Social Media Investigations

- Eli Rosenblatt, iBridge Forensic & Fraud Examiner -

Part 1 : Down the Rabbit Hole

You may not have a “spirit animal” or know much about rodentology, but the best investigators I know are experts at “ferreting out” needed information.

As it happens, the analogy to this lithe, highly intelligent carnivorous mini-weasel is particularly apt when it comes to professional digital forensics and to ensuring the capture, ongoing collection, and presentation of relevant in-depth social network data. With their long, lean build, and inquisitive nature, ferrets are very well equipped for getting down circuitous holes and chasing elusive critters out of their burrows–just like us persistent investigators.In part one of this article, we look at how on our journeys down those burrows, we may be neglecting to retrieve (or lacking the best tools to retrieve) crucial nuggets that could make a real difference in the case at hand.

Certainly much of that data is junk. But the point is that now, there are more places than ever where data relevant to our case could be hiding. So as thorough and diligent as we professionals are, there's likely to be more digital evidence out there we've not yet uncovered.

Following a Digital Trail

Take a look at your current caseload. You may be researching, helping litigate, or otherwise investigating in a criminal defense, civil, workplace, insurance, or fraud case. Regardless of your caseload's makeup, you hopefully know that digital evidence is now a factor in every case.

With our highly surveilled, connected, and electronically-mediated environments, one would be hard-pressed to find a case where digital evidence didn't play some role. You may have a sense of this growth in your own work if you've been in practice since the fax machine (remember fax machines?), but most of us don't fully understand the full scope of the phenomenon.

The folks who track data proliferation globally, IDC, found in their recent study (and their archive of past years' installments of the study) that 2.8 zettabytes of data were created and replicated in 2012.

Most of us don't have a good sense of what 2.8ZB is, exactly. Take a look at that nice little 4-inch terabyte USB back-up drive sitting on your desk. Yes, that one. Don't unplug it! (You'll interrupt that crucial backup.) Now, multiply it in your mind by about 3 billion. If you lined those disks up, they would stretch 110,479.6 miles, or wrap around the equator more than 4 times.

By comparison, in 2005, there were about 130 exabytes of data created or replicated on all the computers and computing devices worldwide. Today the figure is 22 times larger than that. In 2020, it's expected to rise to 40 ZB, or 315 times larger than it was in 2005.

Certainly much of that data is junk. But the point is that now, there are more places than ever where data relevant to our case could be hiding. So as thorough and diligent as we professionals are, there's likely to be more digital evidence out there we've not yet uncovered. In my experience, many of those sources can be one or more of a panoply of social media services.

Unfortunately, discovery standards and professional norms regarding investigation of social media are still somewhat lacking in the breadth and depth necessary to establish reliable benchmarks for how to adequately capture and present all the available information. Those efforts need to take into account the new realities of the social networking landscape and why social media now plays a larger role in our investigations.

More people than ever before are spending more time using more social media services for more kinds of sharing than ever before.

More Users, More Data

More people than ever before are spending more time using more social media services for more kinds of sharing than ever before. (A recent mylife.com infographic details this.) Kids, octogenarians, and yes, even pets, can leave a long trail of potentially useful data. Now, investigators are using that data in more ways than ever.

The number of services in use–and the total number of users–have both grown tremendously in recent years, as seen on Wikipedia's (not complete but huge) list of social network sites. There's a handful of services that stand out, and there are some you might never have heard of, despite their having millions of users. Facebook and Twitter, of course, are the biggest players.

Right behind Facebook and Twitter is a true giant of social media data: YouTube. Videos hosted on YouTube may even have been entered as evidence in some of your cases. Statistics were recently released, however, which completely blew away my estimates of its ubiquitousness:

- More than 1 billion unique users visit YouTube each month.
- Over 4 billion hours of video are watched each month on YouTube.
- 72 hours of video are uploaded to YouTube every minute.
- In 2011, YouTube had more than 1 trillion views, or around 140 views for every person on Earth.
- Traffic from mobile devices tripled in 2011, with people now watching one billion views a day on YouTube mobile.

Emerging Networks

These giants will likely continue to dominate the social media landscape for some time to come, but diligence in this field demands we pay attention to a host of others, and as much as possible, stay up-to-date on emerging players.

The importance of this strategy was underscored recently in an article by Ryan Holmes, CEO of the social media management company Hootsuite. He pointed to the rocketing growth of Instagram, which went from a million users in December 2010 to 100 million users and 58 photo uploads per second just 24 months later.

Holmes looked at seven up-and-coming social networks which could be the next Instagram. That's interesting enough for its own sake, but for our purposes, they show how sources of potentially useful evidence crop up in the space of months, not over the course of years. And what's striking is how few of us are familiar with them.

