Is Smartphone Security Good Enough?

By Keir Thomas, PCWorld

Would you object if a police officer stopped you for speeding, then took your phone and cloned all its data—including photos, videos, e-mails, and recent GPS locations?

If you get pulled over by the Michigan State Police, this might be a reality, courtesy of handheld phone cloners that are designed for forensics use but which the American Civil Liberties Union (ACLU) claims are being used by patrol officers.

The ACLU has asked to see logs for any devices used this way, and the Michigan State Police responded by demanding half a million dollars to pay for retrieving the information. The ACLU has replied with a public letter (PDF link) mentioning constitutional rights and litigation, and that's where the matter rests at the moment.

It's alleged that the police force is using CelleBrite UFED devices out in the field. The handheld tool can quickly clone the data stored on more than 3000 different phone models, even if that data is protected by a PIN. It can even access deleted data no longer accessible by the owner of the phone.

If you get pulled over by the Michigan State Police, this might be a reality, courtesy of handheld phone cloners that are designed for forensics use but which the American Civil Liberties Union (ACLU) claims are being used by patrol officers.

The ACLU has asked to see logs for any devices used this way, and the Michigan State Police responded by demanding half a million dollars to pay for retrieving the information. The ACLU has replied with a public letter (PDF link) mentioning constitutional rights and litigation, and that's where the matter rests at the moment.

It's alleged that the police force is using CelleBrite UFED devices out in the field. The handheld tool can quickly clone the data stored on more than 3000 different phone models, even if that data is protected by a PIN. It can even access deleted data no longer accessible by the owner of the phone.

If you get pulled over by the Michigan State Police, this might be a reality, courtesy of handheld phone cloners that are designed for forensics use but which the American Civil Liberties Union (ACLU) claims are being used by patrol officers.

The ACLU has asked to see logs for any devices used this way, and the Michigan State Police responded by demanding half a million dollars to pay for retrieving the information. The ACLU has replied with a public letter (PDF link) mentioning constitutional rights and litigation, and that's where the matter rests at the moment.

It's alleged that the police force is using CelleBrite UFED devices out in the field. The handheld tool can quickly clone the data stored on more than 3000 different phone models, even if that data is protected by a PIN. It can even access deleted data no longer accessible by the owner of the phone.

Would you object if a police officer stopped you for speeding, then took your phone and cloned all its data—including photos, videos, e-mails, and recent GPS locations?

If you get pulled over by the Michigan State Police, this might be a reality, courtesy of handheld phone cloners that are designed for forensics use but which the American Civil Liberties Union (ACLU) claims are being used by patrol officers.

The ACLU has asked to see logs for any devices used this way, and the Michigan State Police responded by demanding half a million dollars to pay for retrieving the information. The ACLU has replied with a public letter (PDF link) mentioning constitutional rights and litigation, and that's where the matter rests at the moment.

It's alleged that the police force is using CelleBrite UFED devices out in the field. The handheld tool can quickly clone the data stored on more than 3000 different phone models, even if that data is protected by a PIN. It can even access deleted data no longer accessible by the owner of the phone.

Would you object if a police officer stopped you for speeding, then took your phone and cloned all its data—including photos, videos, e-mails, and recent GPS locations?

If you get pulled over by the Michigan State Police, this might be a reality, courtesy of handheld phone cloners that are designed for forensics use but which the American Civil Liberties Union (ACLU) claims are being used by patrol officers.

The ACLU has asked to see logs for any devices used this way, and the Michigan State Police responded by demanding half a million dollars to pay for retrieving the information. The ACLU has replied with a public letter (PDF link) mentioning constitutional rights and litigation, and that's where the matter rests at the moment.

It's alleged that the police force is using CelleBrite UFED devices out in the field. The handheld tool can quickly clone the data stored on more than 3000 different phone models, even if that data is protected by a PIN. It can even access deleted data no longer accessible by the owner of the phone.

Would you object if a police officer stopped you for speeding, then took your phone and cloned all its data—including photos, videos, e-mails, and recent GPS locations?

If you get pulled over by the Michigan State Police, this might be a reality, courtesy of handheld phone cloners that are designed for forensics use but which the American Civil Liberties Union (ACLU) claims are being used by patrol officers.

