

Cloud extraction technology: the secret tech that lets government agencies collect masses of data from apps

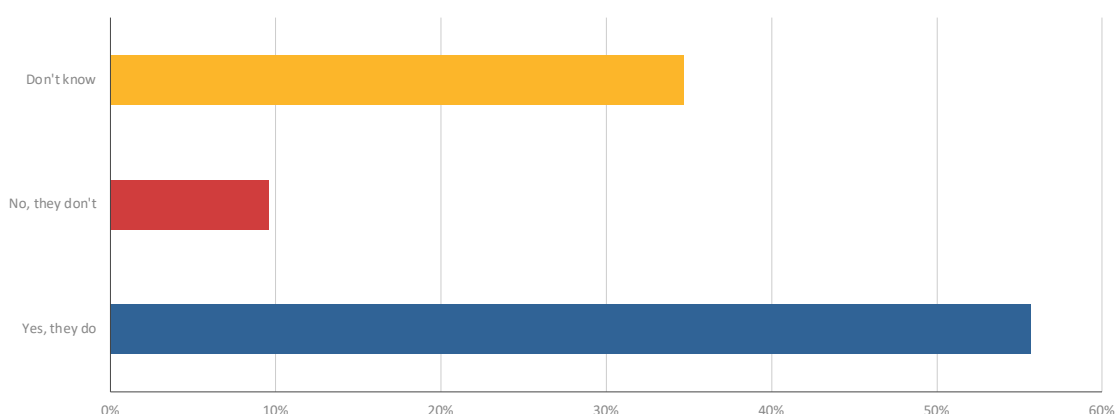
When government searches shift from the phone to the cloud: cloud extraction technology and 'the future of mobile forensics'

Mobile phones remain the most frequently used and most important digital source for law enforcement investigationsⁱ. Yet it is not just what is physically stored on the phone that law enforcement are after, but what can be accessed from it, primarily data stored in the Cloud.

Cellebrite, a prominent vendor of surveillance technology used to extract data from mobile phones, notes in its Annual Trend Surveyⁱⁱ that in approximately half of all investigations, cloud data 'appears' and that *'[t]ypically, this data involves social media or application data that does not reside on the physical device.'* That it *'does not reside on the physical device'* indicates that law enforcement is turning to 'cloud extraction': the forensic analysis of user data which is stored on third-party servers, typically used by device and application manufacturers to back up data.

Yet as law enforcement increasingly turns to cloud extraction to obtain data from apps, a YouGov poll revealed that in the UK 45.6% of people have not thought about where data created by apps on their phone is stored and 44.3% of people do not know or think that apps on their phone use cloud storage.

Do any of the apps on your smartphone use cloud storage?



As we spend more time using social media, messaging apps, store files with the likes of Dropbox and Google Drive, as our phones become more secure, locked devices harder to crack, and file-based encryption becomes more widespread, cloud extraction is, as a prominent industry player says, *“arguably the future of mobile forensics.”*ⁱⁱⁱ

“Private cloud-based data represents a virtual goldmine of potential evidence for forensic investigators.”^{iv}

At Privacy International we have repeatedly raised concerns over risks of mobile phone extraction from a forensics perspective^v and highlighted the absence of effective privacy and security safeguards^{vi}. **Cloud extraction goes a step further, promising access to not just what is contained within the phone, but also to what is accessible from it.**

Your phone, with all the data there for exploitation, becomes the key to unlock your online personal and professional life.

In this context, cloud extraction technologies make for disturbing reading as we grasp how much is held in remote servers and accessible to even those with limited forensic skills who nonetheless are now able to acquire push button technologies that can ‘grab it all’^{vii}.

Greater urgency is needed to address the risks that arise from such extraction, especially as we consider the addition of facial and emotion recognition to software which analyses the extracted data.

There is a failure to inform the public about new surveillance technologies deployed by the state; an absence of clear, accessible legal frameworks; a lack of discernible action by governments and little to protect the public from data exploitation. The seeming wild west approach to highly sensitive data carries the risk of abuse, misuse and miscarriage of justice.

Cloud extraction technologies are deployed with little transparency and in the context of very limited public understanding: this report brings together the results of Privacy International’s open source research, technical analyses and freedom of information requests to expose and address this emerging and urgent threat to people’s rights.

Table of Contents

<i>Cloud extraction technology: a concerning new development in mobile phone extraction.....</i>	<i>1</i>
<i>What is mobile phone extraction.....</i>	<i>4</i>
<i>What is cloud extraction</i>	<i>4</i>
How does it work	6
What types of data can be obtained?.....	8
Currently supported cloud services	15
Facial Recognition and Cloud extraction.....	19
Continual tracking.....	19
<i>Conclusion</i>	<i>21</i>

What is mobile phone extraction

Mobile phone extraction tools are devices and software that allow the police to download data from mobile phones, including:

- Contacts
- Call data – who we call, when, and for how long
- Text messages
- Stored files – photos, videos, audio files, documents, etc
- App data – what apps we use and the data stored on them
- Location information
- Wi-fi network connections – which can reveal the locations of any place where we've connected to wi-fi, such as our workplace and properties we've visited.

