to hide or steal, I'd always privileged convenience over any privacy and security protocols. Not anymore.

I plugged my phone into my computer and opened an application called Lantern, a forensics program for investigating iPhones and iPads. Ten minutes later, I'm staring at everything my iPhone knows about me. About 14,000 text messages, 1,350 words in my personal dictionary, 1,450 Facebook contacts, tens of thousands of locations pings, every website I've ever visited, what locations I've mapped, my emails going back a month, my photos with geolocation data attached and how many times I checked my email on March 24 or any day for that matter. Want to reconstruct a night? Lantern has a time line that combines all my communications and photos in one neat interface. While most of it is invisible during normal operations, there is a record of every single thing I've done with this phone, which also happens to form a pretty good record of my life.

Figuring that I've got nothing to hide or steal, I'd always privileged convenience over any privacy and security protocols. Not anymore. Immediately after trying out Lantern, I enabled the iPhone's passcode and set it to erase all data on the phone after 10 failed attempts. This thing remembers more about where I've been and what I've said than I do, and I'm damn sure I don't want it falling into anyone's hands.

* * *

Last week, two separate news items highlighted the importance of what your phone knows. First, the American Civil Liberties Union in Michigan went public with its Freedom of Information Act request for data on how the state police are using a hardware system called Cellebrite UFED. The ACLU suggested that state troopers were using the UFED during routine traffic stops. While the $4,000-8,000 price tag of the systems would suggest it's unlikely that many cops have the systems in their cars, even the possibility of such a practice has got to set Fourth Amendment alarm bells ringing from here to 1791. Here's a word of advice: if a law enforcement official ever asks for your phone, just say no.

In a June 2008 article, Cellebrite bragged that it had sold 3,500 Cellebrite devices in the eleven months the UFED had been on the market. Throw in other common devices from companies like Cellebrite, Parabens, Micro Systemation and Katana Forensics, makers of Lantern, and you can begin to see the scale of mobile phone data extraction that must be occurring across the nation's law enforcement landscape.

I don't say that to suggest that the police are doing anything wrong. Like computers, phones certainly seem like fair game for investigators. They're scrambling like the rest of us to keep up with a rapidly changing mobile technology landscape that's forcing strange ethical choices onto them. Let's say someone was texting while driving, which may be against the law in your state. They might want that evidence, so they extract the data from the phone and when they look at it, lo and behold, there are several time-tagged photos of the person getting high earlier that day. Suddenly, a minor ticket gets turned into a DUI.

We're not sure how the courts are going to decide whether evidence like this is admissible because it's complicated. Doctrines like "plain view" -- that cops can seize evidence without a warrant if they can see it -- require informational friction and human embodiment to make sense. With a searchable stash of a phone's data, what is in plain view? What isn't? It's just so easy to find out more than you asked.

The other big mobile data news last week came out of O'Reilly's Where 2.0 conference during which two researchers showed in dramatic fashion that the iPhone keeps a location log of where the phone has been, a fact which Apple had declined to tell anyone and which had first been discovered by the same guy who helped Katana Forensics managing director Sean Morrissey create the Lantern software that opened up my phone for inspection.

* * *

Alex Levinson assisted on Lantern from his living room in Rochester, New York. He's still a student at Rochester Institute of Technology*, but he tells me that his room is "basically an information security and forensic laboratory." He ticks off the equipment at his disposal: four MacBooks, a couple other laptops, two desktop boxes running different operating systems, two iPhones, a couple Droids, a Blackberry, all kinds of wireless and networking equipment and terabytes of storage. He may also know Apple's iOS as well as anyone in the world. A mere 48 hours after Apple released the iPhone 4, Levinson had patched Lantern to support the upgrade. He waited in line for ten hours and spent the next two days poking around the file system that sits underneath the ultraslick user experience.

That's one reason he was the first to notice that Apple had begun storing its location data in the new, more easily accessible way. But all that time spent rummaging around under the iPhone's hood also led him to develop an actual philosophy about the difference between mobile and computer forensics. In mobile, he said, no one directly interacts with the file system. You don't pull up documents and save and delete them the way we do with computer.

"How are those new interactions producing evidence that would be relevant to what I'm doing?" Levinson asked rhetorically.

For him, that means knowing every single thing a phone can output for him.

"Take a basic phone, maybe a Razr," he said. "I would map out every single data point within the phone. We've got text messages. We've got pictures. We've also got picture messaging, which could be a subset. We've got call logs. We might have baseband logs." Then, he'd start to correlate one thing with another. If there are timestamps and locations, every message or photo can be fixed in space and time.

"You're beginning to create a forensic model of the human use of the device," he said. "The software's goal is to recreate a rich forensic time line of how this device was used so the analyst can put their shoes in place of the user and see what happened with this device."

Indeed, using Lantern, it's remarkably easy to reconstruct what happened to me on, say, April 13, my birthday, and the next day, when I celebrated the release of my book at an *Atlantic* party.

I missed a call from my best friend at 12:30 a.m. wishing me a happy birthday. I got up at 7:04 a.m., which I know because I sent him back a text message. I got several more birthday greetings and phone calls. Then I had a meeting with Richard Florida and some other *Atlantic* people during which I Googled several things related to the meeting. Then I went on a radio show in Colorado, which I know both because my calendar shows it, but also because I searched the radio station. Then I took a cab to Union Station (I texted, "On my way to Union Station") and snapped a picture of a tour bus that we passed which claimed to be "American-Owned & Operated." I got to New York around 7:45 p.m., when I Googled my hotel's address. The next morning, I went to WNYC at 160 Varick Street to be interviewed by Brian Lehrer, all of which is obvious from my Internet history, text messages and photos. Then I met with a prospective job candidate at Le Pain Quotidien according to my calendar and spent an hour researching RandTXT.com. Then I went to my book party at a private home, and took some photos, which Lantern pinpointed perfectly.

You could export most of this sequence to a Google Earth layer and look at it plotted with a time slider. Without trying to, I'd left a trail spelling out exactly what I did for 48 hours. Mobile forensics and mobile privacy don't have to sit in opposition, but what you can find with the former should inform our views about the latter. And you can suddenly find a ton with relatively simple tools.

The big deal about location data isn't the data itself; rather, the location data makes all the other information that can be extracted exponentially more useful. That's why mobile forensics is different, and why our devices may be where the bubbling privacy concerns of the last decade come to a head.

If our phones have become our outboard brains, we've actually put ourselves in a very difficult privacy position. Even searching a suspect's house could never yield a full inventory of that person's friends and acquaintances, the entire record of their voice and text communications -- and all the web pages he'd ever looked at. Now, law enforcement or a government official can have all of that in two minutes and physical access to one's cell phone.

Or as Cellebrite USA's CEO Aviad Ofrat excitedly told a trade magazine a couple years ago, "mobile device forensics is the future. With the wealth of data even a casual user has stored in his or her cellphone, smartphone, or PDA, it is quickly becoming THE one piece of evidence that is interrogated immediately."

Because where we go, so go our phones.

THE MOBILE PRIVACY SERIES

Atoms vs. Bits: Your Phone in the Eyes of the Law
5 Things You Can Tell From the Words I've Taught My iPhone

I'll be publishing part two of this series tomorrow after I visit the National Institute of Standards and Technology's mobile forensic tool testing lab in Gaithersburg, Maryland. This story has been updated. It originally incorrectly stated Alex Levinson's university. We regret the error.

This article available online at:

http://www.theatlantic.com/technology/archive/2011/04/what-does-your-phone-know-about-you-more-than-you-think/237786/