Shahaf Rozanski explains the importance of being able to access data housed in the cloud for gaining vital evidence of a suspect's location and/or intentions

PEERING THROU

With there now being more mobile phones on the planet than people and smartphones set to achieve saturation in just 10 years, unlocking the data held on them has increasingly needed to be used as vital evidence for police forces. However as apps – and the data held within them – have moved into the cloud, police forces have struggled to follow this data into the ether. Law enforcement agencies could in fact be missing out on critical evidence if they don't have technology in place to extract and analyse this evidence.

What makes it so valuable is that an increasingly large proportion of information now accessed on a modern device – whether that be via Gmail, Dropbox or WhatsApp – is actually stored in the cloud, not on the device itself. Therefore, it is not data that can be easily accessible from traditional mobile or PC extraction techniques. Yet, this data is rich in potential case-solving content for police officers. For example, there are applications that are designed to provide a more accurate search experience for the user, which in turn provides a minute-by-minute accurate log of where they were at any given moment. Thus being important evidence to either place a suspect at the scene of a crime or to corroborate an alibi.

The issue is that, historically, there has been no streamlined or standard method for gaining access to cloud-based data as there are a number of challenges to extracting it. One of the main issues has been the paradigm shift in a consumer's view of their own security and privacy in the wake of numerous scaremongering media stories. This has led to consumers not allowing global access to their data, but making their social media content and information 'private' so that it is restricted to only friends and family being able to view it. This has made it more difficult and time consuming for law enforcement agencies to extract the required data without the subject revealing their credentials and the fear that the data may not be forensically preserved.

Identifying evidence in the cloud is a particular challenge because of the sheer amount of data now housed in the cloud, with current estimates suggesting that at least 2.5 quintillion bytes of data is added every day. Too much, and a search might be overbroad; too little, and investigators could miss important data for their case.

There are a number of challenges law enforcement agencies experience when relying on service providers to extract and provide them with the desired data. Firstly there are the costly legal procedures associated in filing a MLAT (mutual legal assistance treaty) request as the data often resides cross-border. Second is the fact that a provider's response will often be far from swift and more likely measured in weeks or months. Finally, there is the difficulty of a silo-ed analysis of a likely incomplete data set from multiple providers.

For investigators, this collection and analysis of data from distributed and disparate sources is challenging but an unavoidable truth as perpetrators will likely use multiple services from different providers. Yet, they need to persevere as data from multiple social media, file sharing or location-based data accounts (or mobile devices) will enable them to contextualise a suspect's or victim's activities, while showing an investigator's due diligence in building a case.

By investigators being able to effectively infiltrate the cloud, it reduces the risk of missing content, its context and meaning. By viewing and capturing data in context, and placing it alongside other data available from a suspect's mobile device or operator's call detail records, gives investigators further insight into how evidence correlates and can build up a solid case.

Even in cases where a wily suspect has used a so called 'burner phone' to conceal their identity, commonalities will likely exist between devices and cloud accounts. Therefore, investigators will still be able to tie devices and accounts to a suspect.

It is important for police forces to be mindful of legal obligation in regard to data privacy. To ensure this, an investigation will begin with extracting user data, including credentials and cloud access keys, found on a subject mobile device with the proper legal authority. This account-based approach means that they will only selectively acquire data residing in the cloud that is associated with a specific user, unless the account is shared. By doing so preserves the privacy of other tenants collocated on the same cloud server and minimises issues with evidence being scattered around different storage locations.