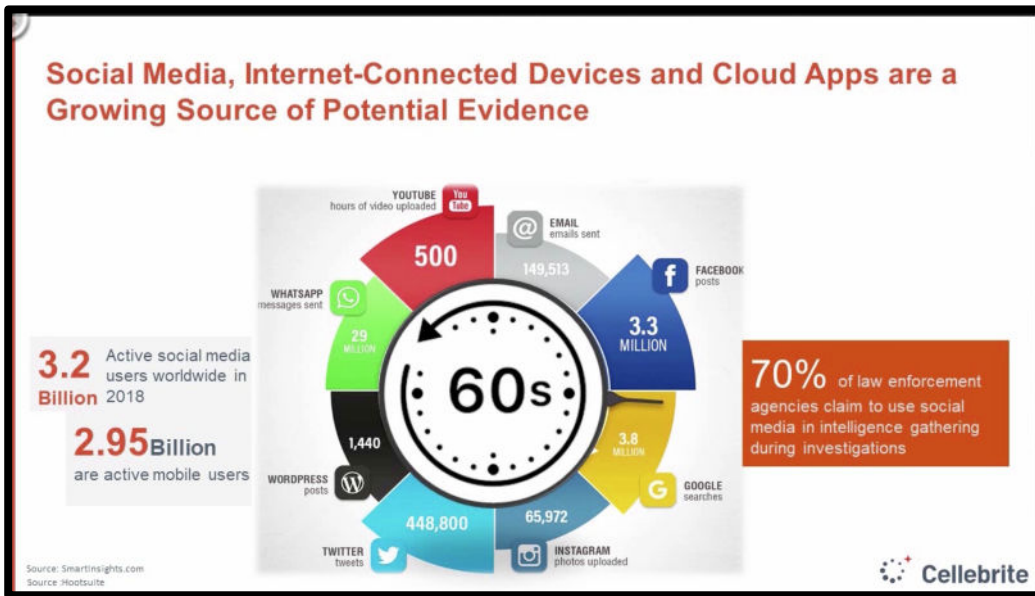
Mobile phone extraction entails the physical connection of the mobile device that is to be analysed and a device that extracts, analyses and presents the data contained on the phone.

However not only does it provide what is contained on the device itself, it can be a gateway to the Cloud and to external sources of information. If you extract logins, passwords and tokens from the examined device, these can be used to validate credentials to extract cloud stored data. ^{viii}

What is cloud extraction

Cloud extraction (or cloud analytics) is the ability to access, extract, analyse and retain data stored in the Cloud^{ix}, a term widely used by technology companies to refer to the storage of data remotely, from applications or devices, typically on a third company's servers. Examples include Dropbox, Slack, Instagram, Twitter, Facebook, Google products such as My Activity, Uber and Hotmail. We explore the types of data that can be extracted in more detail below.

As cloud storage is increasingly used for social media, internet-connected devices and apps, cloud extraction opens the door to a huge amount of personal information. In reports on the explosion of cloud-based data, it is said that by 2025, 49 percent of data will be stored in public cloud environments^x. Cisco Global Cloud Index^{xi} forecasts the growth of global data centre and cloud-based IP traffic and predicts an increase in use of public cloud data centers by 2021.



Social media usage^{xii}

"The lion's share of data from mobile applications are stored within the cloud. With this being said, it should be understandable that there is a massive amount of user data available for collection."^{xiii}

Cellebrite's UFED Cloud Analyzer, for example, uses login credentials that can be extracted from the device to then pull a history of searches, visited pages, voice search recording and translations from Google web history and view text searches conducted with Chrome and Safari on iOS devices backed-up iCloud. **By acquiring the login credentials, it allows its users to then continue to track the online behaviour of the device's user even if you are no longer in possession of the phone.**



Oxygen Forensics tweet

How does it work

There are a number of ways to access Cloud data *"independent of the status or configuration of the mobile device"*^{xiv}, which makes it attractive from a forensics perspective. The first involves applying known user credentials provided by an individual, i.e. when the individual submits voluntarily their login details. The second method is by extracting data from a phone and then using the tokens found on the device or found on another device such as a laptop, where a user might have authentication tokens saved by a browser. The third method involves collecting data in the public domain.^{xv}

*"When a user authenticates successfully to an app or cloud service, the service **returns a token**, which is used to enable the user to access the service without having to enter his or her username and password again. A token is like a pass, and it is used, for example, when you open your Gmail account and it logs you in without requiring any interaction from you. Most tokens have an expiry set at the time of authentication, which varies per app or cloud server. Some are good for a single session only, others for two weeks, some for 30 days, and some forever if the user uses the app on the same mobile device."*^{xvi}

The use of tokens avoids two factor authentication (2FA) being triggered by logging in, which would ordinarily inhibit access to data. 2FA, the process in which a user is prompted to confirm a code sent to an independent device, such as their mobile phone, is a key security feature. However, even if 2FA is triggered, Oxygen Forensics Cloud Extractor states it can notify the investigator and *"several options are provided to bypass the additional steps."*^{xvii}

Tools used to obtain tokens beyond the mobile

Elcomsoft's GTEX tool can search a computer for authentication tokens.

"Passwordless authentication into Google Account is available if Google Chrome is installed on the user's computer, and the user signed in to at least one Google service via the browser. The new Google Token Extractor (GTEX) tool automatically searches the user's computer for authentication tokens saved by the Google Chrome browser. Once the user signs in to their Google Account in a browser session, these tokens enable seamless access to Google services without the need to re-enter the password."^{xviii}

Cellebrite's PC Cloud Collector

"is an independent tool that creates tokens from a suspect's PC using the cookies in the browsers and the applications that are installed on that PC."^{xix}

UFED Cloud Analyser 7.6:

"extends its password collector functionality to include passwords save on mobile web browsers. Examiners can now retrieve password logins from various sites using the password collector to collect the maximum amount of data about a suspect or

victim. This is accomplished by leveraging a person's login details which have been saved in their browser when they access their online accounts."

Another similar tool is Oxygen Forensics' KeyScout to find passwords and tokens on a PC:

"KeyScout installs a flash card and collects credentials from Windows PCs. The collected credentials can then be imported into Oxygen Forensic Cloud Extractor for immediate use."^{xx}

Forensics tools not only offer a simple way to access cloud stored data, they provide more data than an individual can access using their own username and password. Elcomsoft, for example, argues that *"even if proper authentication credentials are available [such as user name and password], access to evidence stored in the Cloud is not a given."^{xxi}* Elcomsoft compared the amount of data they could obtain using Elcomsoft Phone Breaker to what they could get when without using forensic tools. They argue that using their tool is not only simple and quick but can access more data from the Cloud, than can be accessed even when username and password are known.

