Using cloud data to accelerate forensic investigations

Shahaf Rozanski, Cellebrite

Cloud data represents a virtual goldmine of potential evidence for forensic investigators. Together with mobile device data, cloud data sources often present the critical connections investigators need to solve crimes. However, there are a number of challenges that investigators face when it comes to data retrieval from the cloud.

Private data

The overarching challenge is private data in the cloud. As the term suggests, this is private user data (i.e., data that the user has actively chosen to refrain from sharing publically) and there is, for good reason, a significant amount of ‘red tape’ that surrounds private user data. But what happens when the user in question is suspected of committing a crime?

"With something like 38 million social media users in the UK – a staggering 59% of the population – it is evident that, during a criminal case, investigators simply cannot afford to neglect social data"

To add to this, more and more data is being stored in the cloud as many companies, and indeed individuals, look to virtual methods of data storage because of the enhanced flexibility and ease of access they offer. This also correlates with the number of users now on social media. With something like 38 million social media users in the UK – a staggering 59% of the population – it is evident that, during a criminal case, investigators simply cannot afford to neglect social data that is inevitably stored in the cloud.

Out of the 38 million UK social media users, 30 million of them (79%) are using social media on their mobiles, which further highlights the importance of mobile phones in the retrieval of crucial evidence in criminal investigations.

Paramount importance

Investigators need to be able to access this data when it is of paramount importance to a criminal investigation. The problem is that investigators may need to go to the service provider if they don’t have the permissions or capabilities to access the username and password to request this data, which can take time.

If you’re an investigative force requesting private data in the cloud from a company located in the same country where the investigation is taking place, then it can take a few weeks to a few months to obtain this data. However, if you’re requesting the data from another country – bearing in mind the investigation may be taking place in Europe while most of the world’s major service providers are based in the US – then it can take up to a year to retrieve the data.

“The retrieval of evidence needs to be executed in the shortest possible time to ensure that nothing is missed in the evidence gathering process, and to ensure that the investigative team doesn’t run out of time”

The time that it takes to request data relevant to a particular criminal case is a challenge in the sense that the timeline of an investigation is extremely important to the outcome of the case. The retrieval of evidence needs to be executed in the shortest possible time to ensure that nothing is missed in the evidence gathering process, and to ensure that the investigative team doesn’t run out of time when retrieving evidence.

There is also an issue with the records production rate of the cloud service providers, due to the limited resources that these companies have to handle the large number of requests from law enforcement. In the UK during the first half of Continued on page 20...
2014, the response rate from Facebook and Google was 70%, while Twitter’s response rate was only at 40%.

Another challenge is that of forensic data preservation. It is of vital importance that the case team retrieves and handles all private data sources with the utmost care and consideration. In the case of extracting evidential data from the cloud, investigators should feel confident that the information that was extracted from the cloud service provider is authentic, traceable and thus defensible in court.

**Timely manner**

However, the problem of accessing private cloud data in a timely manner for criminal investigations can be rectified with the use of mobile forensic technology. When a mobile phone is seized in criminal investigations, law enforcement can use technology to access private-user cloud data by utilising login details that have been extracted from the mobile device of the suspect or victim. This private-user cloud data is extracted under the appropriate legal authority, be it a search warrant, written consent, or other authority as defined by legal counsel in the relevant jurisdiction.

The investigative procedure when using such technology to retrieve private user cloud data involves a five step process:

- Seize the mobile device and begin a forensic extraction of data.
- Decode cloud services login information from the extracted forensic copy of the device.
- Forensically preserve private user data using login information from the mobile device or manually provided credentials.
- Analyse and report data from different cloud data sources in a unified format.
- Deliver data to additional relevant law enforcement and justice officials.

The analysis and reporting of retrieved data in a unified format is a very significant step in this process. The data that is retrieved has to be understood by a range of investigators and legal personnel, many of who may not be well versed in mobile forensic data retrieval.

This data may also have to be presented in a courtroom, where a jury might be present that will have to understand and digest the data that is being put in front of them. Again, the data must be in a format that can be understood easily so that people with little or no understanding of mobile data forensics can easily make a decision based on the evidential data that has been displayed to them.

**Pool of evidence**

The importance of cloud data in so many areas of everyday life means that law enforcement agencies simply must consider the pool of evidence that is stored in the cloud during criminal investigations. A failure to contemplate this data could easily result in missed opportunities to convict, and during live investigations the consequences could be far worse.

The ever-increasing use of mobile phones to conduct criminal activity in correlation with the vast numbers of social media users worldwide, is a clear indication that criminal investigators must be equipped with the latest technology to rapidly retrieve cloud data and react to all types of criminal who use and abuse different channels to exercise their criminal activity.

**About the author**

Shahaf Rozanski is director of forensics products at Cellebrite. He is responsible for defining and launching Cellebrite’s future solutions to the law enforcement industry. Rozanski brings more than 17 years of experience in merging customer advocacy and technology which he successfully applies in various global industries.

**Resource**

- George, E; Mason, S. ‘Obtaining evidence from mobile devices and the cloud’. 2015.

---

**EVENTS CALENDAR**

8–9 October 2015
BruCON
Ghent, Belgium
http://brucon.org

20–21 October 2015
(ISC)² Security Congress EMEA
Munich, Germany
http://emeacongress.isc2.org/

20–21 October 2015
Cyber-security Summit
Minneapolis, US
www.cyber-securitysummit.org

4–5 November 2015
RSA Conference Abu Dhabi
Emirates Palace, Abu Dhabi
www.rsaconference.com/events/ad15

10–13 November 2015
Black Hat Europe
Amsterdam, Netherlands
www.blackhat.com

10–11 November 2015
Information Security Solutions Europe (ISSE)
Berlin, Germany
www.isse.eu.com

16 November–21 December 2015
SANS London 2015
London, UK
www.sans.org/event/london-2015

24–25 November 2015
Info-Crime 2015
London, UK
www.info-crime.com

25 November 2015
Cloud Law European Summit
London, UK
www.cloud-law.eu