PRISM, the Breadcrumbs of your Political Dissent, and the Economics of International Travel with Mobile Devices

6 critical things you need to know before you take your mobile devices out of the U.S.

Recent developments out of Washington concerning smart phone privacy have us wondering just what our government knows about us and most importantly, what they are doing with that information. Ideally, PRISM, the covert collaboration between social media companies, the NSA and FBI, is merely a necessary intrusion to ensure we don't have another WTC 911 disaster. Much of what is done with the information on your device usage is uncertain, but what is certain is that PRISM did not just happen overnight. According to official government documents, the program has been in effect since 2007, and as far back as 2003, evidence of collusion existed between AT&T and the NSA in an effort dubbed "Room 641A."

Located in San Francisco, Room 641A allegedly splits Internet backbone traffic and routes it to a separate room – known internally as SG3 – where the NSA has access to Internet surveillance and user analytics on a massive scale. In the 2006 class-action court case Hepting vs. AT&T, plaintiffs alleged that the NSA had conducted "warrantless eavesdropping with the cooperation of telecommunications companies." The Hepting vs. AT&T (and the U.S. government) case was terminated before making it to Supreme Court review.

Another high-profile case known as the "DSK case," so named after the former head of the International

Monetary Fund Dominique Strauss-Kahn, was world renown for the number of headlines made across the globe. Strauss-Kahn was accused of rape and attempted murder of a hotel housekeeping attendant. Millions tuned in to media broadcasts to soak up the sex scandal and subsequent downfall of the high-profile IMF managing director and potential political rival to French President Nicolas Sarkozy. Equally compelling was the collapse of the prosecution's case, described by many legal analysts as "shocking" and "stunning." The DSK case was eventually dismissed.

The mass publicity was not the big story here however. Conspiracy theorists suggest Strauss-Kahn was set up by Sarkozy, a speculation that has never been proven. From a mobile technology perspective, the

most compelling aspect of this case that made few headlines was Strauss-Kahn's missing smartphone. It is known that he had several phones in his possession that night, but his IMF work smartphone was the one that disappeared. As Dr. Vivian Norris, PhD blogged shortly after the case, "the future of, well, the world's economy was all in that cell phone." Strauss-Kahn's smartphone was never recovered.

The Obama administration issued a statement shortly after PRISM was exposed assuring U.S. citizens that "nobody is listening to your phone calls; that is not what this program is about." The good news for U.S. citizens is that we still have some rights to privacy and a platform with which to debate the issue. However, privacy rights notwithstanding, we have only created a pinhole of visibility to the capabilities of governments with high-powered surveillance technologies, and the information they have detailing our daily lives, all captured from our phone records. "Right to privacy" is undergoing a metamorphosis before our very eyes, but there is little that governments – ally and adversary – want us to see about their capabilities. And in a time when social media has the power to bring down a political regime (see Egypt 2011), all governments are leveraging technology to protect their respective sovereignties. With the proliferation of high-powered mobile technologies, it is certain that political battles (and possibly full-on shooting wars) will be waged leveraging smartphones and tablets.

Virtual political activism has made you an international target

The rise of this so-called virtual political activism is creating a new playing field for political parties around the globe; some of which are actually embracing the social awareness opportunity. Less objective political regimes however, approach social messaging and awareness with skepticism and paranoia and the impact to you Mr/s. International Traveler, is significant. To these political factions, every one of us is considered a political dissenter, all communications watched because there is no better way to learn what you do and your views on any topic than to spend a few minutes intercepting and storing the communications emanating from your smartphone or tablet. The moment you step foot in these countries you become suspect, the

breadcrumbs of your "political dissent" contained inside your mobile device and slowly but surely, spread through the mobile networks in the country that you're visiting.

Some governments are known to be more aggressive than others in targeting international travelers' mobile devices. Evidence from a series of cyber-attacks against U.S. banks in September of 2012 has been traced back to Saudi Arabia, and China is said to be building an army of cyber soldiers, grabbing recruits straight from college.

U.S. allies can also be added to this list. On the heels of the PRISM revelation, the Guardian newspaper also announced that at the London 2009 G20 summit, a forum for the world's 20 largest national economies, the U.K. intercepted phone and laptop communications from allies Turkey and South Africa. Many of the devices that were hacked had accessed WIFI networks at phony internet cafés that had been set up by British Intelligence.

