Mobile Device Security:
Has Your Client's Smartphone Been Hacked?

by Clark Walton, JD, CCME
Managing Director, Reliance Forensics, LLC

If you're a litigator, cell phones can be a powerful tool in discovery. They may contain a client's (or opposing party's) text messages, e-mails, GPS data, personal photographs, social media, data files and let's not forget - they also contain phone call records. Modern smartphones do so many things, it's easy to forget that these phones are actually, well, phones.

As if we didn't feel the need for privacy in the phones we carry around already, the U.S. Supreme Court recently cemented the individual's privacy interest in their cell phone in *Riley v. California,* decided in June 2014. *Riley* generally stands for the principle that a warrant is needed when phones are searched by the government incident to an individual's arrest.[1] The opinion in the 9-0 decision written by Chief Justice Roberts in large part speaks to the richness of personal data accessible on these phones.[2]

So, it's natural that someone adverse to your client may have something to gain by accessing smartphone data. But is it even possible? Tell me if you've heard the following before: A client or potential client walks into your office and says "my [ex-boyfriend/spouse/business partner] is monitoring my phone. They hacked it. I'm sure because... [Insert reason here]"

If you practice family law, employment law or business litigation, you've quite possibly heard this more than others. Recent press coverage, from the Edward Snowden disclosures on National Security Agency snooping to the British phone hacking scandal involving the downfall of "The World" newspaper, have brought the possibility of phone surveillance to the forefront.[3]

When your client raises the issue, is it paranoia and the dreaded "CSI effect" brought about by all of this media coverage? Or is it something worthy of further investigation? The following are a few points to consider.

---

[1] *Riley v. California*, U.S. Sup. Ct., No. 13-132, decided June 25, 2014, located at http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf, last visited on July 8, 2014.
[2] *Id.*
[3] *See* "Phone hacking scandal: Timeline", BBC News UK, located at http://www.bbc.com/news/uk-14124020, last visited July 8, 2014. *Also see* "Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction", posted June 26, 2013, located at http://www.odni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction?highlight=YTo4OntpOjA7aToyMTU7aToxO3M6NzoicHJvZ3JhbSI7aToyO3M6MTE6InByb2dyYW1taW5nIjtpOjM7czo4OiJwcm9ncmFtcyI7aTo0O3M6ODoicHJvZ3JhbSciO2k6NTtzOjk6InByb2dyYW0nLiI7aTo2O3M6OToicHJvZ3JhbSdzIjtpOjc7czoxMjoiMjE1IHByb2dyYW1zIjt9, last visited on July 8, 2014.

1. Technically Yes, A Cell Phone Can Be Compromised, or "Hacked"

Smartphones are extremely powerful computers. Your personal smartphone actually has more computing power than the computers used by NASA during the Apollo space missions.[4] And, unfortunately, just like other modern computers, smartphones are susceptible to cyber threats.

Viruses are prevalent on the Android operating system, for instance. An Android phone can receive an unsolicited text message saying "Buy Viagra here", the user clicks on the link in the message, and just like that, the phone is infected with malware. There are even free antivirus tools available for download to scan for and mitigate these threats on your phone, just as there are for traditional computers.[5]

If you or your client are interested in reading further on how to prevent malicious code from infecting a smartphone in the first place, the United States Computer Emergency Readiness Team (US-CERT) has published guidelines on measures that an individual can take to mitigate the risks of their smartphones to malicious code, such as not visiting certain types of web sites, and not connecting to unknown networks.[6]

The point being here, yes, it is possible for a smartphone to become infected with malicious code that may do bad things, including stealing your client's information and monitoring their whereabouts.

2. There Could be Malicious Code on the Phone

Some smartphones are more susceptible than others to cyber threats. Android-based devices are far more likely to contain malicious code than Apple devices because of the ability of bad actors to publish Android applications, or “apps”, that are very similar to legitimate apps. Android apps are not as strictly controlled as Apple iOS apps.[7] A bad app may do various things on the phone, such as activate the microphone, steal passwords, or intercept e-mail communications or banking data. A mobile phone forensics expert should be able to scan an Android phone and detect such malicious code if it has a known attack signature. [8]

iPhones, on the other hand, while in theory vulnerable, are generally not as susceptible to malicious code attacks in the wild. A large part of this is due to the tighter control Apple exerts over its App Store and

---

[4] *See, e.g.,* “Do It Yourself Podcast: Rocket Evolution”, NASA Web Site, located at http://www.nasa.gov/audience/foreducators/diypodcast/rocket-evolution-index-diy.html, last visited on July 8, 2014.

[5] "AVG Antivirus FREE for Android Mobiles", available at http://www.avg.com/us-en/antivirus-for-android, last visited on July 8, 2014.

[6] Ruggiero, Paul and Foote, Jon, ““Cyber Threats to Mobile Phones”, US-CERT Web Site, available at https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf, last visited on July 8, 2014.

[7] Tung, Liam, "iOS v. Android: Which is more of a security threat for the enterprise?", ZDNet, posted on June 18, 2014, located at http://www.zdnet.com/ios-vs-android-which-is-more-of-a-security-threat-for-the-enterprise-7000030668/, last visited on July 9, 2014.

[8] See, e.g., “Cellebrite Partners with Bitdefender to Deliver Comprehensive Joint Mobile Malware Detection with Mobile Forensics”, posted December 17, 2012, located at http://www.bitdefender.com/news/cellebrite-partners-with-bitdefender-to-deliver-comprehensive-joint-mobile-malware-detection-with-mobile-forensics-2721.html, last visited on July 9, 2014.

the contents of the store.[9] Of course, if you "jailbreak" your iPhone and allow unapproved and un-vetted apps to be installed, all bets are off and you're more vulnerable (and you've likely voided your Apple warranty in the process).[10] If a client comes to you believing their phone has been hacked and they've got a new iPhone, be skeptical, but it's still possible their phone has been compromised.

3. It May Be Carrier Monitoring or Other "Legitimate" Monitoring Software

Every major wireless phone carrier in the United States sells some type of monitoring service to users with their wireless plans. They may monitor usage, content, location, or any combination thereof. Verizon has "Family Locator", AT&T has "AT&T FamilyMap", and Sprint has its bundled "Sprint Guardian" program.[11] The technical capabilities are certainly there from the carrier's perspective to conduct many types of monitoring on smartphone data. And if your client is on a "family" plan with someone else, especially if they aren't the primary account holder, it's possible that legitimate carrier-based monitoring has been implemented on the client's phone.

Other third party companies also sell monitoring software as their business, which on certain types of phones is transparent to the phone's end user. These vendors assume buyers of their software have the authority to monitor such end users (such as a parent's minor child).

The presence of such software on the phone will likely *not* be detected by phone "malware" scanners. It isn't because detecting such tools is technically impossible, but I would suspect, from conversations with industry experts on the subject, it is because of the possible threat of legal action by the software manufacturers for classifying their products as malicious.

Legitimate monitoring may be hidden for other reasons, for instance, if your client is the subject of a criminal investigation. There are certain tools available only to law enforcement and government entities which may allow them to monitor their targets, such as the recently publicized software "RCS" (stands for "Remote Control System") sold worldwide to governments by a technology firm in Milan, Italy.[12]

To install true spyware on a target phone without the aid of the wireless carrier, you generally need physical access to the phone itself. So there's the first question to ask a client. If they bought the phone

---

[9] Tabini, Marco, "How Apple is improving mobile app security", Macworld, posted on September 2, 2013, located at http://www.macworld.com/article/2047567/how-apple-is-improving-mobile-app-security.html, last visited on July 9, 2014.

[10] "Unauthorized modification of iOS can cause security vulnerabilities, instability, shortened battery life, and other issues", posted February 9, 2013, located at http://support.apple.com/kb/ht3743, last visited on July 9, 2014.

[11] "Verizon Wireless – Family Locator", located at https://wbillpay.verizonwireless.com/vzw/nos/safeguards/SafeguardProductDetails.action?productName=familylocator, last visited on July 8, 2014; "AT&T FamilyMap", located at https://wbillpay.verizonwireless.com/vzw/nos/safeguards/SafeguardProductDetails.action?productName=familylocator, last visited on July 8, 2014; "Sprint Services - Safety and Control - Sprint Guardian", located at http://shop.sprint.com/mysprint/services_solutions/details.jsp?detId=sprint_guardian&catId=service_safety_control&catName=Safety and Control&detName=Sprint Guardian&specialCat=, last visited on July 8, 2014.

[12] Kirk, Jeremy, "Researchers reveal mobile malware tools governments use to spy on phones", PC World Magazine online, posted on June 25, 2014, located at http://www.pcworld.com/article/2367760/police-turning-to-mobile-malware-for-monitoring-study-says.html, last visited on July 8, 2014.

in their own name only a few weeks before, and the person who they believe is monitoring them hasn't has physical access to the phone, especially if it's an iPhone, there is little chance someone is monitoring their phone. If it's a Droid, it may have malware on it, but that will likely be detectable in a virus scan. Worst case, tell the client to go buy a new phone, power down the original phone and retain it for a forensic expert to examine for indicators of monitoring.

4. "Hacking" Sounds Trendy, But Consider Other Factors

Often clients will believe they've been hacked because information they believe to be private was found out by the other party. That could include their location information at a certain point in time, who they were with yesterday, or both (i.e., the client has been on a date with someone new and the opposing party mentioned it to them).

Before rushing to judgment or spending a lot of money investigating the claim, consider other potential sources of the information. Remember, phones may feel personal, but they're constantly calling out to a network to send and receive data. Actually, that's pretty much their only job.

Your client may have posted something to social media such as Facebook or Twitter, or, one step further, others may have posted such clues that would lead a third party to your client's whereabouts. Remember, your client may control what *they* do online, but they have zero control over what their friends and family do. Once your client enters the public domain or gives information to a third party, they've lost their expectation of privacy in that information.[13]

Also consider your client's web-based e-mail. Does the opposing party know their Yahoo Mail password? Or is it easy to guess? Could the other party be able to "auto" login from a device in the home that was previously used by your client? These are also common potential avenues of third party access. And if it's an Apple device, what about iCloud? Can the other party access that information? iCloud allows users to back up text messages, photos, and other sensitive personal data. Who is able to access that?

Have the client enable two-step authentication on any such web-based accounts to prevent such attacks, most online providers are now offering that service (i.e., you try to log in, then it sends a code to your phone which you enter on the web site (step 1), and you *then* enter your password (step 2)).

Conclusion

It's quite a bit to process. There are the traditional notions we hold as to what constitutes our clients' private data, and on the other hand there is popular culture that encourages connectivity and constant information sharing. If your client thinks someone may be monitoring their information, it's important to understand the possibilities that are out there, and, if necessary, involve a mobile forensics expert. How you advise your client now may preserve valuable evidence for later use in court.

---

[13] *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).