

Module 14: Electronic Discovery and Social Media

Learning Outcomes

Upon completion of Module 14, students will be able to:

- Assess social media as an especially rich source of potentially relevant electronic evidence in an e-discovery process.
- Compare and contrast the options for obtaining social media subscriber information and content as part of litigation.
- Evaluate the issues with preservation, authentication and admissibility of social media information and content as evidence.
- Justify whether federal, state, international and common law and other regulations protect social media from being discoverable and admissible in court.
- Interpret the ethical issues when a lawyer wants to use social media as part of an investigation of parties, witnesses and jury members.
- Support when and under what doctrines an employer can or cannot access the social media accounts of employees and job applicants.
- Summarize the important points in Module 14 and the reading assignment.

Please read the following items, which are included with Module 14.

- *Social Media Evidence – How to Find It and How to Use It* – ABA Annual Meeting, 2013
- Social Media and Electronic Discovery: A Potential Source of Evidence in Bankruptcy Proceedings – from *NABTalk: The Journal of the National Association of Bankruptcy Trustees*
- Social Media: Preservation, Harvesting and Authentication – from Nelson and Simek
- Discovery and Preservation of Social Media Evidence – from *Business Law Today*
- E-Discovery and Social Media – from *E-Discovery: An Introduction to Digital Evidence*
- Whaley: Adventures in e-Discovery and Social Media – from *The Indiana Lawyer*
- Oh, Snap! The State of Electronic Discovery Amid the Rise of Snapchat, WhatsApp, Kik and Other Mobile Messaging Apps – from *The Federal Lawyer*
- *Recover Social Network Conversations* – from Belkasoft
- The Top 25 Social Media Analytics Tools – from *Michigan Bar Journal*

For the most complete and current thinking on social media as evidence, please skim through Primer on Social Media, Second Edition (Public Comment Version) – from The Sedona Conference.

Please read the following mini-lecture.

Included with Module 14 is Professor Sara Hook's article Social Media and Electronic Discovery: A Potential Source of Evidence in Bankruptcy Proceedings from *NABTalk: The Journal of the National Association of Bankruptcy Trustees*, which Professor Hook wrote with her undergraduate UROP student (Ms. Katherine Taht). Professor Hook also gave a presentation with her graduate student (Ms. Cori Faklaris) at the 12th Annual International Conference on Law in Athens, Greece, which turned into an article published in *The Federal Lawyer* and then

another version of the article appeared in *The Computer & Internet Lawyer*. The reading assignment features some of the best and most practical articles on how to handle social media as part of an electronic discovery process, including an article by my favorite authors, Nelson and Simek, on the preservation, harvesting and authentication of social media.

The introduction to the article by Nelson and Simek discusses how the value of social media evidence cannot be overstated (postings from Facebook emerge as evidence in as many as 60% of divorce cases, but it is quite common in personal injury and employment cases). However, many companies do not believe that they need to archive this data or produce it as part of discovery. As indicated on page 1, spoliation of social media evidence is not tolerated. On the second page, they discuss how to preserve social media (several tools available) and some of the mistakes that can be made, especially when a law firm or client is expected to do this. As they advise, “[r]espected third party experts constitute the avenue of choice – and remember, experts live and die by their reputations, so their credibility is life’s blood to them.” Harvesting social media presents another challenge, with the least useful route to send requests to the social media provider for non-public social media content (beyond data like subscriber information, dates of connections, IP addresses, etc.) The better process is to go directly to the user or a “friend” of a user. It is unlikely that the judge will require a party to provide his/her login information, which amounts to a “fishing expedition” - with the preference being for a more narrowly tailored requests unless there is some need for overall “lifestyle” kinds of data. Note that the data should first go through the producing party’s lawyer to screen for relevance and privilege. Of course, recall that the 2015 amendments to the FRCP put greater emphasis on proportionality, specificity and cooperation as ways to deal with overly broad requests.

The final consideration covered by Nelson and Simek is the authentication of social media evidence. As they note, this is simple if a third-party expert (who may have to testify and authenticate what he/she recovers) or self-authenticating software has been used or if the parties stipulate to the authenticity of the data (or through a request for admission or deposition). The authors indicate how easy it is to download your own data from Facebook and Twitter. They cite the work of John Patzakakis and recommend his materials as well as the article by Judge Grimm. Judge Grimm’s article includes a checklist for authentication and a discussion of the risks if a party relies on screen printouts. Note the differing standards that courts have used (the Maryland Standard versus the Texas Standard) as well as the “duck” standard, which looks at the distinctive characteristics of social media evidence, including content, nicknames, dates, Internet addresses, abbreviations, slang, knowledge of specific facts, replies to other posts, etc. Their final recommendation is that lawyers would be wise to resolve these issues themselves, most likely as part of the “meet and confer” conference.

Two other articles add to our understanding of social media as an especially challenging form of electronic evidence. In his article, Whaley discusses the relevance of social media in e-discovery, with citations to cases that show that not only is this type of evidence discoverable, but that parties should have little to no expectation of privacy, absent an argument that the evidence is not relevant to the case or that the request is overly broad. He considers the interplay between access to social media evidence and the Stored Communications Act, which was developed in the 1980s with much older technology in mind. The author describes the importance of preserving social media content (and not encouraging a client to alter it) as well as how to authenticate it. Other issues with social media are identifying who actually has possession, custody or control of social media content (recall our discussion of custodians versus owners), the prohibition on seeking “friend” status under false pretenses to inveigle content and

not using social media recklessly through inappropriate blog posts or comments.

Likewise, DiBianca provides considerable practical information in her article on the discovery and preservation of social media evidence. As she notes on page 1, “[d]ata residing on social media platforms is subject to the same duty to preserve as other types of electronically stored information (ESI).” She reminds us that social media content should be included in litigation hold notices. Although Facebook and Twitter offer options for do-it-yourself preservation, she echoes the advice from Nelson and Simek that it may be prudent to use a third-party vendor in order to ensure compliance and to be certain that we have gathered all possible data. The consequences for failing to preserve can be severe, including sanctions from the court as well as loss of potentially relevant evidence, which she illustrates with the *Lester*, *Katiroll* and *In re Pfizer* cases. On page 2, she discusses the additional difficulties that present themselves in a BYOD world, with *Cotton v. Costco Wholesale Corp.* as an example. On page 2, the author dispels a common myth among social media users that their content is “private.” As she notes, discoverability is governed by the standard analysis and not subject to any “social media” or “privacy” privilege. Instead, relevancy is the threshold analysis. As she observes, as more users understand the importance of privacy settings, the burden on the requesting party to show relevance may be more difficult.

As DiBianca notes, one of the most interesting questions is how to access social media evidence. She first considers direct access to social media accounts, which may be the most intrusive and which courts have disfavored as being overly broad and akin to a “fishing expedition” or like giving someone the key to my office and letting him/her sift through all of the drawers (see the *Largent*, *Gatto*, *Trail* and *Chauvin* cases as examples of the various ways that court have handled this kind of request). On the other hand, the lawyer should not only remind the client of the duty to preserve this evidence, but should not encourage the client to make changes to his/her Facebook page, etc. At least one court has sanctioned both the client and the lawyer for this.

A less intrusive option is for the court to conduct an *in camera* review of social media evidence prior to production (see the *Offenback*, *Douglas* and *Tomkins* cases). Interestingly, as reported on page 4, at least one court has agreed to “friend” a litigant for the purpose of conducting an *in camera* review of the litigant’s Facebook page (see *Barnes v. CUS Nashville, LLC*). Another option is to have the party provide the requested information to the opposing party’s lawyer for an attorney’s-eyes-only review for the limited purpose of identifying whether information had been improperly withheld from production. However, note that this information could not be used for any other purpose without a further ruling by the court (see *Thompson v. Autoliv ASP, Inc.*).

DiBianca provides a discussion of the application of the Stored Communications Act (SCA) to requests to social media vendors and other Internet service providers. As she indicates on page 4, most of these providers take the position that the SCA prohibits them from disclosing the contents of social media, even with a subpoena (see *Crispin v. Christian Audigier, Inc.*). However, as we have learned with other types of media and formats, sometimes it is the fact that the communication happened rather than the content of the communication that will be most important. For example, it may be more telling that a variety of telephone calls were made between two parties during a certain period of time than the content of these conversations. Note that the SCA does not override a party’s obligation to produce relevant ESI that is within its possession, custody and control. Thus, a court can compel a party to execute an authorization for

the release of social media content. Most commentators recommend that attempting to obtain this content directly from the party is the best method. As the author concludes, “[p]arties and counsel are well advised to adjust their thinking so that social media becomes just another type of ESI.”

An interesting approach to social media and electronic discovery is taken by the authors of *E-Discovery: An Introduction to Digital Evidence* on pages 228-230. As they observe on page 228, “[i]n the EU and many other countries, such as Australia, personal privacy has precedence over corporate rights.” The authors relate the story of Max Schrem, who challenged the legality of Facebook’s collection and marketing of user data without his consent, including information such as location that is gathered automatically. As reported by the authors, his protest caused more than 40,000 EU citizens to demand their Facebook files. EU countries are trying to curtail the use of tracking cookies as a violation of privacy. A proposed law would include a number of provisions, such as requiring deletion of old information in a timely manner, requiring explicit consent for tracking through cookies and GPS, requiring breach notification and fines for companies that transfer personal data across borders.

The authors wisely recommend that all companies and organizations have Acceptable Use policies for social media use as well as prohibitions on requiring employees to “friend” them. The government (as well as law firms) investigates people through social media (see *Clark v. State* for an Indiana criminal case wherein the defendant’s MySpace posts were admitted as evidence). The authors assert that tools offered by vendors such as Google may generate discoverable evidence and thus companies need to educate employees and develop policies. A recent article noted that although the National Labor Relations Act protects some types of speech/communication for unionized companies, recent cases extend this same protection to social media content posted by employees at non-unionized companies. The authors raise some important questions on page 229, such as where we draw the line between what is private and what employers should be able to request and preserve.

Retention of social media content and subscriber information is another challenge, which could vary depending on laws and regulations as well as best practices and established norms for particular industries. Interestingly, the authors report that a new industry is developing to handle the archiving of social media content for government and corporate clients. Of course, any vendors offering such services will need to comply with federal and state laws and governing bodies, including the Sarbanes-Oxley Act (SOX), the Freedom of Information Act (FOIA), the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), to name but a few.

A really helpful publication is the material from a session at the 2013 American Bar Association’s Annual Meeting. Entitled *Social Media Evidence – How to Find It and How to Use It*, this publication first provides some astounding statistics on the growth of social media and its various forms, including personal and professional interaction (Facebook, LinkedIn), dating, photo and video-sharing, blogs, coupons, news and travel. The authors specifically focus on Facebook, Twitter and MySpace on page 2. They devote pages 2-3 to a list of federal statutory schemes that govern the possession and use of an individual’s private information, including several that we have already covered this semester. The authors then review a number of privacy laws and standards at the state level as well as constitutional provisions found in states such as California. They suggest that if you seek social media information from an entity in another state, you need to review that state’s data privacy laws to be sure that you are in

compliance rather than relying on the party that you are requesting data from to know the laws that apply and how to assert the protection that it is entitled to. Of course, we have already learned that other countries may have much more robust protection for personal data than the U.S., particularly the countries that are members of the EU. There are a variety of common law doctrines that may provide a private cause of action if sensitive information is improperly disclosed, such as the tort of intrusion upon seclusion, public disclosure of private facts and misappropriation of personality.

The authors provide an extension discussion of social media and the Stored Communications Act (SCA) on pages 5-7, with a discussion of many of the major cases such as *Quon*, *Crispin v. Christian Audigier*, *People v. Harris* and *Flagg v. City of Detroit*. As indicated on page 6, “[t]he majority of courts hold that internet service providers and social media websites are ECS providers bound by the SCA not to produce postings and emails of their subscribers/registrants in response to a civil subpoena. Instead, the party seeking discovery must use Rule 34 requests to the opposing party to obtain the postings.” The authors indicate that we should be prepared for arguments about privacy protection under the First, Fourth, Fifth and Ninth Amendments in an attempt to block discovery requests.

The authors advise us to always check the Terms of Service for social media websites because this document and other vendor policies may impact our approach to obtaining the information, with the example of the *People v. Harris* case involving access to a defendant’s Twitter tweets. The authors provide a nice discussion of ethical considerations and restrictions on a lawyer’s use of social media as part of a case, including for research on parties and non-parties, for research on potential jury members, for communicating with a party represented by counsel (see Rule 4.2), for communicating with a witness, for communicating with judges and for self-publicity. It is important to note that Indiana has fairly restrictive rules on marketing, advertising and solicitation, although amendments that would soften some of these restrictions (statistics, testimonials) are being considered.

A particularly interesting aspect of social media is in the context of employment, so the authors have provided a thoughtful discussion on pages 10-13. First, they cover Section 7 of the National Labor Relations Act. They then describe some of the reasons why employers should or should not investigate the use of social media by job applicants and employees, including requiring or requesting login credentials and passwords. Some states have passed – or are considering - laws that prohibit employers from demanding user names and passwords from employees and job applicants.

Section VI in *Social Media Evidence – How to Find It and How to Use It* is devoted to methods and techniques for obtaining social media in discovery. As the authors recommend on page 14, “[a]t the beginning of a case, be sure to notify the opposing party or counsel to preserve the party’s social media information.” Note that you must also tell your own client to preserve all social media accounts (see *Gatto v. United Air Lines, Ltd.*). The usual methods of discovery can be used – informal requests, written interrogatories and document production requests to parties and subpoenas to non-parties. One of the most interesting challenges may be to determine the identity of anonymous Internet and social media posters. As indicated on page 15 and illuminated by various cases, courts have taken several approaches to addressing First Amendment defenses.

Some principles and trends in the discovery of social media evidence are:

- Discovery requests/subpoenas for social media evidence should be narrowly tailored.
- Tie discovery requests to information already in hand that shows that the request is seeking evidence that likely exists and therefore is not a fishing expedition.
- Compulsion efforts are better targeted at the users of the social media, not at the social media providers.
- If you have evidence that the producing party has improperly withheld evidence, go to the court for sanctions and/or for more social media discovery.
- Consider closely who “owns” the social media link. You may have more than one potential discovery target.
- *In camera* review by the court may be needed.
- If the request is too broad, the court may limit it or deny it altogether.

Section VII of *Social Media Evidence – How to Find It and How to Use It* considers the use of social media evidence in litigation. The authors suggest that one of the first places to look for assistance in the use of electronic records as evidence in court is Judge Grimm’s 101-page order in *Lorraine v. Markel American Ins. Co.* In terms of evidentiary issues and uses, the authors add to our understanding of evidentiary issues, such as:

- Authentication – see pages 20-21
- Identification – see page 21
- Relevance – see page 21
- Hearsay – see page 21 (very complicated area of evidence law)
- Unfair prejudice under FRE (Federal Rules of Evidence) 403 and 404

Another aspect of social media in litigation is whether or not lawyers can investigate jury members and potential jury members. Of course, lawyers are prohibited from communicating directly with jury members outside of in-court processes. In other words, the lawyer is not allowed to “friend” jury members or prospective jury members, nor can he/she subscribe to a Twitter account, which means that there has now been a forbidden *ex parte* communication to a jury member. Most courts and formal ethics opinions draw the line at jury research if that research results in some sort of notice back to the person through his/her social media provider, which is often done automatically. An article in the *Grand Rapids Business Journal* alerted people that lawyers were doing this and advised readers about how to make it more difficult for lawyers to investigate them as potential jury members (see *Grand Rapids Business Journal*, 7/14/2014, Vol. 32 Issue 28, p. 3-5).

The final pages of *Social Media Evidence – How to Find It and How to Use It* focus on perhaps the most disruptive issues involving social media and litigation, which is when jury members use social media to conduct independent research during trial, as described on pages 22-24. A variety of model jury instructions have been issued to try to prevent this activity. One source for jury instructions is the result of a 50-state survey published in *Reynolds Courts & Media Law Journal* in 2011. Appendix B also includes sample jury instructions. As indicated on page 23, the problem of jury member use of social media during trial is likely to continue and even grow, especially with advanced mobile devices and the prevalence of texting and tweeting. As indicated on page 23, “[w]hen the possibility occurs of jurors engaging in social media communication about a trial during the trial, the presiding judge generally has inherent authority to investigate to ensure that the jury is not tainted by exposure to evidence outside of that presented at trial.” However, note that the investigative methods vary by court. Page 24

concludes with some recommendations regarding jury members and social media.

Appendix A in *Social Media Evidence – How to Find It and How to Use It* provides some sample interrogatories and document requests that may be useful. Note the statement at the top of the page that “[c]ase law makes clear that social media discovery directed to a party must be narrowly tailored to the issues relevant in the case.” Because of the issues with jury members doing their own research during the trial, many courts have drafted jury instructions to try to curb this expensive and disruptive activity (called a “Google mistrial”), as shown in Appendix B. Interestingly, England and Wales have tried to combat this behavior by penalties that include jail time. (England and Wales Crack Down on Googling Jurors; U.S. Not So Much, *The Wall Street Journal Law Blog*, Dec. 13, 2013, <http://blogs.wsj.com/law/2013/12/13/england-and-wales-crack-down-on-googling-jurors-u-s-not-so-much/>, accessed 11/15/17) Appendix C contains a number of documents related to an anonymous posting about a physician who is suing for trade libel. Recall that pages 14-15 of *Social Media Evidence – How to Find It and How to Use It* discuss the issues with discovering anonymous Internet and social media posters and the cases that illuminate the efforts of courts to balance the need for information about the poster’s identity with the First Amendment.

Here is an interesting case from Indiana about the authentication of Twitter messages:

- *Wilson v. Indiana* No. 45A03-1409-CR-317, 2015 WL 1963860 (Ind. Ct. App. Apr. 30, 2015). – NOTE: Indiana case.
(Twitter)

In a criminal matter, the court said that Twitter messages could be authenticated under Indiana Rules of Evidence Rule 901(b) by, for example, “(1) Testimony of a Witness with Knowledge” and by “(4) Distinctive Characteristics and the Like” and these examples were satisfied where a witness testified that she had communicated with the defendant on Twitter via the account in question and testified that the account contained both pictures of the defendant and references to activities that were sufficient to indicate that the posts had been authored by the defendant. [KLG]

With Module 15, we examine e-discovery in the context of new technologies, including the Internet of Things.

Please let me know if you have questions about Module 14 or the reading assignment.

Module 15: Electronic Discovery and New Technologies

Learning Outcomes

Upon completion of Module 15, students will be able to:

- Assess the e-discovery, privacy and security issues with wearable technology.
- Evaluate the e-discovery, privacy and security challenges with the Internet of Things.
- Analyze the special e-discovery issues with electronically stored information (ESI) that is intended to automatically self-destruct after a certain period of time.
- Interpret how courts should handle ephemeral and transient forms of communications, such as mobile messaging apps, as part of an e-discovery process.
- Predict whether the 2015 amendments to the Federal Rules of Civil Procedure will assist with e-discovery issues related to wearable technology, the Internet of Things and ephemeral and transient communications.
- Summarize the important points in Module 15 and the reading assignment.

Please remember to take Exam #4 between Friday, December 6 at 5:00 p.m. and Sunday, December 8 at 5:00 p.m. Exam #4 will cover Modules 11-14 and be a mixture of true/false, matching and multiple choice questions.

Also, the Close the Loop #3 assignment is due on Sunday, December 8, by noon. You will be in the same group as you were for Close the Loop #1 and #2. Instructions are provided as part of Module 14 and 15.

Please read the following items, which are included with Module 15.

- Privacy, Security, and Wearable Technology – from *Landslide*
- The Internet of Everything: What It Means for Lawyers – from Nelson and Simek
- What Everyone is Wearing: Data from Wearable Devices is Being Eyed as Evidence in the Courtroom – from *ABA Journal*
- Treading Beyond the Iota of Fear: eDiscovery and the Internet of Things – from *Bloomberg BNA Electronic Commerce & Law Report*
- “Connected” Discovery: What the Ubiquity of Digital Evidence Means for Lawyers and Litigation – from *Richmond Journal of Law & Technology*
- A Litigator’s Guide to the Internet of Things – from *Richmond Journal of Law & Technology* (I served on a Board of Advisors for an international legal technology organization with the author, so I am pleased to include her article as part of Module 15)
- The Privacy, Security and Discoverability of Data on Wearable Health Devices: Fitness or Folly? – PowerPoint presentation given by Vishahka Kumari, HCI International 2017
- Court Grants Request to Produce Social Media Data, Orders Supplementation Regarding FitBit Data – from *Exterro*
- IoT – Connected to the Internet and the Courts – from *The Indiana Lawyer*

Please read the following mini-lecture.

In Module 15, I wanted to look at some new technologies and how they are impacting electronic discovery now and the potential challenges in the future. The technologies to consider for Module 15 are mobile messaging apps such as Snapchat and WhatsApp, wearable technology and the Internet of Things. The ability to exploit the opportunity to “go dark” by using ephemeral mobile messaging apps and increasingly robust encryption was recently reported as the reason why French authorities were not able to predict and prevent the terrorist attacks in Paris. In terms of being able to break encryption and when, we continue to see the clear tension between privacy rights and national security.

One type of technology that has implications for e-discovery is wearable technology. As reported in *What Everyone Is Wearing*, on the aggregate level, the data on people’s behavior (heart rates, sleep cycles, etc.) represents a treasure trove of information, with a lawyer in Canada getting this treasure trove entered into evidence in a personal injury case. This case concerned a woman who claimed that her activity levels were significantly reduced after an accident. As indicated in the article, while it is inevitable that data from wearable technology will be admitted in courts in the U.S., there are issues with reliability, privacy and ownership of the data. The e-discovery expert who was interviewed for the article does not expect data from wearables to stand on its own, but that it can be used to corroborate testimony. A more substantial article from the November/December 2015 issue of *Landslide* discusses the privacy and security issues with wearable technology. As indicated on page 30, “[t]he more devices and sensors introduced into our clothes, shoes, and accessories, the greater the volume and sensitivity of data that will be collected through these devices.” On page 31, the author analyzes the challenges that wearables present based on traditional privacy principles, such as the Fair Information Practice Principles (FIPPs), including notice and choice, consent, security risks, whether the data is stored locally or transmitted and stored in the cloud and limitations on use versus its use by third parties.

Another issue with wearable technology is that many of these devices collect location information and track user movements. A study by Symantec found that all of the wearable activity tracking devices that it surveyed were vulnerable to location tracking, which raises a host of privacy concerns. Moreover, consumers are not always aware of where this information goes and who it is shared with. In addition to the risks to personal privacy described on page 31, geolocation information can facilitate criminal behavior, such as stalking, domestic violence, kidnapping and burglary. Note the dearth of legislation over the collection and use of location information, but that proposed legislation would allow its collection without consent only with a court order or request by law enforcement (or in cases of emergency or locating a minor child). As reported on page 32, the FTC has recently pursued vendors through the power of its enforcement actions that have misled consumers about their privacy policies and how the data that was collected would be used. Note that the FTC has already taken action with respect to the Internet of Things in its settlement with TRENDnet, Inc., over its failure to provide reasonable security to prevent unauthorized access to sensitive information from live camera feeds.

The author focuses specifically on the issues with wearable devices in the health sector on pages 32-33. As indicated on page 32, “[t]he flip side of the coin is that the ubiquitous collection of such healthcare information creates a number of privacy and security risks.” For example, in a study of 12 health-related mobile apps, the FTC found that the apps transmitted sensitive health conditions to 76 third parties, such as ad networks and analytics companies. Yet in spite of the

risks involved with health information, existing privacy and security laws may not apply. Note that HIPAA only applies to “covered entities,” which does not typically encompass wearables and the companies that provide them. In fact, as reported on page 33, a recent study found that most data that flows from mobile health apps is not covered by HIPAA. On the other hand, in thinking about wearables as a rich repository for potentially relevant electronic evidence in a wide variety of cases (personal injury, medical malpractice, etc.), more interesting questions are how should the data from these sources be handled at all steps within an e-discovery process and what the likely challenges to the discoverability and admissibility of this data will be. See the PowerPoint slides from a presentation on the risks with fitness devices that was given at the HCI International 2017 conference. (See also *Court Grants Request to Produce Social Media Data, Orders Supplementation Regarding FitBit Data* – from Exterro and *IoT – Connected to the Internet and the Courts* – from *The Indiana Lawyer*.)

Nelson and Simek, my favorite authors, have provided a very nice article on the Internet of Things, which is really an extension of wearable technology. As they note in their introduction, what the Internet of Everything means for lawyers is evidence and lots of new sources of evidence, along with the continuing loss of privacy. They first describe how the Internet of Things will impact the professional and personal lives of lawyers. On the other hand, note the discussion on page 2 about how the NEST thermostat could provide evidence against someone. Ponder the e-discovery issues with this scenario. The authors continue this vein of analysis by noting all of the things that smartphones can – or will be able to - do, such as recognize a face or voice and even determine our moods, emotions or honesty, with the ability to project the results on a screen. As the authors note on page 4, “[i]t is getting to the point where we almost lose track of all the ways in which we are connected to the Internet.” They then discuss the privacy and security issues with all of this data, whether used by vendors such as Apple, third parties, the government or cybercriminals. As indicated by a 2014 survey, 70% of the Internet of Things devices used unencrypted network services and 80% of devices did not require passwords of sufficient length and complexity. In terms of the future of the Internet of Things, the authors predict substantial growth in the not-too-distant future, a lag between the technology and the laws regulating it, failure of companies, organizations and law firms to adopt policies and controls for the Internet of Things in the workplace and diminished privacy. As they recommend in their final paragraph, lawyers will need to be vigilant about their personal and professional use of the Internet of Things so as not to compromise client data.

Another article related specifically to e-discovery and the Internet of Things (IoT) is provided by McGinn and Yankov (*Treading Beyond the Iota of Fear: eDiscovery and the Internet of Things*). As they note on page 2, the data from the Internet of Things “is radically different from current forms of common electronically stored information (ESI): it is not created by humans.” Instead, it represents devices gathering data and ultimately communicating with a centralized database and/or another devices. As a result, much of the data generated by the device may no longer reside on that device after it is transmitted. Thus, preservation efforts need to go beyond placing a litigation hold or preserving the device “as is.” The authors discuss a number of special considerations with handling data generated by the Internet of Things:

- The responding party may not have the requisite control over IoT data to preserve it.
- It may be difficult to target only potentially relevant IoT data for preservation.
- Preservation of IoT may be limited by the 2015 amendments to the Federal Rules of Civil Procedure (see the box at the top of page 3).

- IoT data may be reasonably inaccessible.
- Reviewing IoT data may prove less costly than e-mail review (as compared with the costs of preservation and collection). Note the good news on page 5 that IoT should be unlikely to contain privileged information.

Another topic for Module 15 is near and dear to my heart, which is e-discovery and social media. The reading assignment for Module 15 considers some of the new social media services that go beyond Facebook and Twitter, including several that purport to be even more transient and ephemeral in nature. As part of Module 15, I included an article that Professor Hook co-authored with Ms. Cori Faklaris, Research Assistants at the School of Informatics and Computing. This article, published in *The Federal Lawyer* and *The Computer & Internet Lawyer*, is the expanded version of their presentation at the 12th Annual International Conference on Law in Athens, Greece, in July 2015. The article begins with a discussion of the history of the law on e-discovery. They then discuss several of the most notable mobile messaging apps, including Snapchat, WhatsApp and Kik Messenger. Note the promises that these vendors have made about the storage of and access to any content posted by users. Snapchat recently ran afoul of the FTC for the promises it made about its services. The article then considers a number of e-discovery issues posed by mobile messaging apps, with references to major social media cases:

- Does a permanent archive of such data exist?
- How can legal professionals identify the scope of discovery and tailor it appropriately?
- How can this data be preserved and collected?
- What does spoliation mean in this context?

The article concludes with an examination of the amendments to the Federal Rules of Civil Procedure (FRCP), which took effect in December 2015, and how these amendments might either add to or reduce the challenges associated with increasingly ephemeral and transient forms of communication.

