# Technology

# Keep Your Smartphone Data Secure

## *The Rules of Professional Conduct Require Lawyers to Protect Client Information*

**BY DANIEL J. SIEGEL**

The History Channel, in conjunction with *Popular Mechanics*, recently compiled a list of the 101 All-Time Greatest Gadgets, concluding that the "smartphone" was the number one gadget that changed the world. The magazine reported that mobile phones have become the most widely used gadgets in the world, and that by the end of 2010, 75 percent of the people on earth will use the devices, which facilitate instantaneous personal connections that make phone conversations seem like cave paintings.

One observer correctly predicted in 2008 just how popular these devices would become, *i.e.*, with the advent of smartphones, lawyers will be able to do everything on the road – call, email, browse the Internet, review files, read cases, write memos, etc. — that they now do in the office. The author noted that a lawyer with a smartphone is a walking law firm. Certainly, there is little doubt that the smartphone, a generic appellation that includes iPhones, Androids and BlackBerries, have had an enormous impact upon the legal community. Just look around. Every lawyer seems to have one, and every lawyer seems to be attached to his or her phone, and the uses for these devices continues to expand almost exponentially.

As with any technological advance, smartphones pose security concerns that users should not ignore. In this column, I will highlight some of the issues raised by smartphones and offer some easy ways to be sure that the data on your phone is not stolen or otherwise improperly used by unauthorized persons.

For lawyers, the danger smartphones raise is primarily the relative ease with which data can be stolen. For matters involving our clients, these phones can be fonts of information to be discovered during litigation or administrative proceedings, ranging from domestic disputes to criminal matters to personal injury cases to almost anything else you can imagine.

> "You don't have to have a specialist to do this, it is well-documented by Google. The attacks are very simple."

The concerns are real. For example, a German researcher has demonstrated that Google's mobile phone operating system, known as Android, can easily by hacked if the user is connected to a public Internet connection – allowing all the data to be accessed. "You don't have to have a specialist to do this, it is well-documented by Google. The attacks are very simple," Bastian Könings, a security researcher at Ulm University, told *Der Spiegel*. Könings noted that all of the contacts, diary dates and even photos on a hacked phone could easily be seen and even altered – and not just when the hacker and the hacked phone are using the same network. All a potential hacker has to do is to log onto a public wireless Internet connection, such as those found in cafes, airports or hotels, and use Google's interface for external developers, he said. Google acknowledges this threat and claims to be working on solutions. But, of course, once Google solves one problem, others will almost certainly arise.

The threats are equally real for iPhones, BlackBerries and other portable devices. The iPhone, for example, is also ripe for attack. Just ask Nicholas Allegra, a 19-year-old from Chappaqua, N.Y., whose "hobby" is discovering cracks in the source code of Apple's iPhone, and then exploiting the "holes" to obliterate its defenses against hackers. "It feels like editing an English paper," Allegra told *Forbes* magazine. In fact, Allegra has twice released a piece of iPhone computer code called "JailBreakMe," which allows users to strip away in seconds the ultra-strict security measures Apple has placed on iPhones and iPads.

Blackberries and other devices are similarly vulnerable to hacking and

security breaches. Earlier this year, at the annual "Pwn2Own hacker challenge," competitors discovered a security flaw in the BlackBerry OS 6.0, which led Research in Motion (RIM), the manufacturer of the devices, to turn off JavaScript. The competitors discovered a vulnerability that could allow a hacker to access personal data from the phone.

Hacking these devices does not require a Ph.D. in computer science. In fact, the Internet is rife with websites and videos selling hacking software and demonstrating how easy it is to hack smartphones. For example, searching "how to hack an iPhone" on YouTube returns more than 23,900 results, while the same search on Google generates 30 million results. While writing this column, the number one result for this search was "Jailbreak and unlock the iPhone – Featuring Mac modding tutorials." Modifying the search to "how to hack an Android phone" resulted in 5,280 hits on YouTube, and more than 31.2 million on Google, with the top result, "How to Hack Your Android Phone (and Why You Should Bother)."

Clearly, the threats are real, and lawyers and law firms must take proactive steps to make these devices more secure. To do otherwise would be to ignore the obligation under Pennsylvania Rule of Professional Conduct 1.6 (Confidentiality of Information), which prohibits a lawyer from revealing information relating to representation of a client unless the client gives informed consent. This

# Tech BRIEFS

## Android is Most Attacked

Android phones have become the most attacked mobile operating system, according to security software provider McAfee Labs.

The amount of malicious software or malware attacking Androids jumped 76 percent from the previous quarter, McAfee said, adding that 12 million unique types of malware were discovered in the first half of 2011. That's a 22 percent increase from 2010. McAfee said Android passed Symbian as the most targeted mobile operating system in the second quarter of 2011.

"Overall attacks are becoming more stealth and more sophisticated, suggesting that we could see attacks that remain unnoticed for longer periods of time," said McAfee's senior vice president Vincent Weafer.

AT&T has already announced a mobile security plan for businesses, with a consumer version on the way next year. ■

## NLRB Backs Workers Who Complain Online

Workers complaining about their workplace on social media platforms like Twitter and Facebook may have the National Labor Relations Board on their side because they are involved in "protected concerted activity."

In four different cases, the employees were protected because they were discussing terms and conditions of employment with fellow employees, under Section 7 of the National Labor Relations Act.

The NLRB sided with a luxury car salesman over photos he posted online about a sales event. Hot dogs were served at the event, which the salesman said sent the wrong message. He said the cheap food conveyed the wrong message to his clients and he was voicing the concerns of his co-workers, who are paid on commission.

According to an article by Eric Meyer on TLNT.com, a human resources website, employers can't discipline employees who discuss

workplace responsibilities and performance together online—even if the employees swear, use sarcasm or include insults. And employees can't be disciplined for clicking "like" on Facebook.

Section 7 covers most private sector employees and applies even if the workplace is not unionized, Meyer writes. He cautions that the NLRB's position on social media has not been tested in the courts, and the legal issues are still developing. ■

## Phones Used as Shields

Cell phones are a great way to stay connected when you're away from the office or home. But according to a recent survey by the Pew Research Center's Internet & American Life Project, 13 percent of cell phone users use their devices to avoid interacting with people around them.

Other findings from the survey include:

- Eighty-three percent of American adults own some sort of cell phone.
- Half of all adult cell owners (51 percent) had used their phone at least once to get information they needed right away. One quarter (27 percent) said that they experienced a situation in the previous month in which they had trouble doing something because they did not have their phone at hand.
- Forty percent of cell owners said they found themselves in an emergency situation in which having their phone with them helped.
- Forty-two percent of cell owners used their phone for entertainment when they were bored.
- Despite their advantages, some cell phone owners just need an occasional break – 29 percent of cell owners turned their phone off for a period of time just to get a break from using it. ■

duty of confidentiality extends to "information relating to the representation of a client," and it is now commonly accepted that this duty applies to client information in computer and information systems as well.

Moreover, an amendment to Model Rule 1.6, suggested by the American Bar Association Ethics 2000 Commission and approved by the ABA House of Delegates, requires attorneys to take reasonable precautions to safeguard and preserve confidential information. The "Reporter's Explanation of Changes," notes that new Comment 16 "addresses the lawyer's duty of care when transmitting confidential information. Although much of the current debate concerns the use of unencrypted e-mail, the Comment speaks more generally in terms of special security measures and reasonable expectations of privacy. …"

Faced with the reality of these threats, and a lawyer's duty of "competence" under Rule 1.1, it is clear that an attorney's obligations apply to electronic client data on computers, mobile devices and elsewhere. Thus, the question posed is what reasonable precautions must lawyers take to protect that data.

First, as with technology itself, what is perceived to be reasonable is an evolving concept, *i.e.*, lawyers must remain familiar with any changing obligations placed on them, whether by Rule, or by state or federal law, to ensure that they comply with these changes.

