Legal Investigation in Social Media: How to Do It; How Not to Do It

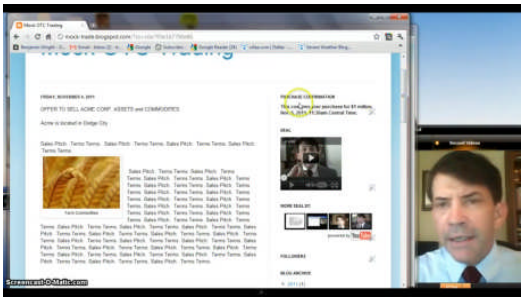
Benjamin Wright, Attorney
SANS Institute: "Law of Data Security & Investigations"
This is not legal advice.

Many Social Networks

- Facebook, Twitter and LinkedIn are just a part of the topic
- Many new social networks, like Google Plus, Quora, Instagram, Groupon, Pinterest, LoveIt
- Thousands of blogs and special interest forums

Screencast

- Captures the look, the words, the images, the interactivity and inter-relationships from one page and link to the next
- Captures webcam narration by witness – which can be compelling to judge and jury
- Free, open-source tool: screencast-o-matic.com



Many Posts and Demos of Screencast Evidence Capture

- http://bit.ly/e825MF - live chat
- http://bit.ly/ePV9E0 - web activity
- http://bit.ly/w3swEC - online financial trades
- http://bit.ly/nsZ6ZG - undercover police in social media
- I welcome your comments, questions and criticism!

Investigative/Recording Tools

- Vere Software
- X1 Discovery
- Hashbot
- Iterasi web archiving service
- Cernam Capture & Preserve
- Others
- Each works differently
- Regardless, an affidavit from a witness is helpful.

Hook into APIs & Collect Meta Data

Consider Terms of Service

- Platform application developers and operators http://www.facebook.com/legal/terms
- Post privacy policy
- "You will delete all data you receive from us concerning a user if the user asks you to do so, and will provide a mechanism for users to make such a request. … You will make it easy for users to remove or disconnect from your application."

General Facebook Terms

- http://www.facebook.com/legal/terms
- "If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it."

Interpretation

- Does this mean no one can, without consent, copy something from Facebook for purposes of an investigation?
- I think not.
- Making limited copies is generally accepted practice.
- But the principle of "proportionality" is relevant.

Admission of Evidence

- Social media evidence is **very commonly** admitted into legal proceedings
- Varying degrees of formality in proceedings
- However, some criminal cases show skeptical courts
- Criminal cases have higher standard of proof

Authenticate Facebook

- *State v. Eleck*, AC 31581 (Conn. Ct. App. Aug 9, 2011) - Witness says she did not talk to defendant after an assault. But defendant shows Facebook messages appear from witness to defendant after assault. Witness suggests someone could have hacked her account. Court: Facebook messages inadequately authenticated.

Recent Litigation: Law Enforcement Demands

- *People v. Harris, Criminal Court of the City of New York*, No. 2011NY080152
- Law enforcement subpoena can force twitter to disclose both content and non-content that's older than 180 days
- Law enforcement needs search warrant for content less than 180 days old
- 7-20-12: Twitter appeals http://goo.gl/Hulvw

Alternative Ways to Authenticate Evidence

- Interact with the user (if permitted)
- Gather corroborating detail about user statements, activities and timeline
- Corroborating details can be collected from multiple sources (Facebook, Twitter, special interest forums, games, phone, witnesses and so on)

Risks: Ethical Limitations

- New York State Bar Ethics Opinion 843 (9/10/2010); NY City Bar Formal Opinion 2010-2; San Diego County Bar Opinion 2011-2
- Lawyers may view public postings of adversaries
- May not friend an adversary represented by a lawyer
- May not use deception to friend someone

Illegality and Impersonation

- California Penal Code 528.5: "any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense."

Managing Risk: Interview the Subject First?

- A formal HR interview or deposition puts pressure on subject to tell the truth
- Yes, subject could delete data, but
  - Deletion of data itself is evidence of wrongdoing that could hang the subject
  - Deleting data is harder than it looks because copies are spread everywhere

Power of a Preservation Letter

- Letter puts adversary on notice not to destroy records
- Focuses the adversary's attention electronic evidence and all the steps that might be necessary to preserve
- http://bit.ly/A5XrGH

Legal Steps to Access Non-Public Data

- Consent of the user
- E-discovery demand to user
- Informal request to social network
- Subpoena to social network
- Search warrant for law enforcement
- Find the data in an alternative, public location

Civil Subpoenas for Content

- Big service providers tend to resist
- Smaller service providers may be more cooperative
- *Crispin v. Christian Audigier, Inc.*
  - Civil subpoena to FB and Myspace quashed
  - Content protected under Stored Communications Act
  - May be difference between private messages and wall postings

Alternative Locations for Evidence

- Notices and copies to email or phone SMS (text)
- Replication at other sites (my Facebook and LinkedIn repeat my tweets)
- Sharing by friends
- Cache on computer

Finding Web History

- http://www.toddington.com/wp/internet-research-tools
- Archive.org – Waybackmachine
- http://mementoweb.org/

Blog: benjaminwright.us