We need take any practical steps to start with the subjects themselves and, through our investigation, determine what (if any) social network sites they may subscribe to.

The seven sites Holmes pointed to were:

- Pheed, a photo and video monetizing site;
- Thumb, a personalized crowdsourcing tool;
- Medium, an invitation-only social network;
- Conversations, a real-time collaboration tool by Hootsuite;
- Chirpify, a tool for purchasing via Twitter;
- Flayvr, an elegant photosharing platform;
- Chirp, a proximity message and photo sharing app.

Investigators: Have you used or at least visited one of these seven services? Two? Five? All seven?

For most of us, the answer is no. What this shows us is that when deciding what social media to search for possible evidence in a case, it's getting to the point where it's not enough to simply check out the top sites to see if perhaps our subject has an account on one.

If you're not looking closely into social media as a central source of information for workplace investigations, you could be doing your client a real disservice by ignoring a huge pool of potentially useful data.

Instead, as much as possible, we need take any practical steps to start with the subjects themselves and, through our investigation, determine what (if any) social network sites they may subscribe to.

In the Courtroom

A growing number of civil and criminal court cases involve social media evidence in some way. Some have even hinged on it. E-Discovery experts studying this closely over the last few years found 689 state and federal court cases during 2010 and 2011, which they believe represent a fraction of cases that in some way directly involved social media evidence (not counting all the cases where social media was merely mentioned or brought up in passing but didn't play a central role). Then last year, we see an explosion. During just the first half of 2012, they found another 320 cases filed nationwide. (See X1 Discovery's list of social media-related cases.)

If you're not looking closely into social media as a central source of information for workplace investigations, you could be doing your client a real disservice by ignoring a huge pool of potentially useful data. Whether you tease out just a "like," find some comments on the page of a contact, or uncover many pages of ranting, social media data of all kinds can have a crucial impact.

Jessica Miller-Merrell's compilation of terminations and firings related to social media activities goes back to 2002 and underscores how essential these investigations can be in any workplace case you may be working.

Investigators may not need to be as concerned with legal privacy issues as attorneys, but there are a few important details to keep in mind when conducting thorough social media investigations:

1. Do not delete the evidence

First, as was sharply illustrated in the case of Lester vs. Allied Concrete, an attorney or his agent can't advise a client to "clean up" or delete the client's social media postings or accounts. This is called spoliation of evidence and it could cost you dearly.

2. Observe privacy laws

Second, there are some complex issues surrounding access that employers may or may not have to an employee's social networking content–postings that are password-protected may be covered by federal privacy laws. Do your due diligence and work with legal counsel to establish boundaries and guidelines on any workplace investigations.

3. Restrict your search to information that's publicly available

Third, conduct your investigation in a way that is transparent and strictly legal. Here's how I phrase this to clients when they ask about what I can and cannot access: The methods and tools I use only capture and index publicly available information from social network sites and any publicly available web postings.

I do not use any pretexting, subterfuge, password cracking, social engineering, or otherwise unethical means to gain access to protected material. (The ethics of these practices are still unfolding in the world of online investigations, but another personal rule for me is "better safe than totally screwed.")

Depending on the particulars of your case, you may indeed be able to capture, index, and prepare privately protected material, using the login credentials provided by a cooperating client or witness (provided that client or witness signs an authorization for release of information). But you'll need to proceed very carefully and work closely with an attorney when treading into these murky legal waters.

In the next segment, we'll be peeling back the layers of social media investigations, looking more closely at lessons from recent cases, and why screenshots are just not good enough.

Part 2 : Peeling Back the Layers

When it comes to sleuthing social sites, getting a screenshot of a Facebook post doesn't cut it. In some cases, you may need to establish relevance before you investigate a site, and you'll need more than just a person's posts—you'll need the underlying metadata. In part two of this article, we explore recent case law and identify some best practices for collecting, authenticating, and preserving social media evidence in civil and criminal cases.

If you have worked backgrounds in a case, you've no doubt come across some interesting or potentially damaging information on Facebook or another network. No doubt your boss or client instructs you to "grab a screenshot of that witness' Facebook wall." Well, that may work in a pinch to get you started, but in the new reality of social media evidence, it just isn't enough.

In part one, we looked at how extensive social media has become and how it's no longer sufficient to just look for evidence on Facebook or Twitter. As much as possible, we need to start with our target, and work our way out to discover other services they might use. We also reviewed some general best practices. But now it's time to go even deeper, to explore aspects which few investigators, attorneys, or other professionals have had a chance to fully grasp.