If the US and Great Britain are setting up these mobile device snares, it is a safe wager to bet that nearly every international government is tracking

mobile devices in some way and that at least a few of these governments are strong-arming device manufacturers to share intelligence data (specifically metadata) without users' knowledge. Case in point is Saudi Arabia's handling of its inability to access metadata from RIM's BlackBerry Messenger Service (BMS). In an apparent condition of doing business in Saudi Arabia, the middle-eastern government told RIM to provide BMS access by X date, or they would order the carriers operating in the Kingdom to remove RIM devices from their networks. RIM has since complied with the government's information sharing orders and is currently allowed to distribute BlackBerry devices in Saudi Arabia.

Negligence too can be a culprit. India, an IT outsourcing superpower, has done little during the past few years to police cyber threat within its own borders where cyber-attacks have exploded from less than 5,000 in 2005, to more than 20,000 in 2012. India appears to be the wild west of cyber lawlessness, described by government leaders as an "anarchic new world of constant and undeclared cyber threat." With the number of Western company executives traveling to India to manage outsourced contracts, this country is probably one of the largest potential mobile device snaring points, second only to China.

The economics of mobile device intrusion and why mobile is so vulnerable

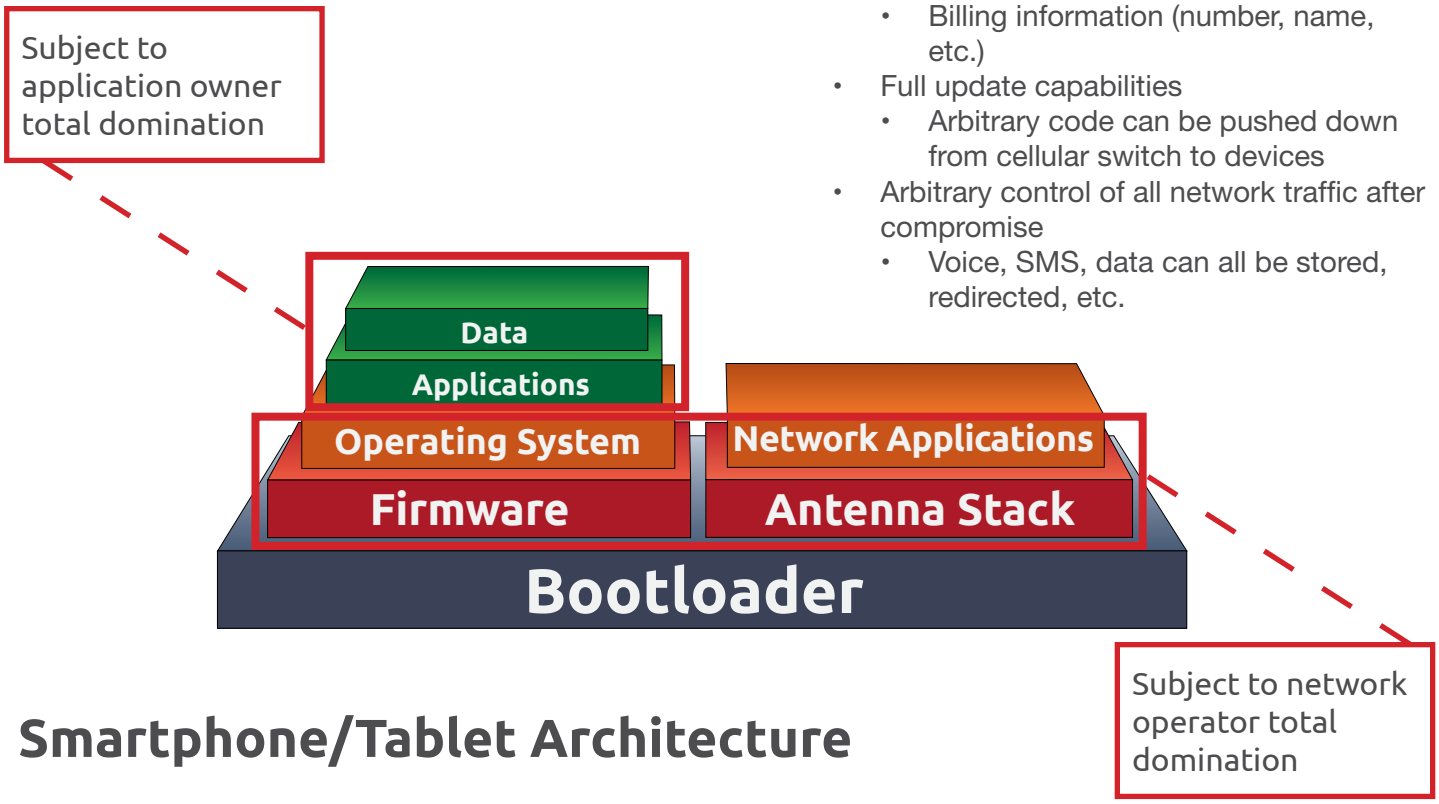
Looking for political dissenters is a pretty good reason for authoritarian governments to track international travelers' mobile device usage, but it isn't the only reason. Without a doubt, tracking mobile devices to protect the fatherland ranks high on a regime's priority list, but there's just no money in it. If you are a regime with a struggling economy and you need capital to stay in power, one of the quickest paths to revenue is to steal as much intellectual property (IP) as possible and use that IP to create new economic opportunities.