Second, as technology advances occur, lawyers must periodically review their security measures to ensure that they still reasonably protect the security and confidentiality of their clients' documents and information. A breach of these duties can result in a malpractice action.

Lawyers must periodically review their security measures to ensure that they still reasonably protect the security and confidentiality of their clients' documents and information.

Third, there may be circumstances when lawyers may have contractual duties to protect client data. This is particularly relevant for lawyers with clients in regulated industries, including health care and financial services, which have regulatory and other requirements to protect privacy and security. In addition, various state and federal statutes and regulations may require protection of defined categories of personal information, including information maintained by lawyers.

Fourth, there are many ways to protect against data loss:

- Do not store information on mobile devices that you cannot afford to lose;
- Be vigilant – Do not allow these devices to be lost or stolen;
- Use "power-on" password settings, which require a user to enter a password before accessing a device. Generally, these settings also require the use of a password when a device has not been used for a specified amount of time;
- Change the default password on your devices, and make certain the password is neither simple nor obvious. Quite often, the default password on a device is the last four digits of the device's phone number, information easily determined. In fact, all journalists had to do was dial directly into the victims' phones and enter a default or easy-to-remember password, such as "1111," to gain access to their voicemails.
- Do not store important information on peripheral storage devices, such as SanDisks, because that data is generally not protected by the power-on password;
- Create a written plan specifying your firm's mobile device security policy;
- Create a written plan specifying your firm's policy if a mobile device is lost or stolen;
- Create an official policy detailing the steps your firm will take if a data breach occurs;
- Store only information you absolutely need to on these devices, e.g., do not store Social Security numbers or other personal client data unless absolutely necessary;
- Backup data on the devices to a secure location at regular intervals; and,
- Password protect documents and other items on the devices that contain confidential information.

Smartphones are extremely popular, for good reason. They allow attorneys to make phone calls, read and respond to email and text messages, browse the Internet, review files, perform legal research and much more. That is also why they are extremely popular among hackers seeking to access and use the data stored on these devices. For attorneys and law firms, the key to mobile security is being aware and taking reasonable precautions to prevent unauthorized access to the devices and unauthorized use of the information stored on them. ■

---

*Daniel J. Siegel (dan@danieljsiegel.com), editor-in-chief of The Philadelphia Lawyer, is a local attorney who operates the Law Offices of Daniel J. Siegel, LLC and is the president of Integrated Technology Services, LLC.*

Tech UPDATE


Olympus PEN EP-3


Sony NEX-C3

**TWO TINY NEW CAMERAS** from Olympus and Sony produce spectacular photos, thanks to huge sensors and interchangeable lenses. You can turn the Olympus PEN EP-3 on, focus and snap a photo in less than a second. The Sony NEX-C3, like the Olympus, takes high-definition video. Both cost more than $600, but if you're willing to pay, you'll appreciate the results.

| FEATURES | OLYMPUS PEN EP-3 | SONY NEX-C3 |
|---|---|---|
| EFFECTIVE PIXEL NUMBER | 12.3 MEGAPIXELS | 16.2 MEGAPIXELS |
| FOCAL LENGTH MULTIPLIER | 2.0 X | 1.5X |
| SENSITIVITY RANGE | ISO 200 - ISO 12,800 | ISO 200 - ISO 12,800 |
| CONTINUOUS SHOOTING | 4.1 FRAMES PER SECOND | 2.3 FRAMES PER SECOND |
| SHUTTER SPEED | 60-1/4,000 SECOND | 30-1/4,000 SECOND |
| FLASH | INCLUDED OPTIONAL | INCLUDED OPTIONAL |
| IMAGE STABILIZATION | SENSOR SHIFT | OPTICAL |
| BATTERY LIFE | 300 SHOTS | 400 SHOTS |
| DIMENSIONS | 4.3" X 2.5" X 1.5" | 4.4" X 2.4" X 0.9" |
| WEIGHT | 11 OUNCES | 10.7 OUNCES |
| PRICE | $699.99 | $649.99 |