Social Media Evidence and the Law

Legal challenges regarding the authentication and preservation of social media evidence are becoming more commonplace. In a recent article and white paper, e-discovery experts illuminated these challenges in all their gory details, but we'll highlight some of the more important ones that investigators should be aware of here. Note that metadata (which e-discovery and data storage nerds call "a little love letter to the future") is central to many of these cases.

1. Failure to Authenticate

In a heavily discussed Connecticut case, State vs. Eleck, the court rejected Facebook evidence in the form of a simple printout for inadequate authentication. The court noted that it was incumbent on the party seeking to admit the social media data to offer detailed "circumstantial evidence that tends to authenticate" the unique medium of social media evidence.

2. Authenticate or Perish

In another case which highlighted the need for proper authentication, the Texas appellate court noted in its Rene v. State decision that the prosecution offered minimal circumstantial evidence to establish the authenticity of the MySpace pages and no evidence to demonstrate that the photos were not altered.

3. Metadata Matters

In the Dallas, Texas gang-related murder trial State vs. Tienda, the drive-by suspect and defendant Ronnie Tienda posted a number of incriminating posts on his MySpace page. The prosecution succeeded in getting the court to admit printouts of Ronnie Tienda's MySpace page over the defendant's objections, laying a foundation through various pieces of circumstantial evidence.

Among this key evidence were relevant metadata fields along with other corroborating information. Despite having won at trial and on appeal, the prosecution faced an uphill battle. The case illustrates how relying on simple printouts of social media site pages would not have succeeded in getting the court to admit crucial evidence. Instead, to reliably succeed in cases involving Facebook, MySpace, Twitter, or other sites, the parties producing social media evidence need to ensure that supporting metadata and other key circumstantial evidence is properly and comprehensively collected.

4. Collect and Catalogue

AmA New York case, Richards v Hertz Corp., was filed last year that represents the tip of a huge iceberg. That iceberg is made up of tons of cases (including a very similar case that garnered attention, Loporcaro v. City of New York et al.) that underscore the importance of having tools for collecting, indexing, searching, preserving, and authenticating social media evidence. In Richards v Hertz, the plaintiff claimed that her injuries from an auto collision impaired her ability to participate in sporting activities and caused her to suffer pain that was exacerbated in cold weather.

The defense investigated the plaintiff's online presence, and what did they find? Yes, publicly available Facebook images "depicting [plaintiff] on skis in the snow," and subsequently served a discovery demand requesting all her status reports, email, photos, and videos posted on her account since the date of the collision.

5. Preserving Virtual Evidence

A case in Virginia last year highlighted the importance of properly preserving social media evidence. In Bland v. Roberts, one of the most important elements of the case was whether or not subjects had "liked" a particular post. With this and other similar cases, we've seen that something as small and innocuous-seeming as liking a Facebook entry can be an important piece of evidence in a wide variety of litigation and investigation scenarios.

The court ruled that while social media is clearly discoverable, there must be some showing of relevance before the court moves to compel full production of a litigant's Facebook account.

6. Establishing Relevance

The importance of collecting and preserving social media in a native, scalable, and searchable format was also underlined last year in a decision by Federal District Court in Michigan (Tompkins v. Detroit Metropolitan Airport). The court ruled that while social media is clearly discoverable, there must be some showing of relevance before the court moves to compel full production of a litigant's Facebook account.

The plaintiff suffered a slip-and-fall and later claimed back and other injuries. She sued her employer, who sought full access to her Facebook account in the course of discovery. In their ruling, the court noted that while "material posted on a 'private' Facebook page…is generally not privileged, nor is it protected by common law or civil law notions of privacy," an opposing party does not "have a generalized right to rummage at will through information that Plaintiff has limited from public view. [T]here must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence."

However, far from completely closing the door on full disclosure of social media accounts, the court noted: "If the Plaintiff's public Facebook page contained pictures of her playing golf or riding horseback, Defendant might have a stronger argument for delving into the non-public section of her account. But based on what has been provided to this Court, Defendant has not made a sufficient predicate showing that the material it seeks is reasonably calculated to lead to the discovery of admissible evidence."

7. When Facebook Is Discoverable

A products liability case last year from Nevada, Thompson v. Autoliv, was another personal injury claim where the claimant's public Facebook postings contradicted her assertion she'd suffered a serious injury. The defendant sought a court order compelling the plaintiff "to produce complete and un-redacted copies of [her] Facebook and other social networking site accounts."

The defense based its motion on the plaintiff's publicly available Facebook wall posts and photographs that contradicted her claims of serious injury (and which the plaintiff changed her privacy settings to conceal shortly thereafter). The court found the plaintiff's Facebook account discoverable and compelled its production.

When social media is collected with a proper chain of custody and all associated metadata is preserved, authenticity is much easier to establish.