In “Connected” Discovery: What the Ubiquity of Digital Evidence Means for Lawyers and Litigation, the author describes e-discovery as it relates to a wide variety of digital evidence. Among the new technology she mentions in her introduction that fall under the heading of the Internet of Things: autonomous vehicles, industrial business operations that incorporate drones and blockchain in banking. As she notes, “[a] review of the cases in this article, however, is sufficient to dispel any doubt about the importance of digital evidence and to confirm the magnitude of its impact on the practice of law.” She considers a number of technologies in depth, including:

- Telematics devices
- GPS navigation systems
- Wearables – note the two cases described
- Dashboard cameras and red light traffic cameras
- Event data recorders
- E-Z Pass transponders
- Social networking sites
- Text messages and tweets – recall the summary of a case from Indiana in Module 14 on the authentication of Twitter messages
- Blogs and chat rooms

- Emails

She concludes,

Digital evidence has disrupted discovery, civil and criminal litigation, and the practice of law. Advances in technology radically changed the way in which information is created, transmitted, preserved, and accessed-as well as the way in which potential litigants communicate. Technological innovation altered the types of claims that are litigated, the way in which they are litigated, and the kinds of evidence that must be used to support and undercut those claims.

There is no turning back. The days of document production consisting primarily of paper and of hard-copy trial exhibits sitting on easels in front of juries are behind us. When asked to find information about an opposing party, the initial inclination of lawyers who have recently graduated from law school and entered the practice of law will be to check social media to obtain information about that party. To investigate the allegations in a complaint, these lawyers' first instinct will be to search the e-mails on the client's office computer and their messages on cell phones and tablets. All lawyers must acknowledge that digital evidence plays an important role in litigation. Those who fail to understand the relevance of technology and digital evidence to the practice of law do so at their-and their clients'-peril.

As the widespread adoption of new technology continues, and more companies, industries, and governmental entities recognize the transformative power of big data and analytics, the volume of data that will be relevant in litigation will increase exponentially. The frequency with which digital evidence will be used in litigation, in government investigations and administrative proceedings, and at civil and criminal trials will soar. It will become clear to lawyers and clients that gaining competence, if not expertise, in the use of digital evidence is not a necessary evil, but a way to enhance the litigation strategy for a case and to increase the likelihood of a successful resolution. The ubiquity of digital evidence means that litigation and data are inextricably intertwined and that mastering "connected" discovery and maximizing the value of digital evidence are critical skills for today's lawyers.

In Section III of *A Litigator's Guide to the Internet of Things*, the author covers a number of technologies, including everyday objects, that are part of the Internet of Things, but which may pose privacy and security risks to users as well as generate potentially relevant evidence for e-discovery. Among these technologies are connected toys, wearable IoT devices and connected cars. She devotes several pages to the e-discovery issues with IoT information and provides insights into how IoT objects could be used as "witnesses." As she concludes:

A tech-savvy lawyer knows how to get the right evidence in the right format from her client or opponent. The fact that IoT raises a number of novel and interesting legal issues and practical complexities means that tech-savvy lawyers, with a good grasp of the basic issues, will be well positioned to provide thoughtful and constructive advice. This guidebook provides some basic information regarding IoT technologies, legal issues, and practical concerns that should be considered. But it needs to be applied to the real world, for each client and case, and in the context of each connected collection of objects,

companies, and people. The IoT movement is your opportunity to continue your self-education journey, and learn more about the implications of IoT on lawyering in the Information Age.

Next Steps

With Module 16, we look at remaining issues and new trends in electronic discovery.

Please let me know if you have questions about Module 15 or the reading assignment.

Module 16: Remaining Issues and New Trends

Learning Outcomes

Upon completion of Module 16, students will be able to:

- Assess the challenges related to privacy and how to balance personal privacy interests with the legitimate needs of national security, law enforcement and e-discovery.
- Evaluate legislation intended to provide greater protection for personal privacy.
- Interpret the implications of new technology on e-discovery rules and processes.
- Outline the steps for determining whether a warrant is needed to search mobile devices in criminal cases.
- Describe some of the anti-forensics methods used to try to thwart forensics investigations and some ways to detect and mitigate the damage to evidence from these activities.
- Summarize the important points in Module 16 and the reading assignment.

Please remember that your Self-Reflection on Electronic Discovery is due on Monday, December 16 by 5:00 p.m. Instructions for the Self-Reflection are provided as part of Modules 15 and 16.

If you have not done so already, please provide feedback about the course. You should have received an email from the university with instructions for how to log into the course evaluation system. All ratings are aggregated and comments are anonymous. I would be very interested in your feedback. Thank you for participating in this important process!

Please read Chapter 9 in *E-Discovery: An Introduction to Digital Evidence*. Please read the following items, which are included with Module 16.

- Deputy Prosecutor Suspended 4 Years for Eavesdropping – from *The Indiana Lawyer*
- Why Paralegals Are the Key to E-Discovery Success or Disaster – from Exterro
- 6 Tips for Successfully Adopting E-Discovery Technology – from Exterro
- Did Protecting Privileged Documents Just Become Unclear? – from Exterro

By Sunday, December 15 at noon, please respond to the questions for Discussion Forum #8 (covers Modules 14, 15 and 16):

- Is social media somehow different than other kinds of electronic evidence? Why or why not? Do you think people are aware that their social media subscription information as well as the content of their social media accounts is discoverable and admissible?
- Of the cases included in the reading assignment for Module 14 and Module 15 on social media and e-discovery, which do you find most interesting and why?
- Go to any of the social media vendor websites. This does not have to be a social media service that you personally use. Review the Terms of Service and other information on the vendor's website. What does this website say about how, when and under what circumstances it saves a user's subscriber information and his/her content and would provide this to the user and a third party? Were you surprised by what you read?
- What is one technology that presents particular challenges for an e-discovery process? How do you see these challenges being resolved in the future by the courts, revisions to the rules, etc.?
- In concluding the course, what aspects of electronic discovery do you find most compelling? What trends do you see in discovery in the future?
- Any other surprising or interesting points from Module 14, Module 15, Module 16 or the reading assignment.

