App to remotely wipe phones leaves police in tech arms race with thieves

October 14 2014, by Andrew Smith

Credit: AI-generated image (disclaimer)

Police play a proverbial cat-and-mouse game with those they pursue, but also with the technology of the day they use. This game of one-upmanship, of measure and countermeasure, sees one or the other side temporarily with the upper hand.

For example, some years ago some UK police forces introduced a device that could read and download data from a suspect's smartphone. However, more recently it's been found that phones in police custody are being remotely wiped by their owners. This is embarrassing for any police force, and demonstrates how technology designed to reduce crime can also be used to potentially cover it up.

Tracking tool

There are now several different ways to track your smartphone. Apple's Find Your Phone service helps its customers find their iPhone, whether mislaid or stolen – and this can provide police with useful information about whether a crime has been committed and the possible location of the phone and possibly the perpetrator. Other third-party apps and services such as Prey can, and have, helped owners locate their stolen possessions.

Some police forces have commended these tools, others aren't geared up to react to the opportunities technology has provided. However, if your phone is not passcode protected or biometrically locked, then it's inevitable that, if stolen, a thief can access some of your personal data as well as wipe the phone for their own use. That's why these locator apps offer the ability to connect to the phone and wipe it of any sensitive data.

Double-edged sword

Such remote control possibilities are a double-edged sword, however. Imagine if, as a junior gang member, you realise that your confiscated phone now in the hands of the police (containing all manner of contacts and incriminating evidence) is still visible via iCloud or some other service. This is good news for you and the gang, less so for the police.

One of the key tenets of digital forensic practice is that all law enforcement officers are trained to not switch off any device, as investigators need to capture the state of the phone as it was received, both stored on flash disk or drive and in volatile memory (RAM). All computer systems – and this includes smart phones – contain temporary information that may be crucial in an investigation. There's also the possibility that a phone may require a passcode on restart that the police don't have.

Worse, with Apple's iPhone iOS 8 operating system and the new iPhone6, Apple has improved its encryption, enabling it by default and no longer storing the encryption key on its servers. This has temporarily thwarted law enforcement's ability to easily subpoena Apple for access to its customers' data stored in the cloud and made it much harder to access data on the phone even with physical access to it.

If an officer is not able to get a phone into a protective bag in time, our suspect may be able to track their phone, wipe data, and hamper police enquiries. These bags operate as a Faraday cage – blocking the phone network's microwave radio signals (a form of electromagnetic radiation), from reaching the phone. The challenge for law enforcement officers is to get the phone to a secure location or one of these bags before the phone is remotely wiped. In a pinch, a microwave oven will do as well.

Traces

However, there are always traces left behind. You or I might be happy knowing that the thief has not got access to the social media accounts, email, online banking or personal photos on the phone – and wiping any lost device clean would be good enough for most. But much of the data that passes through our phones, the online services used and the networks they connect to, leaves behind traces or even copies of it behind in the cloud that forensic digital investigators can retrieve.

Increasingly, as more and more data is stored in the cloud, indirectly or directly as back-ups, it's harder and harder to be "lost". Any advantage now will only be temporary as police and legislators find new ways to keep one step ahead of the criminals. On the internet, there's very little that's hidden forever.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation