Ubiquitous Smartphones, Zero Privacy

Chris Rose, DBA., Capella University, USA

ABSTRACT

If your smartphone has a GPS, your provider knows exactly where you are and where you have been as well as who you have contacted. In addition, tracking software which logs where you have been and what you did has been previously found on Apple's iPhone and just recently, Carrier IQ tracking software has been acknowledged to be on over 150 million smartphones. If this is combined with a recent government directive that no warrant is needed to access this information, then if you have a smartphone, you really have zero privacy.

Keywords: Smartphones; Apple iPhone; Carrier IQ; Cell Phone Privacy

INTRODUCTION

In 1999, when the chief executive officer of Sun Microsystems, Scott McNealy told a group of reporters that consumer privacy issues are a "red herring." and that "You have zero privacy anyway," "Get over it." (Sprenger, 1999), perhaps he never dreamt how prophetic his words would become as we now move into the realm of ubiquitous smartphone usage.

But society is changing and confidentiality is being replaced by openness. Norms are changing and millions of people are willing to give up some privacy to join social media sites. "Of people with an online profile, nearly 40 percent have disabled privacy settings so anyone may view it, according to a Pew Internet survey released a year ago. The percentage is probably higher today (McCullagh, 2010).

Facebook CEO, Mark Zuckerberg has already stated that Internet users don't care as much about privacy anymore and that people have gotten more comfortable sharing information, but these are all voluntary declarations. This is in stark contrast to government or corporate intrusions into our privacy; "if one can choose how much or how little to divulge about oneself to another voluntarily, privacy is maintained," ..."If another person can influence how much information we divulge about ourselves or how much information input we let in about others, a lower level of privacy exists" (McCullagh, 2010).

GOVERNMENT INTRUSION

Logically, your cell phone provider knows where you are since your phone is connected to the nearest cell tower and they would also keep a record of your location since, for example, you might be outside your normal service area and roaming or other charges might be incurred. Whether you are actually using your phone or not, as long as it is on it will continue to ping cell towers and register your location. Of course, that data can be sent to law enforcement if requested. But following you around is just a part of the legitimate service provided by the carriers and that also means they know where you live, what apps you download, and what web sites you visit. All this information is now being used by the government and law enforcement agencies.

There is a case currently before the US Supreme Court, US vs Jones, which is going to determine if police officers have the right to plant GPS tracking devices on a suspect's' car without a warrant. This case stems from a nightclub owner, Antoine Jones, who was suspected of drug smuggling. Law enforcement officers attached a GPS tracking device to his car for 28 days so his movements could be tracked. His legal team argued before the supreme Court that his 4th Amendment right which guaranteed him protection against invasive searches were violated. Lawyers for the Obama administration argued that Jones did not have a legitimate expectation of privacy because

his car was in a public place and that tracking him by this GPS tracking device was no different than tailing him, which has always been legal (Wheeler, 2011).

If the Supreme Court agrees with the government, this could be the beginning of mass unwarranted surveillance of suspects using GPS devices, but since you phone already contains a GPS device, law enforcement no longer has to physically plant a device on a suspect's car, they can use mobile tracking software unless the Supreme Court bans all warrantless surveillance when they deliver their verdict in the Jones case.

Police officers can sit in the comfort of their own stations and use this technology to watch not just one person, but many people, over long periods of time... GPS tracking can actually be quite revealing about who a person is and what they value. It can show where a person goes to church, whether they are in therapy, whether they are an outpatient at a medical clinic, whether they go to a gun range. Without police officers being forced to go before a court to obtain a "probable cause" warrant, the technology is wide open to abuse (Wheeler, 2011).

CORPORATE INTRUSION

A new method of monitoring people is going to be implemented this holiday season in shopping malls in the US. People are now being tracked by their cell phones using technology, from a Portsmouth, England based company called Path Intelligence. This new software is called Footpath and it uses monitoring units that are distributed throughout a mall or store to track the movement of customers by triangulation by the strength of their cell phone signals. The collected data is run through analytics by Path, and the results sent back to the retailers on a secure website (Gallagher, 2011). All this personal data is extremely valuable to businesses and advertisers. "There's a lot of money to be made in the largely untapped local advertising markets. A BIA/Kelsey study from March predicts that U.S. local online ad revenues will reach $42.5 billion annually in 2015" (Goldman, 2011).