Reports suggest that there are other ways to gain access to cloud-based accounts using tokens. In July 2019, the Financial Times reported that malware sold by NSO Group's, Pegasus, can carry out cloud extraction by copying authentication keys from an infected phone, allowing a separate server to then impersonate the phone, including its location^{xxii}. NSO Group refuted the report.^{xxiii}

Despite companies such as Amazon, Apple, Google and Microsoft commenting to the FT's story on NSO Group, it is unclear what their position is in relation to cloud extraction technologies used by law enforcement. Google told the FT that it found *"no evidence of access to Google accounts or systems"* with respect to Pegasus. Given the number of forensics companies openly promoting access to Google products however, it must be aware this is a significant issue for the security of their customers' data. We have written Google and other companies asking for their position on cloud extraction technologies. The reality is that in many cases their customers do not know this technology exists and it is being used against them in a vacuum of legal safeguards.

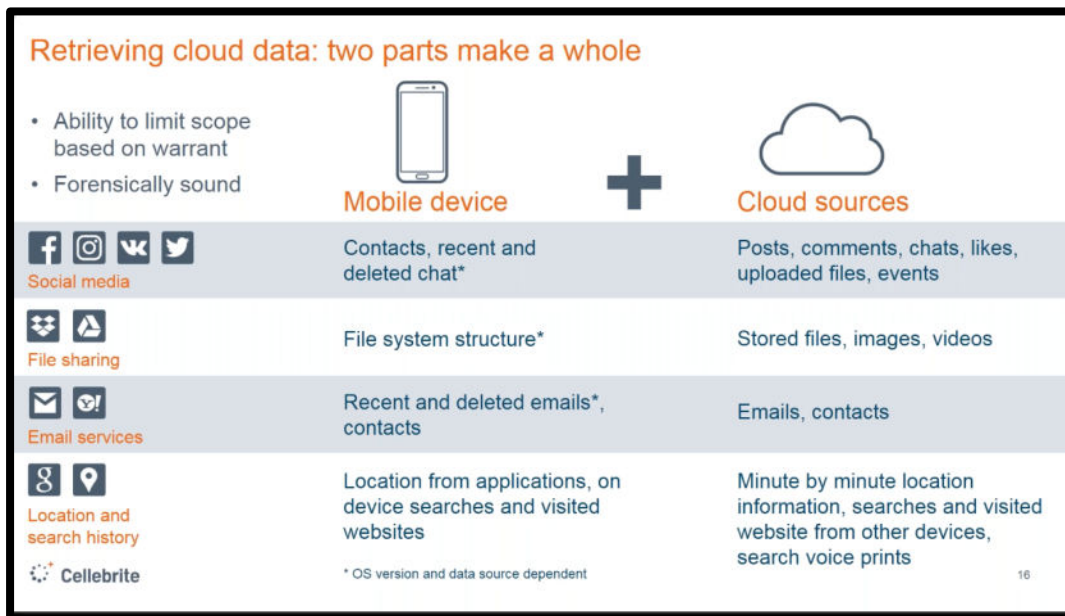
What types of data can be obtained?

Claims by surveillance companies regarding what the types of data can be accessible via cloud extraction are as impressive as they are concerning. Cellebrite's Cloud Analyser, for example, claims to *"extract, preserve and analyze public domain and private social media data, instant messaging, file storage, web-pages and other cloud-based content using a forensically sound process"*.^{xxiv} This includes a whole suite of Google products, whose 'History' function alone enables:





"insights into the subject's intentions and interests by pulling out the history of text searches, visited pages, voice search recordings and translations from Google web history and viewing text searches conducted with Chrome and Safari on iOS devices backed-up iCloud." – Cellebrite^{xxv}

Forensic experts claim to be able to acquire undelivered messages, unanswered calls, information about messages deleted from private and group chats, profile pictures and status messages of the account owner and contacts, original messages embedded into the reply and broadcast messages^{xxvi}. The data relates not only to the user of the services but their friends, family, colleagues and anyone the user interacts with.

The below images show a comparison by Cellebrite of the amount of data you can extract from a phone compared to what you can extract from Cloud sources, showing significantly more in relation to social media, emails, file sharing and location and search history from the latter. Notably *"Minute by Minute location information, searches and visited websites"* using Google's time-stamped Location History and Google My Activity data and backups.



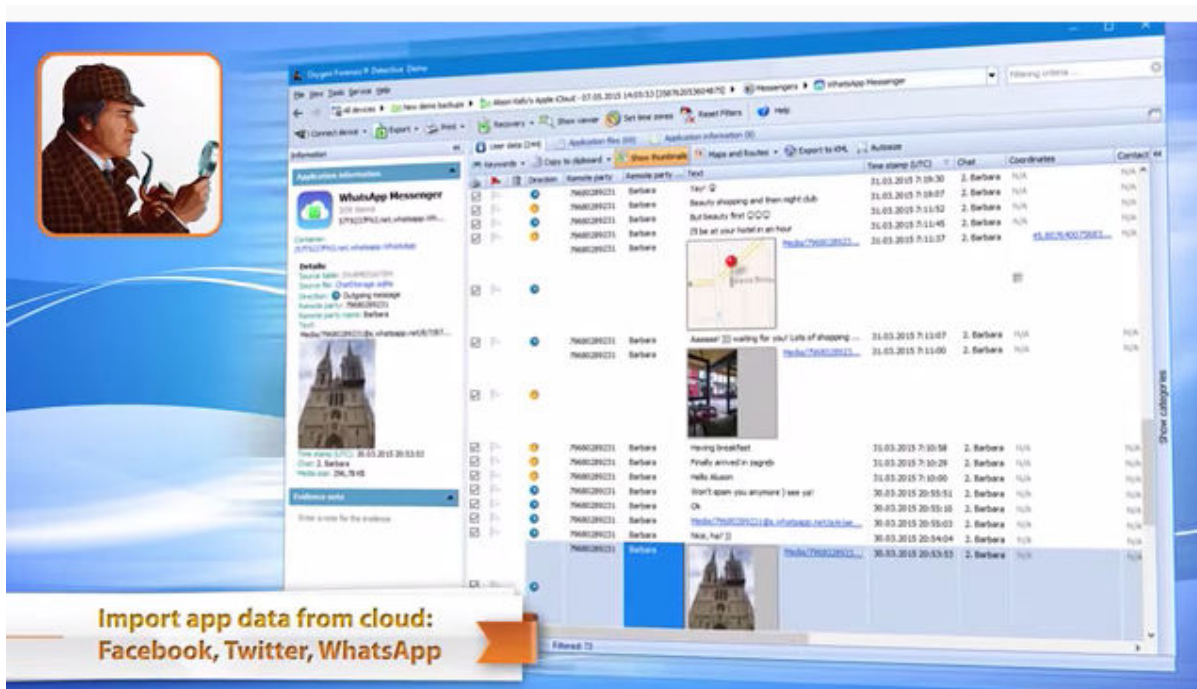
COMPARISON BETWEEN MOBILE AND CLOUD DATA^{xxvii}