The continued evolution of mobile device technology (it is the ultimate microcomputer) makes the international business traveler's mobile device a prime target for a foreign regime looking to steal and monetize IP. But it is the very nature of keeping mobile device technology secure that makes it highly vulnerable to cyber-attack. For example, mobile device operating systems are often out of date as updates are not as easily pushed to the device as other network components.

Also the patch process can be very complex, involving multiple hardware and software vendors who must work together to arrive at a patch version, and who then have to submit the patch to the carrier for testing, debugging and pushing to consumers' devices. It can be weeks before a simple security patch is made available to consumers. Manufacturers are sometimes the main hindrance in the supply chain for security updates as it is not uncommon for them to discontinue smartphone patch support 12-18 months after release. This is mainly due to the economics of the rapidly evolving smart device market – there just isn't money to be made in properly maintaining the security patches on devices that have already been sold.

However, the most critical mobile device attribute that makes it a prime target for a regime or malicious operator to steal IP may have been created by the U.S. government. The Communications

Figure 1.



Smartphone/Tablet Architecture

Assistance for Law Enforcement (CALEA) Act of 1994 required telecom operators and manufacturers to build in wiretap, trap & trace and other surveillance technology to assist law enforcement to track criminals through their mobile devices. Ironically, the technical architecture that was borne from CALEA-driven requirements makes mobile a prime attack channel. (Figure 1)

As we see in the mobile/smartphone architecture diagram in Figure 1, there are several layers or "roots of trust" in the base architecture. These layers provide several options for a hacker to compromise the device from the bootloader to the top of the stack where the data/IP resides. The most nefarious of attacks will come from the rogue mobile carrier overseas. The rogue carrier circumvents any defense mechanisms deployed at the firmware or OS layer and has access to your device and any networks your device connects to at all times. The only protection from a rogue carrier is to construct a barrier between the device and the carrier, a piece of hardware separated from the device with an encrypted token. IntegriCell Group has such a device, a hardware token called KeyLime (it looks like and is the size of a lime wedge). IntegriCell Group is also working on a high-integrity handset designed to thwart different classes of attacks called Anvil.

The bottom line is that your mobile device or tablet is the conduit to your organization's IP, and the very nature of its architecture makes it a security liability. In terms of OS updates, patches, and security software, it is often last thought of or worse case, the forgotten network infrastructure device. Yet, it is a device that is always connected to your network and the perfect portal for extracting IP for sale to the highest international bidder.

What does this mean for you, the frequent or occasional international traveler?

1. Social media awareness is creating movements of dissent in countries abroad and the movement is strong enough to bring down political regimes. Countries viewing social movements as threatening are skeptical and paranoid, and they are stealing data in part to protect their regimes.
2. Add international governments – adversary and ally – to the overflowing pool of hackers trying to attack your mobile device to steal your data and access other networks you connect to.
3. Because of your connection to social websites and hence social's virtual activism, you are a target the moment you connect your device abroad. And since your mobile device tells the best story about who you are, what you do and your political preferences, governments abroad want access to you through your devices. In addition to intelligence gathering, there are open markets where data like contact lists and usernames and passwords are openly bought and sold among organized criminals for use in spearphishing attacks and other forms of cyber-attacks.
4. As much as we love their clever TV commercials, your wireless carrier is sitting this fight out. You are on your own when you leave your carrier's coverage area. In fact, your carrier would rather keep you in the dark about the threats of traveling with your mobile devices abroad because many overseas intrusions originate from malicious carriers in disguise. Even the "trusted" carriers are pressured by governments into providing some intelligence metadata on your device usage.
    a. A carrier-originated intrusion is nearly indefensible because the carrier accesses your mobile device at the base root of your device's architecture, underneath the software and firmware layers (Figure 1) where all security software resides.
5. In nearly every intrusion, you will not know your smartphone or tablet has been compromised by hacker or worse yet, the government of the country you are visiting. Often their MO is gain access, take your data, and destroy the device to kill the evidence trail, but probably not before…
6. They attack the organization you work for. Many times after gaining access, your attacker will go quiet, observe, and collect information about what you do online and how you do it. Then, they will go through the door you left wide open into the most secure parts of your organization's IT network. In terms of financial risk, your enterprise has the most to lose here.

