Fields Associates
Litigation Consultants

In response to concerns over the safety of our data and right to privacy, SGP Technology has developed the Blackphone which, whilst it possesses fairly unremarkable specs, does have a unique feature: it automatically encrypts all telephone calls and text messages whilst also offering anonymous web browsing. But can those of us that purchase a Blackphone genuinely expect absolute privacy?

In short, the answer is no. There are a variety of organisations who, should they wish to decrypt the data in question, possess all of the resources required to do so. Still, individuals that purchase a Blackphone can rest easy safe in the knowledge that, as the encryption key is stored on their phone only, any data concerning them that is held on SGP's servers will be encrypted and, as SGP themselves do not hold the relevant encryption key, should a hacker gain access to them, their data will not be immediately compromised.

In terms of how such a device would impact on the work of those of us operating within the field of digital forensics, many questions will remain unanswered until it is possible to subject the device to rigorous analysis. There are, however, reasons to doubt the anti-forensics capabilities of such a device.

Firstly, any individual that is charged with a criminal activity would be legally obliged to provide an investigator with a encryption key in the event of them possessing storage devices that contained encrypted data. Failure to do so would constitute a criminal offence in itself and it is likely that this information could be obtained with relative ease as a result should the data need to be analysed as part of a criminal investigation. Additionally, in the event of such a device needing to be analysed as part of a civil matter, a court order forcing the relevant party to provide the encryption key could be obtained.

Equally relevant is that mobile telephones are frequently used to determine the user's approximate whereabouts at the time that a crime was committed. Whilst not an exact science, cell site analysis utilises information obtained from a phone's baseband (essentially a black box that communicates with cell towers), a piece of entrenched hardware which, as it possesses its own CPU and operating system, contains information that a skilled forensics investigator can access with relative ease – even on a Blackphone.

Ultimately, Blackphone's target audience is not the criminal underclass, but rather ordinary people who are concerned about how third parties access and use their data. Blackphone is not designed to be used as an anti-forensics device and is of little concern to those operating in the field of digital forensics as a result.