Source	Type		UFED Cloud Analyzer
	• Social	• Contacts, recent and deleted chats	• Posts, comments, chats, likes, files, events
	• Storage	• Files stored on the device	• Any uploaded file
	• Email	• Recent and deleted emails, contacts	• Any email on the server
	• Location	• Locations from on device applications	• Minute by minute location with accuracy
	• Browser	• Searches, auto complete, bookmarks and visited pages	• Searches, auto complete, book visited pages and passwords
	• My activity		• Passwords, My activity from an including Google home
	• Backup		• Searches, contacts, call logs, cl from locked phone

COMPARISON BETWEEN MOBILE AND CLOUD EXTRACTION^{xxviii}

Oxygen Forensics, who developed Oxygen Forensics Detective forensic analysis tool, have built-in Oxygen Forensic Cloud Extractor to acquire *“data from the most popular cloud services”* including WhatsApp, iCloud, Google, Microsoft, Mi Cloud, Huawei, Samsung, E-Mail (IMAP) Servers and more. *“Also various social media services are supported to include but limited to: Facebook, Twitter, Instagram, and many more.”* It *“...supports, at the time of writing, 54 different types of cloud services, ranging from file storage, to messengers, drones, health apps, and social media.”*^{xxix}

Even if you use end to end encrypted messaging, if you back up your WhatsApp messages to the Cloud, they are accessible to law enforcement.



xxxOxygen Forensics slide showing extracting data from WhatsApp messenger

Magnet Forensics also provides a cloud extraction service, AXIOM Cloud^{xxxix}, which “supports approximately 25 cloud artefacts in nine parent services to include Apple Box, Dropbox, IMAP/POP, Facebook, Google, Instagram, Microsoft and Twitter. Each service is broken down into different subservices.”

Looking at the types of data that can be extracted in more detail, Cellebrite’s Product Updates for Cloud Analyser show the increasing appetite for data from smart devices such as Alexa and Google Home. Cellebrite’s UFED Cloud Analyser 7.2^{xxxix} “provides access to user requests including audio^{xxxix}. As Cellebrite notes,

“The Internet of Things (IoT) has created more ways to use data to make our lives easier, but it has also created more sources of digital intelligence for investigators to access in their criminal investigations.” – Cellebrite^{xxxix}

Cellebrite is not the only mobile extraction company promoting access to data from home assistants. Oxygen Forensics views digital assistants as the new eye-witness^{xxxv} with an estimated number of users of these devices projected to reach 1.8 billion by 2021:

“The valuable data extracted can contain a wealth of information to include: account and device details, contacts, user activity, incoming and outgoing messages, calendars, notifications, user created lists, created/installed skills, preferences, and more. One amazing feature in the software is the ability to extract the stored voice commands given to Alexa by the user. The users actual

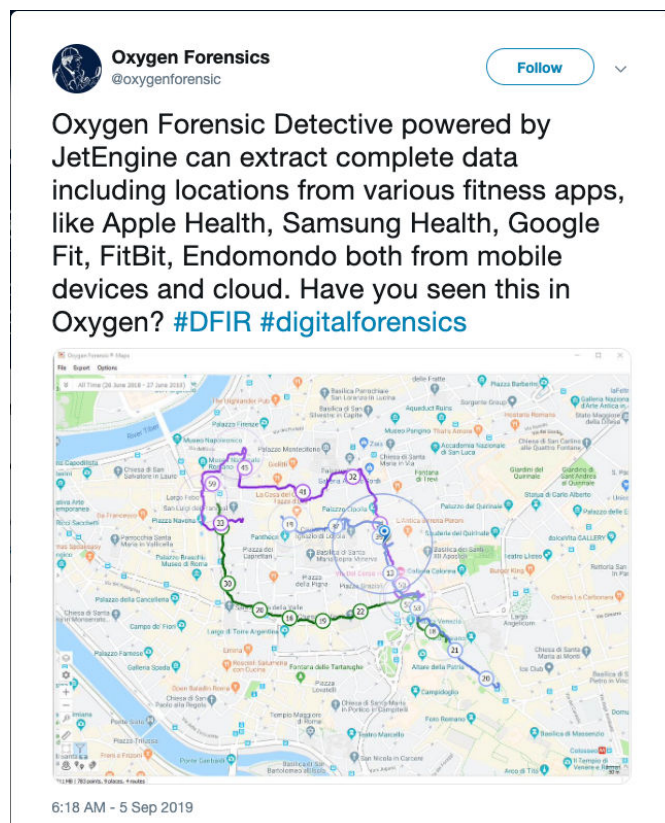
voice! The information extracted from Amazon will undoubtedly give tremendous insights into the user's everyday activity, their contacts, shared messages, and valuable voice commands."^{xxxvi}

"When an Alexa user utters the wake word to perform a skill a recording of the query is sent to the user's Amazon cloud account. The user specific request is processed and a response is returned to the device. Investigators, armed with Oxygen Forensic Cloud Extractor, can extract Amazon Alexa data to include these valuable recordings of that actual utterance by the user."^{xxxvii}

As the number of devices connected to the internet and thus storing data in the cloud continues to grow, cloud extraction not only reaches into people's homes but also their bodies with access to data from health wearables.