What can you do about being hacked while traveling internationally?

1. If you just don't care, you could tell your boss or client "sorry, risk too great to my organization, my people can't travel overseas." Obviously not a good choice.
2. Add a security software package to your mobile devices.
    a. There are many good products out there but unfortunately, hackers are also software coders

so you are still going to be very vulnerable with this option.

b. Also, remember that software-based controls will never be effective and reducing the risks associated with malicious carrier attacks, since carriers can attack from the bottom-up.

3. Add security to a hardware component on your devices separated from the software, on a SIM card perhaps.
   a. Another very good option, but unfortunately the SIM hardware is still a device component with firmware and software that is connected to the OS of the device. You are still vulnerable if a rogue mobile carrier is the attacker, which is very common overseas.
4. Abstract the wireless access point from your devices with a piece of hardware that has a secure token only accessible to the device owner. Because this hardware-based token is an abstraction and not integrated into the phone/tablet's architecture, a malicious carrier could only gain access to your devices through the hardware token. This is the most secure way to travel internationally and ensures a locked down mobile device.
   a. This hardware device should be universal for all phones regardless of OS.
   b. There is now an IT security product for your mobile devices available from mobile security solutions provider IntegriCell Group. The device is called KeyLime. Visit www.integricell.com for more information on KeyLime.

Conclusion

Smartphone and tablet technology is revolutionizing the way we work. We are connected to our organizations' servers 24/7/365, downloading e-mail, sending/retrieving files, essentially using these devices as if they were computers connected to our enterprise networks. From the users' perspective these devices are serving as functional network workstations, but from most network enterprises' security perspectives, these devices are just phones. With this mentality, senior IT managers are missing an opportunity to shore up all avenues of network intrusion. Some organizations do understand mobile device vulnerability. These "security aware" organizations are taking measures to stave off the threat, but their numbers are few, and they are the minority. The majority of vulnerable enterprises is reactive to mobile/tablet threat and those CIOs are only able to take action after breach. The problem with this approach is that it only takes one breach to end a career and make CxOs a cyber-news headline.

Exacerbating the problem, mobile carriers do not want you to know how dangerous it is to travel overseas with mobile devices. There seems to be an out-of-sight-out-of-mind mentality to a problem that is just too technologically overwhelming to solve. Or perhaps, the issue of multiple-party (manufacturers,

software vendors, carriers, etc…) collaboration is too overwhelming to solve the problem holistically. Whatever the case, CxOs do not have the luxury of waiting for the carrier/manufacturer collective or the government to protect your IP when your co-workers are traveling overseas.

The IP loss numbers are staggering:

- $1 billion theft in R&D IP at Fortune 500 company that wishes to remain anonymous
- $10 billion theft in R&D IP at Fortune 200 company that wishes to remain anonymous
- Lockheed Martin: $3 billion lost in IP theft
- These are just a few of the known IP thefts, yet there are countless others that never make it out of corporate board rooms.

You and the organization you work for have the most to lose. The time to act is now.

About IntegriCell

IntegriCell delivers mobile security solutions and consulting services that provide insight to advanced persistent threats (APTs) that impact enterprise organizations, government agencies and end-user consumers. IntegriCell's featured mobile security products are KeyLime, a universal hardware device for mobile security, and SyncDog, a software solution that correlates phone message logs to reveal patterns of user behavior indicative of cyber threat. The roots of IntegriCell date back to the early days of information security at Microsoft where IntegriCell founder Aaron Turner served as security strategist. Turner eventually landed in research and development at the U.S. Department of Energy's Idaho National Laboratory, where significant research into cross-domain cyber security vulnerabilities has been conducted for more than a decade.

Originally a services company, IntegriCell's professional services offerings are designed to be accelerated knowledge-transfer engagements targeting enterprise risk managers, network operators, infrastructure managers, government entities and law enforcement. For more information on IntegriCell, please visit http://integricell.com.

The KeyLime system protects smartphones and tablets by creating an encrypted protection barrier between the device and rogue carriers and malicious operators.

INTEGRICELL

IntegriCell, Inc. | **www.integricell.com**

455 Massachusetts Ave. NW
Suite 430
Washington, DC 20001

Contact:
Phone: +1-208-360-3746
E-mail: contact@integricell.com

Fax: +1-208-621-3947
Support: support@integricell.com