The ACLU has asked to see logs for any devices used this way, and the Michigan State Police responded by demanding half a million dollars to pay for retrieving the information. The ACLU has replied with a public letter (PDF link) mentioning constitutional rights and litigation, and that's where the matter rests at the moment.

It's alleged that the police force is using CelleBrite UFED devices out in the field. The handheld tool can quickly clone the data stored on more than 3000 different phone models, even if that data is protected by a PIN. It can even access deleted data no longer accessible by the owner of the phone.

Would you object if a police officer stopped you for speeding, then took your phone and cloned all its data—including photos, videos, e-mails, and recent GPS locations?

If you get pulled over by the Michigan State Police, this might be a reality, courtesy of handheld phone cloners that are designed for forensics use but which the American Civil Liberties Union (ACLU) claims are being used by patrol officers.

The ACLU has asked to see logs for any devices used this way, and the Michigan State Police responded by demanding half a million dollars to pay for retrieving the information. The ACLU has replied with a public letter (PDF link) mentioning constitutional rights and litigation, and that's where the matter rests at the moment.

It's alleged that the police force is using CelleBrite UFED devices out in the field. The handheld tool can quickly clone the data stored on more than 3000 different phone models, even if that data is protected by a PIN. It can even access deleted data no longer accessible by the owner of the phone.
technical barriers to protect the data on handsets from snoopers, whether that's law enforcement or anybody else?

A lot of work has gone into protecting transmissions, but it's wrongly assumed that if a person or agency has physical access to the phone, then they can be trusted. This simply isn't the case.

Modern smartphones contain extremely personal records of our lives. If Near Field Communications (NFC) take-off then phones may literally become our wallets when we use them to pay for purchases.

It's not just about handsets. Are app creators doing enough to protect confidential data they generate? For example, geolocation apps are all the rage right now, but are they protecting the GPS data we willingly record?

I decided to do a few tests. I attached my iPhone to a fresh Windows install and, after installing iTunes and iPhone Explorer, a piece of software that makes accessible the iPhone's file system, I tried to see what I could find.

It was a shocking experience. I use the Navfree satellite navigation app, for example, and was able to easily uncover my "home" address--street name as well as latitude and longitude coordinates--as well as recently visited destinations. All of that was contained within simple text files on the iPhone. With similar ease, I was able to uncover my recent Yahoo Messenger conversations.

Remember: I was able to do all this by doing little more than plugging my iPhone into a computer via USB and installing easily available, entirely legal software. I could do the same with your iPhone, provided I have access to it for a moment or two.

In my cursory explorations I wasn't able to view e-mails, and this is probably because the iPhone incorporates Data Protection, which encrypts e-mails and any attachments. Indeed, the iPhone has encryption built into the hardware along with an application programmer interface (API) allowing programmer access to this feature, allowing theoretically easy access for apps. However, it appears few make use of it.

My iPhone isn't jailbroken but I understand that even more data is freely accessible on such phones. I doubt many people consider this when choosing to jailbreak.

To be fair, iPhones set with a passcode are inaccessible to iTunes (and therefore iPhone Explorer) unless some first enters the passcode on the device. But how many people use this feature, which can make activating the phone for use each time a slightly annoying experience?

Google Android phones are no better. Android 3.0 will bring with it some powerful encryption features, and there's talk of a new open-source project called Guardian that will add fundamental encryption to Android and could be integrated into Android devices by handset manufacturers. But right now Android phones and tablets have almost no data protection.

RIM BlackBerry phones offer a much higher standard of protection, perhaps because they're aimed at enterprise users, and there's the rub. Data encryption on phones tends to be seen as an enterprise-level feature, where it's employed to protect employer data--and often in response to legislation.

However, every level of user can reasonably demand the same level of data protection.

Modern ARM processors used in most phones have encryption routines built into them, making data protection operations very simple to integrate without requiring huge amounts of battery power. So there's really is very little reason not to encrypt data.

Systems need to change, and handset manufacturers need to start taking the issue of data security far more seriously. Ultimately, it should be impossible for anybody--including law enforcement officers--to access our data without our express permission.

Sponsored Resource: How to protect your PCs and servers in minutes.

Read more like this: data protection
It underscores the vulnerabilities of our newest technology and the opportunistic tendencies of the government. It's quite sad that you were safer with a pen and agenda book and an analog Motorola phone.

It also shows that there needs to be more laws against theft of information, if our information is not considered property than our privacy will soon become worthless.