"Many of today's users are into health wearables, from the Fitbit to the Apple Watch, which includes information such as heart rate, location, food intake, messaging and other valuable data that is often available only on the cloud service and not on the mobile device."^{xxxviii}

Cellebrite can access Fitbit "user profile, logs, activities, goals, friends, heart rate, exercise track (speed, location, time etc.)."



Another source of data relates to travel and location with UFED Cloud Analyzer 7.3 accessing Google location data and Booking.com "user profile, purchase history,

messages and searches" and UFED Cloud Analyzer 7.6 supports extraction from the UBER App and can:

"gain passenger and driver profile data, pick-up and drop-off location logs, and the last 4 digits of a user's credit card...retrieval of ... credit card details that new users are required to fill in on their first login. As the passenger chooses their pickup location, desire destination, and available driver, each journey is well documented. Recorded routes are aggregated and then categorised by favourite designations. The driver's information includes the name and photo identification." -- Cellebrite^{xxxix}



Given the popularity of Amazon and Facebook, these are obvious targets for cloud stored data. As of the fourth quarter of 2018, Facebook had 2.32 billion monthly active users.^{xi} Amazon had 300 million users in 2017^{xii}. An update for Cellebrite's UFED Cloud Analyzer 7.5^{xiii} includes "five brand new capabilities that enable access to activity logs, search histories, pages, user group data and IP address records [for Facebook]." The software can:

"... extract information from the stories and photos a suspect was tagged in to find new leads or new suspects. Additional data points include identification of connections made when liking a page or adding someone as a friend, as well as comments posted, articles read, videos seen, places visited and more.

For user data on groups and pages, UFED Cloud Analyzer 7.5 can also flag if a suspect is a member or administrator of a certain page or group.

This version can also surface the Facebook Log IP address records to allow you to identify a phone or computer's location used to access an account."

UFED Cloud Analyzer 7.5^{xliii} "enables access to [Amazon's] search history, purchase history and delivery addresses that can contribute vital digital evidence to an investigation."

"In this version, you can also view the last 4 digits of a credit card registered on an Amazon account, including the billing and shipping addresses."

"The buyers' search history and wish list over time can indicate suspicious behaviour leading up to a crime."

Cloud extraction technologies also access data from drones, such as UFED Cloud Analyzer 7.6^{xliiv} which added DJI Drone App and SkyPixel social network. This

"Allows examiners to access the app as well as the corresponding users account on the SkyPixel social network. User profile data and stored drone flight log data is retrievable and includes: date, distance, flight time, location, video and imagery. SkyPixel user profile can also assist examiners to verify if any collaboration was performed on specific videos as well as track tags, follows and more."^{xliiv}

As more and more companies rely on cloud storage for work related activities, accessible data which can be obtained from tokens on devices relates not just to personal life but includes their work. For example:

"Cellebrite delivers access to shared files and instant messaging data from Slack, the popular communication tool of the business community."^{xlivi}

UFED Cloud Analyzer 7.9^{xlvii} also includes support for Snapchat and Instagram enhancements. This is relevant when we consider below the growing facial recognition capabilities inbuilt into analytics software that analyse extracted data both from mobile phones and obtained via cloud extraction.

"Snapchat is a global multimedia messaging app that enables users to share pictures and messages that are only available for a

short time before they become inaccessible to their recipients. To date, Snapchat has 190 million daily active users worldwide and more than 400 million Snapchat stores are created per day.

UFED Cloud Analyzer 7.9 introduces first-time support for the Snapchat application, with access using tokens retrieved from any Android device. With this version, you can retrieve backed up files, also known as Memories, and review direct message communications between contacts. Get access to the contact information of the account and password protected My Eyes Only files."

"This version of UFED Cloud Analyzer introduces comprehensive support for the Instagram application. On top of already supported data sets in previous versions, you can now view responses to posts which include images and videos. You can also get access to all data associated with chat messages including sharing of post/story, likes, comments within a message."



Oxygen Forensics
@oxygenforensic

Follow

Did you know that you can use our Cloud Extractor, built into Oxygen Forensic Detective, to acquire data from the most popular corporate cloud services, like iCloud, Google Drive, OneDrive, Dropbox, Box, Email Server, secure Wickr Messenger, etc?

[#cloudforensics](#)



6:24 AM - 30 Aug 2019

Currently supported cloud services, according to companies' claims and academic research:^{xlviii}

	Oxygen Forensics Cloud Extractor	UFED Analyzer	Cloud	Magnet Axiom
Alexa	YES			
Android Cloud (Google)	YES			
Apple Watch	YES			
Box	YES			YES
DJI Cloud	YES			
Dropbox	YES	YES		YES
Endomondo	YES			
Facebook	YES	YES		YES
Facebook Workplace	YES			
Fitbit	YES			
Google Accounts		YES		YES
Google Bookmarks	YES	YES		
Google Calendar	YES	YES		
Google Contacts	YES	YES		YES
Google Chrome	YES			
Google Drive	YES	YES		
Google Events				YES
Google Fit (Google Takeout)		YES		
Google Keep	YES	YES ^{xlix}		
Google Location History	YES	YES		
Google Mail	YES			
Gmail		YES		YES