Chains of Custody and Metadata in Social Media Evidence Collection

A number of these examples were civil, but of course as we've learned, social media evidence plays an essential role in an overwhelming number of criminal cases as well. In November of last year, eDiscovery experts compiled some of the best examples of these, and wrote an article highlighting the ways that 5 representative cases further showed the importance of social media in the courts.

So, to properly address these authentication and preservation challenges, social media data must be properly collected, preserved, searched, and produced in a manner that's consistent with best practices so that all available circumstantial evidence is available, including metadata. When social media is collected with a proper chain of custody and all associated metadata is preserved, authenticity is much easier to establish.

When you look at (or take a screenshot of) a Facebook photo or status update, what you are getting is merely content, not underlying corroborating evidence. The metadata that lies "beneath" that photo or posting is crucial. Looking in detail at all of the available metadata fields is beyond our scope here, but some of the key ones include the obvious necessary items such as user name, posting date, time, ID, and recipients.

Beyond this, however, there are many others that can be tracked such as:

- The unique ID of the message thread which that posting belongs to;
- URLs of any included links within the posting;
- The platform and applications that were used to create the posting;
- The number of comments posted in relation to this posting.

Taken together (and compared to other evidence, be it digital or non-digital), these forms of metadata can provide important information to establish the authenticity of a

post, if they are properly collected and preserved. Any one or combination of these fields can be key circumstantial data to authenticate a social media item, or constitute substantive evidence in and of itself. (Twitter, LinkedIn, and other services' postings have their own unique but generally comparable metadata.)

Techniques, Tools, and Terminology

So, why do we want to use special tools or techniques when collecting social media data? The short answer is this: When you are doing screenshots, you are not collecting all the juicy bits under the surface, or the "digital fingerprints."

So, why do we want to use special tools or techniques when collecting social media data? The short answer is this: When you are doing screenshots, you are not collecting all the juicy bits under the surface, or the "digital fingerprints."

In addition to collection of all such key metadata, it is important that MD5 hash values of each social media item are automatically generated at the time of their collection. (For those of you who might not know that term, hash values are the long string of numbers that uniquely identifies an item of digital content).

It's also important to generate unique case information that will support a proper chain of custody.

Unfortunately, many ad hoc measures currently used to collect social media for use in court do not meet these requirements. Screen capture tools and many archive services, when they capture social media items, just don't collect most available metadata or generate hash values for individual social media items.

Working with a professional who can ensure that social media evidence will be handled according to these best practices is essential. Here are a few important factors to consider when choosing a provider to work with:

• Reliability of authentication: Does the provider have the right tools and knowledge to capture and index all the needed social media evidence in a way that will maintain crucial metadata, identifiers, or other digital "fingerprints" (doing so in a "read-only" way, without risk of altering the original information or raising the awareness of the posting subject)?

• Speed: How quickly can the provider search for relevant terms and return needed reports?
• Scalability: Can the provider accurately and reliably handle searches that range from one simple term on the page of a single subject all the way to dozens of complex strings amongst tens of thousands of social media postings strewn across the various sites of dozens or

hundreds of witnesses?

Summary

Traditional capture techniques, such as logging in with a fake or one-off account and taking screenshots, may suffice for an initial look (though as we discussed last time, tread carefully here). But given this new landscape, a comprehensive analysis and deeper integration are necessary in most of today's civil and criminal cases.

Many of you have had at at least one mega-case where the volume of emails, documents, photos, and spreadsheets threatens to overwhelm you. Some of you may work only mega-cases like this. (My heart goes out to your families.) But you no doubt use some excellent software and/or databases (such as Casemap, iConnect, Relativity, Equivio, or others, or even well-developed Excel files) to help your team manage this mountain of information.

Fortunately, tools are now being developed that are specifically designed to effectively address this proliferation of social media content from sites such as Facebook, Twitter, LinkedIn, YouTube and more.

The trouble is that until recently, there have not been adequate tools for systematically capturing and integrating social media data into a team's workflow. Fortunately, tools are now being developed that are specifically designed to effectively address this proliferation of social media content from sites such as Facebook, Twitter, LinkedIn, YouTube and more. If your firm is in need of such tools, contact a social media investigations professional to learn how they can help you navigate the new social media landscape and get the hidden information you need.

About Eli Rosenblatt and iBridge
Eli Rosenblatt is a Certified Forensic Examiner, Certified Fraud Examiner, and licensed investigator. iBridge is a locally-based provider of forensic and eDiscovery services.

If you would like to learn more about
how iBridge can help you with
your digital forensics,
please contact us.

info@ibridgellc.com
503.906.3930

Follow us!