Working Titles: Digital Evidence Moves to the Cloud

Cloud Forensics: Digital Evidence Recovery for 2020

Caption/Teaser: Online accounts like Google, iCloud, Dropbox, and others are emerging as best evidence sources when cell phones, tablets, and laptops are destroyed, damaged, or lost. Is it time lawyers look for evidence in the cloud first?

Author: John J. Carney, Esq., Chief Technology Officer
Carney Forensics, https://www.carneyforensics.com

Everyone in the U.S. has a smartphone today. Some of us have two, one for business, and one for our personal life. The average child begins using a smartphone at ten years old.

In the U.S. roughly 40% of us use iPhones, and 60% use Androids. Therefore, everyone in the U.S. has either a Google account or an iCloud account, and many of us have both. Why is that? Most Android smartphones connect to the user's Google account. And most iPhones connect to the user's iCloud account.

Why do smartphones connect to cloud accounts? There are four basic reasons.

- Sharing data with the user's other devices (tablet, laptop) and his or her family members.
- Storage and data management reasons. The user can backup data, messages, photos, and video to the unlimited capacity of the connected cloud account.

- Security and privacy reasons. The cloud provides a safe administrative interface for protecting the user's smartphone and then finding or wiping its precious data when lost.
- Financial reasons to include using the smartphone as a credit card (Apple Pay, Google Pay) and managing purchases from app stores.

Digital forensic examiners now collect evidence from web-based online, or "cloud" accounts, like Google, iCloud, and others for lawyers' clients. Increasingly it's a plan "B" for challenging litigation and investigations. Often smartphones, tablets, and laptops are destroyed, damaged, lost, or encrypted with a forgotten password. Backups of digital device evidence from the cloud, when forensically recovered, have the power to save a lawyer's case.

Today we see cloud evidence playing an important role in litigation and investigations equal to data recovered from digital devices. Cloud evidence is rapidly becoming "best evidence" for civil and criminal cases and is admissible in federal and state courts across the U.S.

Direct Cloud Evidence

Direct cloud evidence sources are subscribers' cloud accounts managed by Internet Service Providers, ISPs. They are preserved like any other electronically stored information usually with a preservation letter or litigation hold. Digital forensic examiners collect them using professional cloud forensic tools. ISPs will produce them on request by subscriber consent, subpoena, or court order. Often digital forensic examiners analyze subpoena returns from ISPs.

Web mail was perhaps the first cloud-based evidence source. AOL and Yahoo! Mail followed by Google Gmail and Microsoft Hotmail were the pioneers. Today every local ISP offers web mail. Microsoft developed Office 365 for the cloud and Google did the same for G Suite.

Social media emerged next in the cloud. Myspace and Facebook were first, but now Instagram, Twitter, LinkedIn, Pinterest, Reddit, and many others are discoverable.

Users began sharing documents, files, and folders in the cloud using Dropbox, the first popular offering, which was followed by Google Drive, Microsoft OneDrive, Box, and many others. Users share photographs online using Flickr, iCloud Photos, Google Photos, Amazon Photos, and many others all of which are forensically collected today.

Specialty cloud accounts abound for local community (Foursquare, Nextdoor, Yelp, Meetup), for dating (Tinder, OKCupid, Match.com, Bumble), and for professional networking (LinkedIn, Classmates.com, Scribd, WordPress, Blogger).

Cloud accounts exist for collaboration between companies and for employees and contractors within larger enterprises (G Suite, Office 365, SharePoint, Slack, Trello, Basecamp). Cloud accounts are often collected today instead of traditional email servers.

And evidence from new wearable devices, fitness trackers, and smart speakers can only be collected from their users' cloud accounts. These include Fitbit, Amazon Alexa, and Google Home.

Collecting Publicly Facing Cloud Evidence

Digital evidence posted on social media and blogs publicly available on the Internet has great potential to support investigations with new facts and insights. Digital forensic examiners collect it from sites like Facebook, Instagram, Twitter, WordPress, and Blogger using professional cloud forensic tools. They authenticate evidence by recording foundation for admissibility in court. Foundation includes metadata like site name, web address, date and time stamp, Internet Protocol (IP) address, geolocation (latitude/longitude), and one or more hash codes to record digital signatures of the publicly facing evidence collection.

Legal authority by subpoena, court order, or consent is unnecessary to collect publicly facing, online digital evidence in pursuit of investigations. Viewing or collecting publicly accessible online content for represented and unrepresented parties is fair game ethically. Oregon Ethics Opinion 2013-189 states it is comparable to reading a book or magazine article which the rules of professional responsibility do not prohibit lawyers or their nonlawyer agents from doing.

Consider popular public Facebook evidence and its potential for admission as one or more exceptions to the hearsay rule. Also its propensity to reveal character evidence and produce evidence deemed credible by the trier-of-fact.

- Party Admissions – Facebook's Posts, Comments, Friends, Friends of Friends, Friend Requests, Pokes.
- State of Mind – Facebook's Status Updates with date and time stamps.
- Character Evidence – Facebook's Photos, Videos, Likes, Apps.
- Credible Evidence – Facebook's Posts, Comments, Friends, Friends of Friends, Friend Requests, Pokes, Contact Info, Places.

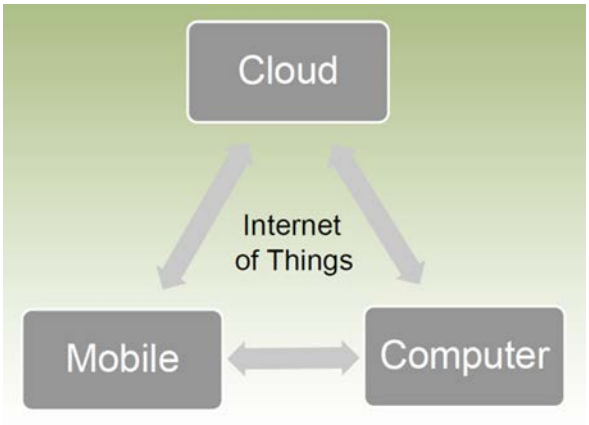
Collecting Private Cloud Evidence

Digital forensic examiners collect private cloud evidence with legal authorization using subscriber supplied or court ordered cloud account credentials from individuals, groups, or institutions.

Private evidence collections go beyond the limited scope of publicly available online evidence. They recover stored email, often called web mail. And they recover direct messages, which are private text messages between parties or correspondents. Facebook stores both email and direct messages (Facebook Messenger). Instagram, Twitter, Pinterest, LinkedIn, and Google all store direct messages besides publicly facing cloud evidence. And yet another group of cloud accounts store only direct messages (iCloud's iMessages, WhatsApp, Snapchat, Telegram, Viber, and others).

The news here for lawyers is twofold. 1) Email recovery is now as likely from a private cloud account as it is from a computer or server. 2) Text message recovery is now as likely from a private cloud account as it is from a smartphone.

Indirect Cloud Evidence



I have identified and explained direct sources of cloud evidence available today for forensic collection or return by subpoena power. But other, indirect sources of the user's cloud evidence are also available to lawyers through digital forensic techniques. These sources include the user's smartphone and computer, which when forensically collected, recover evidence remnants or traces of prior cloud access. The smartphone and computer serve as answers to digital interrogatories, if you will, about the user's cloud accounts. They highlight relevant cloud evidence. And they identify connections between the cloud and a smartphone, or between the cloud and a computer proving document movement or cloud-based activity relevant to the investigation.

I will expand on an integrated approach to digital evidence recovery focusing on cloud, mobile, and computer evidence in the next article in this series.