Google My Activity	YES	YES	
Google Photos	YES	YES	YES
Google Password		YES	
Google Profile		YES	
Google Play (Google Takeout)		YES	
Google Tasks	YES	YES	
Google Search History		YES	
Google+ (Google Takeout)		YES	
Keep (Google Takeout)		YES	
Profile (Google Takeout)		YES	
YouTube (Google Takeout)		YES	
Hangouts (Google Takeout)		YES	YES
Chrome – Autofill, Browsing, Bookmarks, Passwords		YES	
Huawei Cloud	YES		
iCloud Applications	YES	YES	
iCloud Backup	YES		YES
iCloud Calendars	YES	YES	
iCloud Call History	YES		
Call Logs (iCloud)		YES	
iCloud Contacts	YES	YES	
iCloud Drive	YES	YES	YES
iCloud iTunes Store	YES		

iCloud Location		YES	
iCloud Mail			YES
iCloud Notes	YES	YES	
iCloud Photo Stream	YES		
iCloud Photos	YES	YES	YES
iCloud Reminder		YES	
iCloud Safari Bookmarks	YES	YES	
iCloud Safari History	YES	YES	
Safari Search (iCloud)		YES ^{li}	
iTunes purchases		YES	
Instagram	YES	YES	YES
Live Calendars	YES		
Live Contacts	YES		
MAIL (IMAP)	YES		
Mi Cloud	YES		
OneDrive	YES	YES	YES
Outlook Mail IMAP		YES	
QQ Mail	YES		
Samsung Cloud Backup	YES		
Samsung Cloud Data	YES		
Samsung Secure Folder	YES		
Swarm (Foursquare)	YES		
Telegram	YES	YES	
Twitter	YES	YES	YES

Viber (Google Backup)	YES		
Viber (iCloud backup)	YES	YES	
VKontake	YES	YES	
WhatsApp Cloud	YES		
WhatsApp Google Backup	YES	YES	
WhatsApp iCloud Backup	YES	YES	
WhatsApp (iCloud)		YES	
Windows Phone Cloud	YES		
Yahoo Mail (IMAP)		YES	
Hotmail			YES
IMAP Mail			YES
Live			YES
MSN			YES
Office 365			YES
Outlook		YES ^{lii}	YES
POP mail			YES
SharePoint			YES
Slack App ^{liii}		YES	
Lyft ^{liv}		YES	
Uber ^{lv}		YES	
Drone Apps ^{lvi}		YES	

Facial Recognition and Cloud extraction

The analysis of data extraction from mobile phones and other devices using cloud extraction technologies increasingly includes facial recognition capabilities. If we consider the volume of personal data that can be obtained from cloud-based sources such as Instagram, Google photos, iCloud, which contain facial images, the ability to use facial recognition on masses of data is a big deal. That it is potentially being used on vast troves of cloud-stored data without any transparency and accountability is a serious concern.

In August 2017 Cellebrite introduced what it called “advanced machine learning technology” for its analytics platform, which can be used to analyse data extracted from the cloud and which included face recognition and matching^{lvii}.

From July 2019, Oxygen Forensics JetEngine module, which is built into the Oxygen Forensic Detective, provides the ability to categorise human faces. Not only do Oxygen provide the categorisation and matching of faces within extracted data, facial analytics allows them to categorise gender, race and emotion recognition^{lviii}.

Lee Reiber, Oxygen’s chief operating officer said the tool can “search for a specific face in an evidence trove, or cluster images of the same person together. They can also filter faces by race or age group, and emotions such as “joy” and “anger”.”^{lix}

Oxygen Forensic® Facial Recognition

Available at **no additional** charge in Oxygen Forensic® JetEngine

15 million comparisons/second

One of the world's **most accurate** Facial Recognition algorithms*

DETAILED FACE ANALYTICS

- GENDER
- RACE
- AGE
- EMOTION

Facial recognition on **photos** and **videos** found in mobile, cloud or drone extractions

Identification of known individuals from images captured from mobile devices and cloud services in investigative cases.

Assistance in locating endangered children, human trafficking, etc by searching across all the images/videos in cases in Oxygen Forensic® JetEngine

Analysis of drone captured images and videos to identify possible known terrorists

*as measured by the National Institute of Standards and Technology (NIST)

Continual tracking

Once you have a users’ credentials, not only can you obtain their cloud-based data, you can track them using their cloud-based accounts. For example, the

capabilities of Cellebrite's Cloud Analyzer include the ability, once you have an individual's credentials, to:

"Track online behaviour. Analyse posts, likes, events and connections to better understand a suspect or victim's interests, relationships, opinions and daily activities."lx

This offers a very private insight into an individual's life. The individual themselves will never know that someone has access to and may be using their cloud profile.

Fulfill requests for cloud-based private data pursuant due process

Gather private user data with appropriate legal authority from over 50 of the most popular social media and cloud-based sources. Use login credentials provided by the subject, extracted from digital devices or PCs, retrieved from personal files or via other discovery means to gain access to time sensitive evidence. [See full list of cloud sources here.](#)

Visualize data in a unified format

Normalize different cloud data sources in a unified view to analyze by Timeline, File Thumbnails, Contacts or Maps formats. Search, filter and sort available data across platforms.

Search their searches

Gain insights into the subject's intentions and interests by pulling out the history of text searches, visited pages, voice search recordings and translations from Google web history and viewing text searches conducted with Chrome and Safari on iOS devices backed-up iCloud.

Collaborate and integrate data

Share critical evidence with team members by easily generating reports and exporting data into Cellebrite's Analytics Series or other advanced analytical tools for additional insights.

Capture and review public data

Easily access, view and incorporate publicly available data into your investigations, such as location information, profiles, images, files and social communications from popular apps, including Facebook, Twitter and Instagram.

Accelerate data collection from web pages

Acquire digital evidence from HTML-based web pages using an automated process to generate new leads and quickly corroborate statements and findings. Search, capture and forensically preserve web-based content in minutes and create powerful visual reports with captured screen shots and comments that can be easily explained to colleagues and juries.

Explore location history

Extract detailed location information from a suspect or victim's private Google Location History, so investigators can track time-stamped movements minute by minute.

Track online behavior

Analyze posts, likes, events and connections to better understand a suspect or victim's interests, relationships, opinions and daily activities.

