NOW LOOK, BOND, IT'S OUR BEST GADGET YET

Your mobile will tell a spy almost anything he wants to know about you, reveals Secret Agent **Mark Harris**

The revelations about Prism, the US government's surveillance programme, have left many smartphone owners looking warily at their devices — and rightly so. The price of convenience is that almost everything your smartphone knows about you — from your location to your contacts and your taste in music — is available to prying eyes. Companies and agencies can track it and extract information from it without it leaving your pocket. And the more advanced your smartphone, the better a spy it makes.

"If you asked GCHQ [the British listening post] or the NSA [National Security Agency, America's spy centre] what they need to track a suspect, they would say a microphone, a GPS locator and a camera — everything that today's smartphones have," says Justin Cappos, a computer science professor at NYU-Poly in New York.

Surveillance can start the moment you turn on your phone. As the recent exposé of call-tracking in America shows, mobile phone operators collect, and can be forced to hand over, all kinds of information about your calling habits. This includes the numbers you dial and the phone base station your handset used, which locates it with an accuracy of about a mile.

If the authorities want more precision, the network can measure radio signals on your phone from multiple base stations. A process called triangulation calculates your position to within a few hundred feet, placing you in a building or following you as you travel in a city. A more advanced process called trilateralisation can calculate your height above the ground, putting you on a certain floor in a building.

The new data snooping centre in Utah

Most modern smartphones are constantly checking for wi-fi networks to join. Every time they find one, that connection can be logged. If investigators have that information too, they can pinpoint your phone to within just a few feet — even if you never make a call, go online or turn on your phone's GPS receiver.

Spies can even take control of a smartphone's camera, microphone and GPS. For anyone who doubts that this is possible, just load an app such as Prey (for Android and Apple devices), which allows owners to activate the camera, microphone and location finder over the internet if their phone has been stolen. If an owner can do this, then so can an intelligence agency with the help of its supercomputers.

Google and Amazon have already shown that they can delete software from phones and tablets, with or without users' knowledge or permission. "I would suggest that if Google can do it, there may well be a way that law enforcement can do it," says Gary Kessler, professor of homeland security at Embry-Riddle Aeronautical University in Florida.

Once you start using the software on your phone, the potential for snooping increases. Almost every app and service reveals something about you. Opening Google Maps shows where you plan to go, Hotmail contains your personal communications and Facebook yields friends and contacts. Permission for the software supplier to use this data may have been granted by you in the terms and conditions most users tick without reading — see Dragon Dictation for an example in Planet of the Apps, right.

As part of its controversial Prism programme, the NSA claims it has access to these digital services and many more. Your Skype video calls, iPhone photos in the cloud and AOL instant chats are all subject to interception. In March alone the NSA indexed nearly 100bn pieces of digital intelligence like this from users around the world, according to documents leaked as part of the recent revelations.

Even the sprawling American intelligence network does not have the staff to sift through that many status updates, photos of cute animals and spam emails. Instead, it relies on computers in data centres as big as any owned by the tech companies it targets. In September, a £760m NSA server farm will open in Utah that is capable of storing and processing more than five zettabytes of data (one zettabyte is equal to about 1.1 trillion gigabytes) — enough to fill a stack of DVDs stretching from Earth to the moon.

Some of that processing muscle will be used to search for suspicious key words in emails, texts and voice calls, and to cross-reference call logs with, say, flight plans and banking transactions. The real challenge, though, is dealing with multimedia content such as video calls and YouTube videos. America's Intelligence Advanced Research Projects Activity aims to harvest intelligence from billions of hours of mobile phone footage. One program, codenamed Aladdin, searches uploaded videos for images and audio that suggest extremist content. Another, called Finder, aims to identify where a video was shot by analysing scenery in the background — a project that requires images of almost every place on Earth.

If a security agency should get hold of your phone itself, it can extract even more data. "From a technical standpoint, a Pin is not going to keep the government out of your phone," says Cappos. "That's not a threat manufacturers want to protect their users from."

Standard software tools available to police forces can crack passwords and extract data from many phones within minutes (see panel). If that doesn't work, investigators might resort to "flashing" the phone (copying its whole memory onto another device) or removing its memory chips entirely and connecting them to a reader.

Security features such as facial and voice recognition, used to wake up a phone, have made devices tougher to crack. "There was a sweet spot a couple of years ago when we could pretty much get inside any phone," says Kessler. "It is now becoming harder."

Pressure on phone makers to introduce such features has come from consumers concerned about lack of security. The latest measure is the "kill switch", which allows users to wipe data from a stolen phone remotely and — if it is fitted with an unauthorised Sim card — prevent it from working. Apple announced such a kill switch for iPhones last week. At a meeting in New York on Thursday, American government lawyers asked Google, Samsung and Microsoft to follow suit.

The industry is touting this development as a way of reassuring consumers their phone data is safer than ever. This is true, but users aren't the only people able to shut down their phones. Government agencies can do so as well, leaving you wondering whether, in the final analysis, it's you that controls your phone, or them.

Peeper in your pocket

As soon as your mobile is switched on it can be tracked to within 30 yards in a city. Turn on wi-fi and GPS and that distance narrows to just a few feet

Your mobile phone network logs every call you make, where you make it from, to whom and for how long — it's how it knows what to charge you. The NSA has been given this data by networks on request

Smartphones also contain cameras and microphones, which can turn them into bugging devices. The software to activate them remotely has to be installed — as many people do by adding security apps such as Prey

If you use cloud services, such as Apple's Photo Stream, your contacts, snaps and other personal information are sitting on servers. It is claimed the NSA is reading this data

When you install apps, they tell you what data they want to use — such as your contacts book. Don't tap past this without reading: even the most innocuous apps may upload private material to the app developer

No wireless connection is ever secure. A voice call or data packet can be intercepted, decrypted and read. The volume of traffic means this is not done by humans; instead, security agencies are building huge 'server farms' to store data, and are buying the world's most powerful computers to analyse it

FORCED ENTRY

Spooks can extract data from your smartphone in minutes with the Cellebrite Touch Ultimate computer. The £6,500 device is sold, the company says, only to law enforcement agencies, among them the West Yorkshire police.

30 seconds Investigators identify the phone by answering questions about its appearance. The Touch Ultimate can distinguish between 4,000 models in no more than eight questions.

60 seconds Agents select the right data connector and plug the phone into the console.

90 seconds The system bypasses locks and passwords using known security flaws, or cracks them using 'brute force' combinations of letters and numbers. Only a few modern phones, including the iPhone 5, can resist the latter attack.

150 seconds The Touch Ultimate extracts all passwords and data, even if they have been deleted. This includes call records, calendar entries, email, GPS information, text messages, photos, video and audio.

300 seconds The unit displays the most-called numbers, key contacts and Facebook friends for investigators to follow up.