Shahaf Rozanski examines the legal aspects of obtaining and analysing forensic evidence from the private cloud

EXTRACTING EVIDENCE FROM THE CLOUD

Cloud data offers a digital footprint that can prove vital in forensic investigations. Sources can generate critical leads, which can help investigators piece together criminal cases and provide important evidence. This evidence can then be put forward by prosecutors in a court of law or provide defence lawyers with a much-needed alibi for their client. The process may sound simple, but there are a number of aspects that both police forces and legal professionals need to consider before the data can be presented and accepted in a given case.

There are three types of cloud data, which can be categorised by their organisational deployment: enterprise, public and private cloud data. The latter has an infrastructure which is operated solely by the organisation that owns that particular cloud service, as such this type of cloud data in particular can pose limitations to forensic investigations before cases even reach the criminal courts.

Legal framework and specific procedures apply to collecting private cloud data and this can differ from country to country. There is no one model fits all solution so the problem has the potential to escalate when investigations spread overseas. Investigating authorities can only obtain this data when either party agrees to provide access, a judge issues a warrant, where parties to the Convention on Cyber crime can obtain access to data under the provisions of Article 32 or when the concept of 'virtual presence' is accepted by the courts for the purposes of seizing data.

When investigators don't have consent from the user to access such data, they have to turn to the service provider. In this instance, a number of questions can arise regarding the ownership of the data. Is the owner the user who uploaded it to social media or is it the provider? Some legislators may claim that the user is the owner of data, much like they would own equipment they stored in a third-party warehouse. If this is the case, why should data be requested from the cloud provider and potentially put the investigation on hold for weeks, if not months? In such cases investigators can then turn to mobile forensic technology, which can provide access to private-user cloud data by utilising login details that have been extracted from the mobile device of the suspect or victim.

> **There are three types of cloud data, which can be categorised by their organisational deployment: enterprise, public and private cloud data.**

The next question to be asked is where the data is and what jurisdiction is applied to retrieving it. Is there a way to determine where the data actually resides? With the complex architecture of the internet it is impossible to know if data resides in a specific datacentre operated by the cloud service provider or if it's cached on your internet service provider servers. Due to this lack of clarity, some legal systems use the notation of virtual presence, which means that as long as the cloud provider is providing a service in your country, where rules can apply on the data and law enforcement, you should have access to that data under relevant local legal authority. Such is the case of Yahoo in Belgium where the court ordered the company to provide relevant records even if it doesn't have local presence in the country. This case is now being discussed

Private cloud data can pose limitations to forensic investigations before cases even reach the criminal courts

in higher court hierarchies.

Finally, to be able to submit data in court, it should be forensically retrieved. A piece of data can be easily removed by someone that has access to a private account, and as such, being able to repeat the process of private cloud data acquisition and get the same results might be a challenge. The legal system needs to appreciate that when dealing with cloud data there may not be any other resort but to take a snapshot of the data that existed in the cloud at a certain time. This is similar to a murder case taking place in a park in which the police can't confiscate the entire park and preserve it as is. Instead measures are taken to document a snapshot of the park as close as possible to time of the crime.

There are a number of hurdles investigators have to clear in order to extract and present private cloud data in criminal cases. As criminals take advantage of technological advances to aid their criminal activities, governments have had to adapt and adjust the legal framework to deal with new types of crime. It's essential that the process of carrying such data from field to court has clarity to ensure justice can be served in the modern, technological age.

Shahaf Rozanski is Director of Forensics Product at Cellebrite and is responsible for defining and launching future solutions to the law enforcement industry, including the UFED Cloud Analyzer. He brings more than 17 years' of experience in merging customer advocacy and technology, which he successfully applies in various global industries.