Social Media and Forensics:
How Digital Investigations Peel Back the Layers in Today's Complex Cases

by Eli Rosenblatt CFE, CFI, MiCFE, SMIA, SMFI, CCDI, ACSP

Presentation Notes

- Stereotypes, Myths, and Misconceptions (re professional investigators via Pursuit Magazine).
- In all our cases, crucial elements include:
  - Who generated or knew the information?
  - When did they generate or learn it?
  - How did that information get broadcast or transferred?
- In our investigations, 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. Digital evidence is now or can be a factor in **every** case, no matter what.
- IDC found in their recent study (and their archive of past years installments of the study) that 4.4 zettabytes of data were created and replicated in 2013.
- Terabytes >> petabytes >> exabytes >> zettabytes. In 2005, about 130 exabytes of data. Now nearly 35 times larger, 4.4 zettabytes. In 2020, it's expected to rise to 44 ZB, or 346 times larger than in 2005.
- Huge change in size & cost for data storage; cloud computing/BYOD also changed how we work.
- Holes in our digital evidence often where we'd find potentially useful data, often from multitude of social media services.
- Discovery standards regarding social network data are still somewhat lacking in the breadth and depth necessary to adequately capture and present available information. Collection and presentation efforts need to take into account the new realities of the social networking landscape:
  - More users, more services, more sharing: (see Wikipedia's (not complete but huge) list of social network sites and this slightly dated infographic, and mylife.com infographic).
  - Therefore more investigations: see the compilation of firings for social media activities, 81% of AMA members report social media info in their divorce cases (as seen at totaldivorce.com)
  - The tragic & personal to the screens of millions: Casey Anthony; Stuebenville Ohio rape case; Parish Bennette.
  - Facebook and Twitter biggest players but many others with millions of users.
  - Right behind is giant of social media data: YouTube. Stats:
    - More than 1 billion unique users visit YouTube each month

12725 SW Millikan Way, Suite 200, Beaverton OR 97005 | Office: 503.906.3930 | Fax: 503.906.3931 | Email: info@ibridgellc.com | www.ibridgellc.com

    - Over 6 billion hours of video are watched each month on YouTube
    - 100 hours worth of video are uploaded to YouTube every minute
    - In 2011, more than 1 trillion views or around 140 views for every person on Earth
    - Traffic from mobile devices tripled in 2011, now one billion views/day on YouTube mobile.
  - 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.
  - Importance of this strategy underscored recently in article , pointed to the rocketing growth of Instagram: 1 million users in 12/10 to 100 million users & 58 photo uploads/second in 12/12.
  - Looked at up-and-coming social networks which could be the next Instagram (sources of potentially useful evidence can crop up in the space of months, not over the course of years). Few of us familiar with them: Photo and video monetizing site Pheed, personalized crowdsourcing tool Thumb, invitation-only social network Medium, social learning platforms Sulia and Learnist, (Portland) purchase-via-twitter tool Chirpify, photosharing platform Flayvr, proximity message and photo sharing app Chirp, video microblogging service Keek, and the minimalist blogging service Ghost.
- When deciding on what social media to look for as possible evidence in a case, not enough to simply search the top sites to see if perhaps our subject has an account on one of those sites. Instead, or in addition to this, need take any practical steps to start with the subject themselves and through our investigation, determine what if any social network sites they subscribe to.
- Growing number of court cases involve social media evidence. Some 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 represent a fraction of cases which in some way directly involved social media evidence. Then,during the first half of 2012, another 320 cases filed nationwide (see X1 Discovery's list of social media-related cases).
- Legal challenges regarding authentication and preservation of social media evidence are becoming more commonplace (more details in an article and a white paper from X1 Discovery):
  - In heavily discussed Connecticut case, State vs. Eleck, court rejected Facebook evidence in the form of a simple printout, for failure of adequate authentication.
  - Rene v. State, prosecution offered minimal circumstantial evidence to establish the authenticity of the MySpace pages and no evidence to demonstrate that the photos were not altered.
  - In the Dallas, Texas gang-related murder trial State vs. Tienda, the drive-by suspect and defendant posted incriminating posts on MySpace; prosecution was successful in getting the court to admit printouts of Ronnie Tienda's MySpace page over the defendant's objection, laying a foundation through various pieces of circumstantial evidence.

