Compliance & Ethics Professional®

September 2017

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Lillian Wylie

Compliance Manager
Oceaneering International Services Ltd
Aberdeen, United Kingdom

See page **16**

by Dan Coney, CCEP, CFE, CFCS

Capturing true value in social media investigations

» Social media has become so prevalent in society that not having the means to include this in your investigative planning is to overlook a potential treasure trove of incriminating evidence.

» Access issues are the first consideration in planning and pose an ethical risk if done improperly.

» Intent and knowledge evidence are key nuggets that can be developed out of social media.

» The inefficiencies of hunting for the needle in the haystack are too costly, so the only answer is software that aggregates web-based content and automatically conducts user-designed searches.

» Investigators must keep their eye on employing the best methods of collection to address authentication and chain-of-custody issues with electronic evidence.

Sleuthing in the digital age makes for less wear and tear on the gumshoe. More and more, evidence comes in the form of zeroes and ones. The explosion of electronic devices, both at home and work, means potential evidence is ubiquitous and mobile. This will only grow with the proliferation of cloud-based computing and device miniaturization. It is estimated that every adult in the developed world generates 1.8 terabytes of data annually as of 2012, but the information available *about* a person is 4.1 terabytes.[1] It is obvious that your investigation will likely result in the consideration of social media as a source of evidence.

Coney

Investigative planning is a wonderful process, because there you have to think through the how of your objective. There often is a point of realization that as much as you know about our data-driven world, when it comes to real understanding, most of us are ill-equipped to handle it. The questions you need to ask are both basic and vexing, partly because technology quickly changes. Here are considerations for diving into the social media pool.

Access issues

Puzzle with me over the first logical question concerning social media: how do I get my hands on it? There is some public-facing information that a simple Google search might pull up. If your culprit is lazy or not particularly informed, their privacy settings might allow you to see everything on that person's page. An estimated 25% of all Facebook users do not utilize privacy controls.[2] However, if there is one thing I have learned about people involved in misconduct—they are awfully particular about their privacy.

Be wary of ruse "friending" to try to penetrate a suspect's privacy settings. Akin to the pretexting debacle in 2006 involving Hewlett-Packard, and more recently with Uber,[3] this kind of subterfuge could run afoul of ethical obligations. Pretexting is illegal in some contexts, such as obtaining

financial records[4] or telephone records,[5] and is a small leap to applying these standards to social media, where one could stumble across medical and other private information. Also pay attention to the terms of use of the various social media sources. Since 2011, the Electronic Frontier Foundation has strongly objected to law enforcement ignoring Facebook's rules against using false names to create an account. In October 2014, Facebook wrote a "strongly worded letter" to the Drug Enforcement Administration (DEA) concerning the practice,[6] and the incident that provoked the letter resulted in the DEA settling a lawsuit for $134,000.[7] All this to say, you need to know enough not to fall into one of these ethical traps.

So the question of access is an important one, for the value of the evidence you obtain is at the mercy of your ability to obtain it. Even if legal process is at your disposal, at least some courts have ruled that "discovery demands are improper if they are based on 'hypothetical speculations calculated to justify a fishing expedition,'" nor is the fact that someone uses a Facebook account enough.[8] Law enforcement officers may develop probable cause and be able to access private content through legal means, but for many compliance professionals, social media evidence may be beyond reach.

Not to be deterred, remember within your organization there are likely sources of information in company computers, email, instant messages, and possibly cell phone data that you have unfettered access to, depending on your organization's policies and banners. If your business uses social media, it is likely a business record that must be collected and maintained, and therefore available to you. Furthermore, the majority of employees end up using organizational resources to do personal business, so be resourceful in keeping investigative avenues open.

Communications posted by a suspect can help you make sense of what the person knew and when they knew it. The governance aspect of electronic communications is important because key decisions may be documented in the bits and bytes.