CELLEBRITE CLOUD ANALYZER^{lx}

The short- or long-term monitoring of activity, particularly without possession of the phone and outside of what is on the device, is highly intrusive, and presents yet another worrying aspect of cloud extraction capabilities.

Not only can you track and monitor behaviour, messages and location data at any time, with their login credentials or ability to access their cloud-based accounts, you may be able to send messages, impersonate them, send mail with illegal content to someone else.

Conclusion

There is an absence of information regarding the use of cloud extraction technologies, making it unclear how this is lawful and equally how individuals are safeguarded from abuse and misuse of their data.

The volume of data that can be extracted from cloud services, the inclusion of facial recognition technology to analyse images and the implications for the large number of people whose personal data will be obtained even just extracting cloud data related to one individual make this a subject that deserves far greater transparency and accountability.

This is part of a dangerous trend by law enforcement agencies and we want to ensure globally the existence of transparency and accountability with respect to new forms of technology they use.

Recommendations

A search of a person's cloud-based data can be more invasive than a search of their home, not only for the quantity and detail of information but also the historical nature of legacy data and the future data that can continue to be analysed in the cloud. The state should not have unfettered access to the totality of someone's life and the use of cloud extraction requires the strictest of protections. Therefore, Privacy International recommends that:

- An immediate independent review be initiated into the use by law enforcement of cloud-analytics by relevant policing bodies and border control with consultations taken from the public, civil society and industry as well as government authorities.
- The police must have a warrant issued on the basis of reasonable suspicion by a judge before forensically examining any cloud-based data, or otherwise accessing any content or communications data stored therein.
- A clear legal basis must be in place to inspect, collect, store and analyse data from cloud-based services which provides for adequate safeguards to ensure intrusive powers are only used when necessary and proportionate. It must be considered whether such intrusive technology should only be used in serious crimes.
- Guidance aimed at the public regarding their rights and what such extractions involves must be published and provided to persons whose devices are to be analysed.
- Individuals be informed that their cloud-based data has been extracted, analysed and retained.

- Anyone who has their cloud-based data examined should have access to an effective remedy where any concerns regarding lawfulness can be raised.
- There must be independent oversight of the compliance by law enforcement of the lawful use of these powers.
- Cyber security standards should be agreed and circulated, specifying how data must be stored, how long it is to be retained, when it must be deleted and who can access it.
- All authorities who use these powers must purchase relevant tools through procurement channels in the public domain and regularly update a register of what tools they have purchased, including details on what tools they have, the commercial manufacturer and expenditure amounts.
- Technical standards be created and followed to ensure there is a particular way of obtaining data that is repeatable and reproducible, to ensure verification and validation. This should be accompanied, for example, by a clearly documented process.
- Technical skill is required as with this unprecedented amount of data comes the need for highly skilled forensic investigators. Consideration must be given to the risk of miscarriage of justice if raw data is misinterpreted or individuals cannot afford experts to review the data.
- Testing, trialling and deployment of cloud extraction technologies must be accompanied by impact assessments, adequate safeguards and engagement with the public and civil society.

ⁱ Cellebrite Annual Industry Trend Survey 2019: Law Enforcement [ONLINE] Available at: <https://www.cellebrite.com/en/insights/industry-survey/>

ⁱⁱ Cellebrite Annual Industry Trend Survey 2019: Law Enforcement [ONLINE] Available at: <https://www.cellebrite.com/en/insights/industry-survey/>

ⁱⁱⁱ Afonin, O (September 2018) Elcomsoft [ONLINE] Available at: <https://blog.elcomsoft.com/2018/09/cloud-forensics-why-what-and-how-to-extract-evidence/> [Accessed on 31 March 2019]

^{iv} Rozanski,S (May 2015) Beta News [ONLINE] Available at: <https://betanews.com/2015/05/27/forensic-investigations-retrieving-data-from-the-cloud/> [Accessed on 29 April 2019]

^v <https://privacyinternational.org/news-analysis/2901/push-button-evidence>

^{vi} <https://privacyinternational.org/campaigns/phone-data-extraction>

^{vii} <https://privacyinternational.org/news-analysis/2901/push-button-evidence>

^{viii} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.78

^{ix} The Cloud is essentially a server that is remotely accessed by another device, being your phone or an app on your phone.

^x <https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html>

^{xi} <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html>

^{xii} Cellebrite webinar (December 2018) [ONLINE] Available at: <https://www.cellebrite.com/en/webinars/building-an-investigation-using-social-media/> [Accessed on 20 December 2018]

Every 60 seconds there are 29 million WhatsApp messages sent, 500 hours of video are uploaded to YouTube, 149,513 emails are sent, 3.3 million Facebook posts, 65,972 Instagram photos are uploaded and 448,800 tweets are posted on Twitter.

^{xiii} Forensic Focus (February 2019) [ONLINE] Available at: <https://forensicfocus.com/News/article/sid=3390/> Accessed on 20 April 2019]

^{xiv} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.70

^{xv} Cellebrite Webinar, *How to incorporate cloud evidence into your investigations for maximum results* [2019] Available at: <https://www.cellebrite.com/en/webinars/how-to-incorporate-cloud-evidence-into-your-investigations-for-maximum-results/> [Accessed on 20 December 2019]

^{xvi} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.73

^{xvii} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.78

^{xviii} Elcomsoft Cloud Explorer (2019) Elcomsoft [ONLINE] Available at: <https://www.elcomsoft.co.uk/ecx.html> accessed on [1 April 2019]

^{xix} Release Notes (March 2018) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2018/03/UFEDCA7.1_ReleaseNotes.pdf [Accessed on 20 April 2019]

^{xx} Oxygen Forensic (undated) *Oxygen Forensic Detective Getting Started Guide* Available at: https://www.oxygen-forensic.com/en/uploads/doc_guide/Oxygen_Forensic_Detective_Getting_started2.pdf [Accessed on 3 March 2019]