12725 SW Millikan Way, Suite 200, Beaverton OR 97005 | Office: 503.906.3930 | Fax: 503.906.3931 | Email: info@ibridgellc.com | www.ibridgellc.com

- Cases where plaintiff's online postings seemed to contradict their assertions that they'd suffered serious injury: Richards v Hertz Corp., Tompkins v. Detroit Metropolitan Airport, Thompson v. Autoliv (tip of iceberg). These underscore how important to have tools for collecting, indexing, searching, preserving, and authenticating social media evidence.
- In Bland v. Roberts, the case basically hinged on whether or not certain witnesses had "liked" a particular Facebook post.
- A number of these examples were civil, but of course social media evidence plays an essential role in an overwhelming number of criminal cases as well. In November of last year, eDiscovery experts compiled best examples of these, wrote an article highlighting the ways that 5 representative cases further showed the importance of social media in the courts.
- Also articles on this from law and scholarly journals: (Westlaw links)
  - Understanding and Authenticating Evidence from Social Networking Sites
  - Tips for Authenticating Social Media Evidence
  - Social Media and the Rules on Authentication
  - What Happens on MySpace Stays on MySpace: Authentication and Griffin v. State
  - Internet, Email, and Social Media Evidence

- Screenshots not enough today! To properly address authentication and preservation challenges, social media data must be properly collected, preserved, searched, and produced in a manner consistent with best practices so all available circumstantial evidence is collected, 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.
- Why use special tools or techniques when collecting social media data? Short answer: When doing screenshots, 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 (MD5 is a cryptographic function commonly used to check data integrity).
- 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, don't collect most available metadata or generate hash values for individual social media items. (The Facebook self-collection mechanism currently will not collect most available metadata information, will not generate hash values, and will only provide content from the user's own account while omitting content contributed by that user to their friend's account, such as their "walls.")

12725 SW Millikan Way, Suite 200, Beaverton OR 97005 | Office: 503.906.3930 | Fax: 503.906.3931 | Email: info@ibridgellc.com | www.ibridgellc.com

- Working with a professional who can ensure that social media evidence will be handled according to these best practices is essential. 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?
- Lessons learned in doing all kinds of investigations, that especially apply to social media investigations:
  - Never underestimate the lengths some people will go to, or that you'll have to go to to unearth crucial information.
  - Ridiculous to assume any kind of investigation could be conducted entirely based on what's found on social media. However, investigation can be hurt dramatically by forgetting to look for easy stuff, or by incorrect assumption that everybody these days locks down their privacy settings on the social media services they use (not the case).
  - Metadata. Watching out for it, working with an expert who can correctly interpret, index, search, maintain, and present it could be amazingly useful. Failing to understand and account for metadata can unravel and utterly destroy your investigation altogether.
- Traditional capture techniques, such as logging in with a fake or one-off account, taking screenshots, may suffice for initial look (though as discussed in my article, tread carefully here). But given this new landscape, a comprehensive analysis and deeper integration are what is needed in most of today's cases. In mega-cases, the number and volume of emails, documents, photos, and spreadsheets threatens to overwhelm you. 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.
- But until recently, there have not been adequate tools for systematically capturing and integrating social media data into a team's workflow. Fortunately, tools now being developed specifically designed to effectively address this proliferation of social media content from sites such as

12725 SW Millikan Way, Suite 200, Beaverton OR 97005 | Office: 503.906.3930 | Fax: 503.906.3931 | Email: info@ibridgellc.com | www.ibridgellc.com

Facebook, Twitter, LinkedIn, YouTube and more. A social media investigations professional can help navigate the new social media landscape and get the hidden information you need.

Slideshow photo credits:

- Ferret CC photo by Duncan McNeil
- courthouse CC by Jimmy Emerson
- Magnifying Glass CC designed by Carol Santos from The Noun Project (hereafter NP)
- Gun designed CC by Simon Child, NP
- Skier CC by Samal Bemen-Benrud
- Thumbs Up designed by Nick Holroyd NP
- Slipping designed by Luis Prado, NP
- Crutch designed by Olivier Guin, NP
- Roller Derby photo used with explicit permission to use and alter, with attribution, from Rick A. Brown (email of 04/08/13)
- Cost per GB graph by Matthew Komorowski, mkomo.com
- Fujitsu HD image Wikimedia CC by PJ & Piko
- Floppy image Wikimedia CC by Andreas Frank
- Dime & SD Card CC by Alvin Trusty
- Cheetah CC by William Warby
- Tools ("Scalability") CC by Robby van Moor
- Information designed by Phil Goodwin, NP
- Paper designed by Zach Vandehay, NP
- Business person designed by Murat Yalcin, NP
- Clock designed by Vasu Adiga, NP
- Megaphone by Natasha Fedorova, NP
- Binder CC by Jonathan D. Blundell
- Road CC by Stuck in Customs
- Gun CC by The Knowles Gallery
- Brutus CC by Casandra Caras
- Charted CC by Shelah Gosheshe
- *NOTE: all other images not listed above are licensed as royalty-free or free for non-commercial use.*

Presentation and notes are licensed under:

Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

12725 SW Millikan Way, Suite 200, Beaverton OR 97005 | Office: 503.906.3930 | Fax: 503.906.3931 | Email: info@ibridgellc.com | www.ibridgellc.com