OnStar is basically a cell-connected device on cars (it actually uses Verizon's cell phone CDMA network) and provides various services including turn-by-turn navigation and emergency services. Recently, reports have also emerged that OnStar changed their privacy policy and has reserved the right to track and sell information about a vehicle's location and speed even after the driver cancels service. This is the same type of information that privacy advocates have complained the government is seeking to collect in the Jones case, now before the Supreme Court. "With computers, it's now so simple to amass an enormous amount of information about people that consists of things that could have been observed on the streets" (Wilk, 2011).

Facebook is also reportedly building a phone with the social network integrated at the core of its design. This phone will reportedly run on a Facebook-tailored version of the Android operating system (Castillo, 2011). With Facebook having hundreds of millions of registered users, many people see a huge security-related problem emerging with this new phone.

CARRIER INTRUSION

Earlier this year, the Apple iPhone was found to have software on it which secretly recorded the location of the user. Security researchers found a hidden file which recorded everywhere the user had been and this could be combined with other software to generate a map of the user's movements. Of course, Apple denied it was being used to track users and blamed a bug in the software but they did release a fix for it. However, the fix now only stores one week of data and no longer automatically downloads this data to a computer whenever the owner connects the phone to their computer. Users can also now disable location services for the iPhone to stop storing their location (Cellan-Jones, 2011). However, disabling location services reduces the functionality of your phone since many social media applications use these services to keep users connected.

Recently, 25-year-old Trevor Eckhart of Connecticut found a piece of software called Carrier IQ. This software records the total user experience presumably so phone manufacturers and carriers can improve the quality of service for these devices. In a video he released, he showed that the software was logging everything including text messages and even encrypted web searches. The video shows the software even logging his online search of "hello world" even though he was using the HTTPS version of Google, which theoretically is supposed to hide

searches from those who would want to spy by intercepting the traffic between the user and Google. The software logs each number as he touches the dialer and every button that is pressed. The data, including the content of the text message is sent to Carrier IQ servers. Carrier IQ claim their software is for "gathering information off the handset to understand the mobile-user experience, where phone calls are dropped, where signal quality is poor, why applications crash and battery life." However, the software cannot be turned off except by rooting the phone, (installing alternative software after removing the manufacturer software) something the average user would not likely be doing and users aren't even given the option to opt out of Carrier IQ (Kravets, 2011b).

Carrier IQ recently admitted that their software is installed on more than 150 million smartphones and has "the capacity to log web usage, and to chronicle where and when and to what numbers calls and text messages were sent and received. The software also monitors app deployment, battery life, phone CPU output and data and cell-site connectivity, among other things". They however claim that they are not logging every keystroke but do admit that they do send some website addresses to carriers as a diagnostic tool and since the URL comes directly from the phone they are able to record even encrypted search terms (Kravets, 2011c).

In a digital world, information is valuable, so now providers have begun to sell all this collected information to the highest bidder. Verizon Wireless recently changed its privacy policy "to allow the company to record customers' location data and Web browsing history, combine it with other personal information like age and gender, aggregate it with millions of other customers' data, and sell it on an anonymous basis". This type of data could be valuable to businesses who are now able to purchase a marketing report from Verizon, but to be fair, Verizon is the first provider to publicly confirm that they are selling data. All four national carriers (Verizon, AT&T, Sprint and T-Mobile) use aggregated customer data to help third parties sell ads to their customers therefore all carriers are using this as a revenue stream, although AT&T, Sprint and T-Mobile claim they never actually hand over subscriber data (Goldman, 2011).

POSSIBLE INTRUSIONS

Nobody knows for sure if the government, through the National Security Agency, is secretly collecting electronic communications without warrants. However, the Electronic Frontier Foundation alleges this is the case in a lawsuit they filed based on information given by a former AT&T technician Mark Klein, who demonstrated that AT&T had installed a secret spying room in an Internet hub in San Francisco (Kravets, 2011).