^{xxi} Afonin, O (November 2018) Elcomsoft Blog [ONLINE] Available at: <https://blog.elcomsoft.com/2018/09/cloud-forensics-why-what-and-how-to-extract-evidence/> [Accessed on 23 March 2019]

^{xxii} <https://www.ft.com/content/95b91412-a946-11e9-b6ee-3cdf3174eb89>

^{xxiii} Business Insider (2019) [Online] Available at: <https://www.businessinsider.com/nso-boasted-it-can-hack-apple-google-amazon-cloud-servers-2019-7?r=US&IR=T>

^{xxiv} Cellebrite (2019) [ONLINE] Available at: <https://www.cellebrite.com/en/products/ufed-cloud-analyzer/> [Accessed on 30 March 2019]

^{xxv} Cellebrite (2019) Cellebrite [ONLINE] Available at: <https://www.cellebrite.com/en/products/ufed-cloud-analyzer/> [Accessed on 12 March 2019]

^{xxvi} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.78

^{xxvii} Cellebrite webinar (December 2018) [ONLINE] Available at: <https://www.cellebrite.com/en/webinars/building-an-investigation-using-social-media/> [Accessed on 20 December 2018]

^{xxviii} Cellebrite webinar (December 2018) [ONLINE] Available at: <https://www.cellebrite.com/en/webinars/building-an-investigation-using-social-media/> [Accessed on 20 December 2018]

^{xxix} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.78

^{xxx} Oxygen Forensic Cloud Extractor <https://www.youtube.com/watch?v=PjSmZkt87Dw>

^{xxxi} <https://www.magnetforensics.com/blog/how-to-acquire-and-analyze-cloud-data-with-magnet-axiom/>

^{xxxii} Cellebrite Product Release Notes <https://www.cellebrite.com/en/support/product-releases/>

^{xxxiii} Goldberg, M (March 2018) Cellebrite webinar [ONLINE] *Leverage the IoT to close cases faster* Available at: <https://www.cellebrite.com/en/webinars/leverage-the-iot-to-close-cases-faster/> [Accessed on 19 September 2018]

^{xxxiv} Goldberg, M (March 2018) Cellebrite webinar [ONLINE] *Leverage the IoT to close cases faster* Available at: <https://www.cellebrite.com/en/webinars/leverage-the-iot-to-close-cases-faster/> [Accessed on 19 September 2018]

^{xxxv} Blog (February 2019) Oxygen Forensic [ONLINE] Available at: <https://blog.oxygen-forensic.com/digital-assistants-the-new-eye-witness/> [Accessed on 20 April 2019]

^{xxxvi} Forensic Focus (February 2019) [ONLINE] Available at: <https://forensicfocus.com/News/article/sid=3390/> Accessed on 20 April 2019]

^{xxxvii} Forensic Focus (February 2019) [ONLINE] Available at: <https://forensicfocus.com/News/article/sid=3390/> [Accessed on 20 April 2019]

^{xxxviii} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.81

^{xxxix} Release Notes (January 2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2018/12/ReleaseNotes_UFEDCloudAnalyzer_7.6.pdf [Accessed on 4 February 2019]

^{xl} The Statistics Portal [ONLINE] Available at: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

-
- ^{xli}Smith, C (April 2019) DMR [ONLINE] Available at: <https://expandedramblings.com/index.php/amazon-statistics/> [Accessed on 25 April 2019]
- ^{xlii} Cellebrite Product Releases <https://www.cellebrite.com/en/support/product-releases/>
- ^{xliii} Cellebrite Product Releases <https://www.cellebrite.com/en/support/product-releases/>
- ^{xliiv} Cellebrite Product Releases <https://www.cellebrite.com/en/support/product-releases/>
- ^{xliv} Release Notes (January 2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2018/12/ReleaseNotes_UFEDCloudAnalyzer_7.6.pdf [Accessed on 4 February 2019]
- ^{xlvi} *ibid*
- ^{xlvii} Release Notes (January 2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2019/08/ReleaseNotes_CA_7.9-web.pdf [Accessed on 4 February 2019]
- ^{xlviii} Reiber, L, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation*, New York, McGraw Hill, 2019, p.78-80
- ^{xlix} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31.03.2019]
- ^l Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31.03.2019]
- ^{li} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31.03.2019]
- ^{lii} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31.03.2019]
- ^{liii} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31 March 2019]
- ^{liv} Product Update (2019) Cellebrite [ONLINE] Available at: https://cf-media.cellebrite.com/wp-content/uploads/2017/08/UFED_CloudAnalyzerSupportedDevices.pdf [Accessed on 31 March 2019]
- ^{lv} Cellebrite Release Notes, Release Version 7.6: UFED Cloud Analyzer, (January 2019) Cellebrite [ONLINE] <https://www.cellebrite.com/en/support/product-releases/> [Accessed on 31 March 2019]
- ^{lvi} Cellebrite Release Notes, Release Version 7.6: UFED Cloud Analyzer, (January 2019) Cellebrite [ONLINE] <https://www.cellebrite.com/en/support/product-releases/> [Accessed on 31 March 2019]
- ^{lvii} <https://www.cellebrite.com/en/press/cellebrite-introduces-advanced-machine-learning-technology-to-analytics-solution-to-accelerate-evidence-discovery/>
- ^{lviii} <https://forensicfocus.com/News/article/sid=3567/>
- ^{lix} https://www.wired.com/story/amazon-detect-fear-face-you-scared/?mbid=social_twitter_onsiteshare
- ^{lx} Cellebrite Cloud Analytics (2019) Cellebrite [ONLINE] Available at: <https://www.cellebrite.com/en/products/ufed-cloud-analyzer/> [Accessed on 20 December 2019]

^{lx} Cellebrite (2019) [ONLINE] Available at: <https://www.cellebrite.com/en/products/ufed-cloud-analyzer/> [Accessed on 2 May 2019]