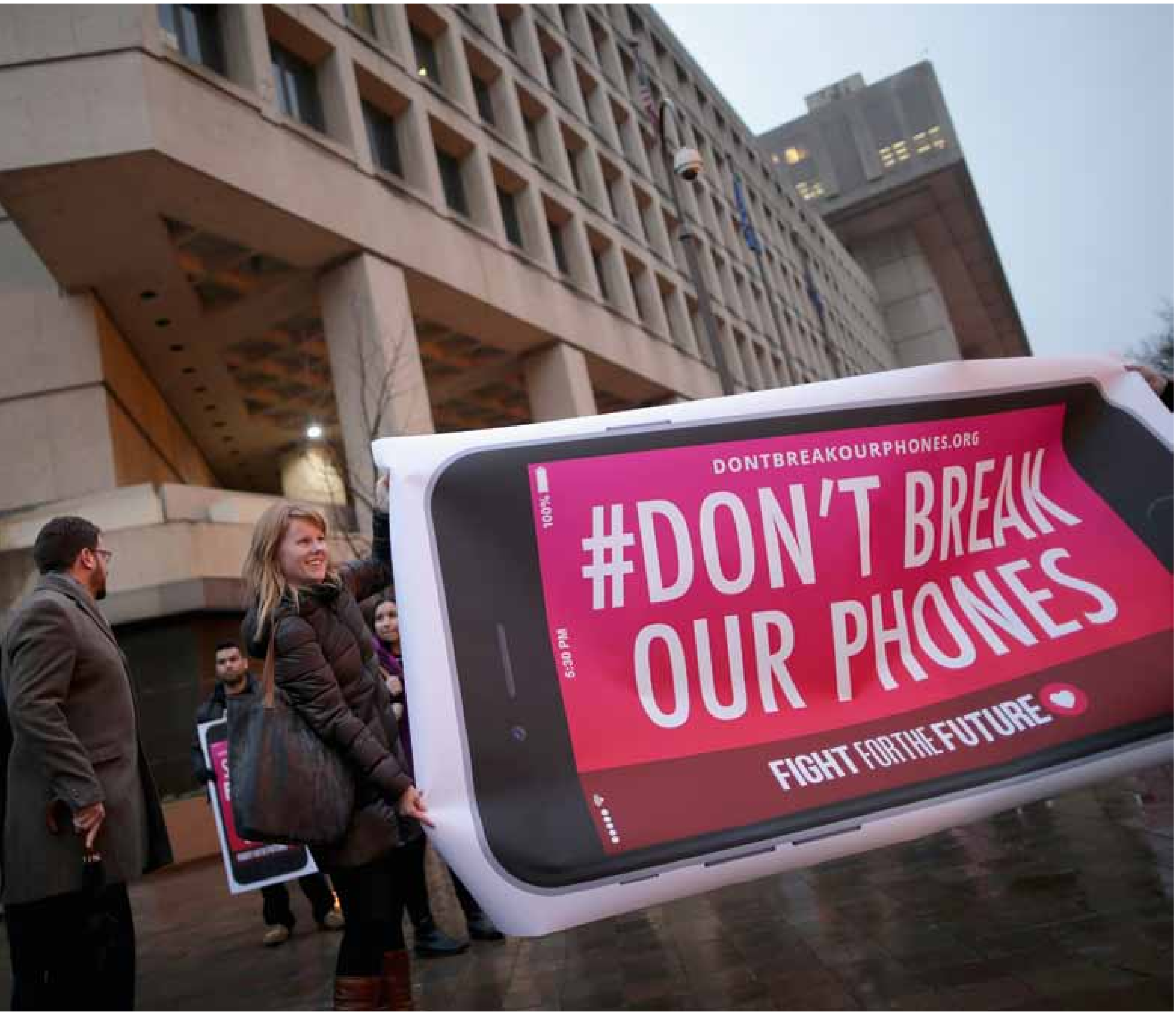
Specific cloud analysers designed for police forces promote forensic best practices around validation and

©Getty Images

Protestors demonstrate against a move by the US federal Government to force Apple to create a 'backdoor' to the iPhone

> **"Historically there has been no streamlined or standard method for gaining access to cloud-based data"**

IGH THE CLOUD



authentication by relying on provider APIs to perform extractions. They will then hash (disguise) each individual artefact and, separately, the associated metadata. Not only does this ensure repeatability; it also allows for proper validation using records obtained directly from the service provider. This in turn helps speed the access to evidence and makes it instantly actionable for the investigation.

Most legacy digital forensic training materials are outdated as they were authored before the emergence of cloud-based environments. Therefore, investigators need training not just on cloud forensics policy and procedure, but also the foundation of cloud computing technology itself. Otherwise, the lack of knowledge about cloud technology may interfere with remote investigations where systems are not physically accessible and there is an absence of proper tools to effectively investigate the cloud computing environment.

Cloud data sources represent a virtual goldmine of potential evidence for modern day forensic investigators. Together with mobile device data, they can capture the details and critical connections investigators need to solve crimes. By peering through the cloud to correlate evidence from multiple cloud-based accounts and disparate data formats, police forces can reduce the risk of missing valuable evidence for their investigations.