Stingrays are another high-tech tool that is used by the government. These devices, about the size of a suitcase, are designed to spoof a legitimate cell tower and are set up as a trap to capture your phone signal and communications. The government maintains that stingrays are legitimate tools of law enforcement since Americans do not have a legitimate expectation of privacy for data to and from cell towers to phones or other wireless devices. "While the technology sounds ultra-new, the feds have had this in their arsenal for at least 15 years, and used a stingray to bust the notorious hacker Kevin Mitnick in 1995" (Kravets, 2011). Stingrays can locate a mobile phone even when it is not being used. Since they spoof cell phone towers, they can intercept and record "the unique ID numbers, traffic data and the location of the device before sending it on to a real cell phone tower" (Network World, 2011).

The U.S. government also has a border search policy. This allows Customs and Border Protection agents to seize and search a laptop or other electronic device belonging to anyone crossing a U.S. border. They can search through files on laptops, phones or other mobile devices, read any files, email or view digital snapshots without needing any specific reason. The 9th U.S. Circuit Court stated that searching through a laptop is no different than looking through a suitcase therefore there is a 'border exception' to the Fourth Amendment (Kravets, 2011).

The Patriot Act gives the government the power to acquire phone, banking and other records using what is called a "national security letter," and this does not require a court warrant. These are written demands from the FBI that compel Internet service providers, banks and other financial institutions and others to hand over their confidential customer records, and this could be anything from subscriber information, to phone numbers and e-mail addresses, or bank records and perhaps even websites you have visited. The FBI only needs to claim in writing that the information is "relevant" to an ongoing national security or terrorism investigation. People who get a national

security letter are prohibited from even disclosing that they received one. "More than 200,000 letters have been issued by the FBI, despite a series of stinging reports from the Justice Department's internal watchdog, who found FBI agents weren't just routinely sloppy; they also violated the law" (Kravets, 2011).

Governments also have their own spyware that they use, the version used by the FBI is called CIPAV. If the FBI convinces someone to install it by clicking a link or opening an attachment, the program sends back a report on everything done online. In Germany, a similar program was reported to be able to turn on a computer's camera and take screenshots and there are reports of a surveillance company that states it has the ability to infect a computer using a fake iTunes update, and this company sells this product to governments around the world (Kravets, 2011).

In the US, the law allows the government to obtain email messages without a warrant, if those messages are stored on another company's servers for more than six months. However, this Electronic Communications Privacy Act, is 25 years old, having been adopted in 1986, and at that time six months would have been an extremely long time for storing email and those email messages would be considered abandoned but today most people have email messages that are many years old. "A proposal to demand a court warrant for any and all e-mail never got a Senate hearing and was opposed by the Obama administration" (Kravets, 2011).

CONCLUSION

The ubiquity of smartphones has given the mobile carriers a wealth of marketable data since smartphones are personalized devices that know more about their owners than any other product on the market. The customers are now the products that the wireless providers are selling, using the playground of the wireless environment to attract people and then sell those people to advertisers where there is a substantial fortune to be made (Goldman, 2011).

The future of computing is mobile but the fact is that the phone in your pocket records almost everything. Special software developed by private companies can record all you do and send it to the carriers. The carriers also keep just about everything you do including text messages and call-location data but none of these carriers actually reveal what data they collect or how long they store it. Law enforcement doesn't even have to provide probable cause to a judge to get historical data or real-time tracking data (Kravets, 2011).

But if the government can track you by your phone, then so can anyone else by installing tracking software, and sometimes physical access to the phone is not even needed, just the type of phone, your carrier and your phone number is sufficient. Many companies even market tracking software to allow a parent or spouse to track location and communication on a smartphone. A spouse can install a tracking device on a jointly owned vehicle and this is not an invasion of privacy according to a New Jersey appellate court, therefore the same should apply to jointly owned phones. In addition, many apps especially Android apps, ask to allow tracking your location even if there is no need for this (Gatto, 2011).

The Obama administration claimed before the Supreme Court that Americans have no right to privacy in their public movements. This allows law enforcement agencies to track anyone and engage in round-the-clock surveillance for any period of time meaning they can collect vast amounts of information about anyone. If the government knows your location and knows who you are by using cell phone tracking, this can "reveal our private associations and relationships with one another. The government could make note of whenever people being tracked crossed paths or spent time together, showing who our friends, associates and lovers are" (Network World, 2011).

Combine all this with other possible intrusions such as the border exception, the Patriot Act, the use of stingrays or the simple fact that your email has been on another company's server for more than six months and it is easy to see that although smartphones provide an invaluable service and keep the modern world connected, this also means that we all now have zero privacy.

AUTHOR INFORMATION

Professor Chris Rose, DBA, teaches at Capella University, USA. E-mail: christopher.rose@capella.edu

REFERENCES

1. Castillo, M. (2011, November 23). Facebook Phone Code Name Is Buffy, But We're Not Slayed Yet. Portfolio.com. Retrieved 11/29/2011 from http://www.portfolio.com/views/blogs/the-tech-observer/2011/11/23/a-year-after-first-reports-emerge-facebook-makes-deal-with-htc#ixzz1es7kQUTy
2. Cellan-Jones, R. (2011, May 5). Apple acts on iPhone tracking bug. *BBC News*. Retrieved 11/29/2011 from http://www.bbc.co.uk/news/technology-13292313
3. Gallagher, S (2011, November 25). We're watching: malls track shopper's cell phone signals to gather marketing data. Ars Technica. Retrieved 12/1/2011 from http://arstechnica.com/business/news/2011/11/were-watching-malls-track-shoppers-cell-phone-signals-to-gather-marketing-data.ars
4. Gatto, K. (2011, November 21). Is it legal for your cellphone to track you? MSNBC.com. Retrieved 11/28/2011 from http://www.msnbc.msn.com/id/45394735/ns/technology_and_science-security/#.TtGoqtV81VI
5. Goldman, D. (2011, November 1). Cell phone companies selling personal data. *CNN Money*. Retrieved 11/29/2011 from http://www.chicagotribune.com/business/technology/ct-biz-cell-phone-selling-personal-data-110111,0,7594011.story
6. Kravets, D. (2011a, November 24). 9 Reasons Wired Readers Should Wear Tinfoil Hats. Wired.com. Retrieved 11/30/2011 from http://www.wired.com/threatlevel/2011/11/reasons-to-wear-tinfoil-hats/
7. Kravets, D. (2011b, November 29). Researcher's Video Shows Secret Software on Millions of Phones Logging Everything. Retrieved 12/3/2011 from http://www.wired.com/threatlevel/2011/11/secret-software-logging-video/
8. Kravets, D. (2011c, December 2). Carrier IQ Admits Holding 'Treasure Trove' of Consumer Data, But No Keystrokes. Retrieved 12/4/2011 from http://www.wired.com/threatlevel/2011/12/carrier-iq-data-vacuum/
9. McCullagh, D. (2010, March 12). Why no one cares about privacy anymore. *CNet News*. Retrieved April 5, 2010 from http://news.cnet.com/8301-13578_3-20000336-38.html
10. Network World (2011, November 14). Do you give up a reasonable expectation of privacy by carrying a cell phone? Networkworld.com. Retrieved 11/30/2011 from http://www.networkworld.com/community/node/79173
11. Sprenger, P. (1999, January 26). Sun on Privacy: 'Get Over It'. Wired.com. Retrieved 12/4/2011 from http://www.wired.com/politics/law/news/1999/01/17538
12. Wheeler, B (2011, November 22). How much privacy can smartphone owners expect? *BBC News*. Retrieved 11/29/2011 from http://www.bbc.co.uk/news/magazine-15730499
13. Wilk, J. (2011, November 22). Does What Happens in Your Car; Stay in Your Car? Maybe not, say OnStar and the Washington, D.C. Police Department. JDSupra. Retrieved 11/29/2011 from http://www.jdsupra.com/post/documentViewer.aspx?fid=294168b0-8103-40e4-a292-96fde001c7ac

NOTES