Scope and process issues

Assume for the moment that you have full access to a suspect's social media account. What are you looking for? What exactly do you expect to find that will be relevant to your investigation, and how do you find it? This is the second planning question and the one that is most practical for the investigator. If it is merely intelligence information—photos, where somebody spends their time, who they communicate with, when they tend to be active, what their interests are—then you can learn quite a bit. It could be the items that initially appear only to have intel value also end up being key points of evidence. For instance, being able to link your suspect with another person, or being able to geotag them at a particular place and time may prove important.

In most compliance investigative work, intent and knowledge evidence is the value proposition. Communications posted by a suspect can help you make sense of what the person knew and when they knew

it. The governance aspect of electronic communications is important because key decisions may be documented in the bits and bytes. If you hit the jackpot, a suspect will have been careless enough to post some rather direct admissions. Those posts may identify accomplices, methods, or provide "'stream-of-consciousness statements that highlight a person's instant thoughts and impressions."[9] You might think people would avoid making these kinds of statements against self-interest, but in this age of oversharing, it happens all the time. No doubt the potential to find great evidence of intent makes social media searches worthwhile, but realize they are time-intensive and a hit-or-miss proposition.

Once you know what you are looking for, the rubber meets the road in finding a way to do the actual search. The inefficiencies of hunting for the needle in the haystack are too costly, so the only answer is software that aggregates web-based content and automatically conducts user-designed searches.

My experience with virtually all of the free online platforms that claim they search across a wide spectrum of social media sites is mixed. For those who have few privacy protections in place, these may be useful searches. Sites like Social Searcher, WhosTalkin, and snitch.name are examples of such search sites. There are also sites like Pipl People Search and Spokeo that can at times produce a social network username. I tested some family names whose account settings I knew and had abysmal search results on all these sites, even on public pages. A simple Google search yielded better results, and for those adept at using Google's advanced search, there are more powerful tools that help filter websites and images. You can search the web for a plethora of resources that explain search terms and operators that may help. There are other commercial applications that tend to produce more reliable outcomes—packages you have to pay for and which I will not endorse here. But if you are serious about using this as an investigative tool, you get what you pay for in most cases.

The inefficiencies of hunting for the needle in the haystack are too costly, so the only answer is software that aggregates web-based content and automatically conducts user-designed searches.

Collection and preservation issues

Which brings us to the third planning element: proper collection. Considering just doing a screen print and putting it in your evidence file? Think again. Case law has repeatedly and emphatically made clear that screen prints are worthless because of authentication issues. There are a number of legal hoops that social media evidence must jump, but none more essential than authentication—how you prove the statement was made by the party to which you seek to attribute the statement. Federal Rules of Evidence (FRE) 901 and 902 are the guiding principles for authenticating evidence. The courts have held that whether a piece of paper, or electronically stored information, evidence "without any indication of its creator, source, or custodian may not be authenticated under Federal Rules of Evidence 901."[10] Because of the ease in manipulating electronic data, the courts tread carefully in this area.[11]

Electronic evidence differs from traditional paper evidence in that it is intangible, creates incredible volumes, is transient, and is typically associated with metadata that can itself be evidence (for example the date and time a document was written could be useful in a case). Preserving this metadata with associated file level MD5 hash values is critically important to aid in authentication because it can answer key questions about who created or changed content, when those actions occurred, what unique IP address was used, geolocation, when the evidence was collected, and other key data points. In short, metadata tracing is the fingerprint evidence of today.

Once the goods are in hand, with the time-stamped hash completed, it is then a matter of how to properly collect and preserve the evidence in a way that will hold up in court. This is a subtle difference from the authentication issue, which focuses on how we can prove the electronic evidence as presented to the court is what actually existed at the time of collection. Preservation involves a chain of custody that provides the court with assurance that once collected, nobody had an opportunity to subvert the integrity of the evidence.

The ephemeral nature of electronic evidence, particularly web-based content, means the moment of evidence collection may be the only time that evidence will exist. A proper chain of custody "show[s] that the evidence presented to the court is the same as what was originally collected, and that the evidence was preserved without tampering or alteration."[12] The courts seem primarily concerned, and rightfully so, with being reasonably certain that electronic evidence is not intentionally or accidentally altered. Most people are unaware that the mere opening of a spreadsheet or word-processing file changes key metadata without a single key stroke. An investigator's curiosity makes opening a piece of electronic evidence irresistible, unaware their action may have just destroyed the ability to introduce that piece of evidence. Using the proper write blockers and other forensically sound methods to make working copies, while safeguarding the original evidence, requires extra work, but it is necessary to show nothing was changed.

Once the goods are in hand, with the time-stamped hash completed, it is then a matter of how to properly collect and preserve the evidence in a way that will hold up in court.

Investigative policies that spell out acceptable methods for collecting evidence and keeping a chain of custody will come into play when a court evaluates whether an effective history of evidence handling has occurred, so be sure to have your evidence policy on a regular rotation for review to keep up with best practices.

Authentication case law is complex and inconsistent across many jurisdictions, including whether profile pages are business records under FRE 902, and threshold standards for authenticity.[13] Best practices for investigators involve having good policy and employing forensically sound methods of collecting and maintaining social media evidence.

Social media can be a tool for both evil and good. Children have killed themselves

because of social media bullying, and conspirators have planned vicious crimes. Those same data streams are treasure troves for investigators to at least address the wrong that was committed. Crime victims have identified their assailants through social media, predators have been prevented from peddling their filthiness, hackers have been thwarted, and you can build an airtight case if you embrace the technology, learn how to avoid pitfalls, and properly secure social media evidence. Now go out there and get 'er done! ✳

The opinions in this article are the author's and do not necessarily represent the position of any government agency.

1. "Managing big data" *Professional Security*, April 29, 2013. Available at http://bit.ly/2uCYHhY
2. Justin P. Murphy & Adrian Fontecilla: "Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues" *Richmond Journal of Law & Technology*, 2013;XIX(3): 6-7. Available at http://bit.ly/2ucdZHz
3. James Covert: "Judge probes whether Uber's private eye lied to dig up dirt" *New York Post*, June 8, 2016. Available at http://nyp.st/2vFvm3m
4. The Financial Services Modernization Act of 1999, codified at 15 U.S.C §§ 6821 et seq.
5. The Telephone Records and Privacy Protection Act of 2006, codified at 18 U.S.C. §1039.
6. Dia Kayyali and Dave Maass: "Cops Need to Obey Facebook's Rules" *Electronic Frontier Foundation*, October 24, 2014. Available at http://bit.ly/2ttg98T
7. Lauren Walker: "Feds Settle Over Fake Facebook Profile Used in Drug Case" *Newsweek*, January 21, 2015. Available at http://bit.ly/2uG2evg
8. Lawrence N. Rogak: "No Fishing On Facebook, Holds Appellate Division" *Insurance Advocate*, March 28, 2016, 26–27. Available at http://bit.ly/2ttDSFR
9. Siri Carlson: "When Is a Tweet Not an Admissible Tweet? Closing the Authentication Gap in the Federal Rules of Evidence" *University of Pennsylvania Law Review*, 2016;164:1033. Footnote 54, page 1041, citing Megan Uncel, "Facebook is Now Friends with the Court": *Current Federal Rules and Social Media Evidence*, 52 JURIMETRICS 43, 68 (2011). Available at: http://bit.ly/2ucrerS
10. *United States v. O'Keefe*, 537 F. Supp. 2d14, 20 (D.C. 2008). Available at: http://bit.ly/2uCL1Dz
11. *See* Carlson, footnote 68, page 1043.
12. Patrick Schweihs and Stephen Nazaran: "Establishing Digital Chain of Custody for Web Page Evidence" *Law Practice Today*, October 14, 2015. Available at http://bit.ly/2uFKsbG
13. *See* Carlson, page 1054–1055.

***Daniel Coney**, CCEP, CFE, CFCS (danconey@comcast.net) has been a law enforcement professional for nearly 33 years, with the last 25 years being both an agent and supervisor in four different Office of Inspector General organizations. He has managed a digital forensics laboratory program, as well as been the project manager for acquiring and implementing an e-discovery system designed for investigations, including ingesting and analyzing social media sources. Dan can also be reached on LinkedIn at bit.ly/li-DanielConey*