16: Summary of Major Points

Please read the following mini-lecture.

Chapter 9 in *E-Discovery: An Introduction to Digital Evidence* is titled The Future of E-discovery and thus seems a perfect way to end the semester. As asserted on page 222, e-discovery has become a multimillion dollar industry and changed business processes and the way information is viewed. The authors devote the first two pages of Chapter 9 to the continued challenges with privacy and a variety of efforts to protect it through current and proposed legislation at the national and state level. For example, the proposed Online Communications and Geolocation Protection Act (OCGPA) would severely restrict using GPS locators to track citizens through mobile devices. The authors cover an ISO standard that is intended to help set more specific guidelines for digital evidence: ISO 27037:2012: Information technology -security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. http://www.iso.org/iso/catalogue_detail?csnumber=44381. Intended for forensics investigations, this ISO standard sets guidelines for managing digital evidence in an attempt to harmonize practices worldwide. Another challenge is the question of what qualifications digital forensics experts should have, such as required education and years/types of experience. As the authors note, the close relationship between e-discovery and digital forensics is evident. A long list of other related standards that have been published or are under development is available at:

http://www.iso.org/iso/home/store/catalogue_ics/catalogue_ics_browse.htm?ICS1=35&ICS2=030&

Of course, we have already observed what the authors state on page 224, which is that new technology - and the interconnectedness it has brought - has meant challenges to e-discovery that no one could have foreseen a decade ago. Among these technologies are cloud computing, social networking, tweets and blogs, to which I will add mobile devices, wearable technology, the Internet of Things and increasingly transient and ephemeral communication activities such as mobile messaging apps. The authors describe global positioning systems (GPS) and their ability to track suspects as another example of where the law needs to keep pace with technology. Formerly, surveillance had to be done by law enforcement personnel physically following suspects, but tracking devices make the process so much easier and less expensive – and almost automatic. Another issue that we have discussed is the special considerations when employers move towards requiring employees to use their personal devices for work activities (BYOD). How do we enforce a litigation hold? How do we protect the employee's privacy while still being able to collect and preserve the potentially relevant electronic evidence that might reside on that device? What policies are needed? As recommended by the authors, policies should cover mobile devices that are issued by and paid for by the employer as well as devices which are purchased and paid for by the employee. We need to be particularly careful when dealing with employees in countries that give deference to an employee's privacy.

The authors describe how to retrieve data from mobile devices on page 225, which complements what we have already covered this semester. Note again that how much and how long data is stored depends on the provider, the subscription type and any third-party software that the device is using. The number and variety of mobile devices mean that data formats vary widely and the data can be located in the device's memory, on a server or in cloud storage. If employees connect through their own mobile hotspots, their usernames may not show up in a company's wireless network server logs. Note that BYOA (Bring Your Own Application, also referred to as Bring Your Own Technology, or BYOT) can pose security risks, because the apps that employees have downloaded personally may contain embedded malware and might record usage data and other information, even a company's confidential information.

Although the focus of this course is on civil cases, pages 226-228 describe the considerations for searching for data on mobile devices in criminal cases. The authors pose the question of whether a law enforcement officer can search the contents of a cell phone or other mobile device from a suspect or person who has been arrested. As the authors note, two issues must be considered: inventory searches and closed containers. The authors review some older cases and then recent decisions from the Supreme Court of Ohio and the Oregon Supreme Court that considered searches for data on cell phones. Figure 9-1 shows a flowchart for whether a warrant is needed to search a cell phone. Although Module 14 was devoted to e-discovery and social media, pages 228-230 add to our understanding of this important topic. Note especially the *Schrems* case. (He has become an activist for information privacy and was recently featured on an episode of *60 Minutes* – see https://en.wikipedia.org/wiki/Max_Schrems for more information.)

The authors provide several paragraphs on the e-discovery aspects of storage in the cloud. The many benefits of cloud storage are described on page 230, including that it eases concerns about transporting proprietary information across borders. However, they observe that if someone accesses the file on a home computer, it is stored on that machine, which could mean challenges for determining a timeline in a criminal case. Privacy can be an issue with cloud storage, thus it is best to avoid mingling work and personal files. The authors assert that companies should create clear policies explaining the use of cloud storage and recommending that personal versus work files be labeled clearly. In fact, Australian privacy laws assume that some personal data will exist on company systems. However, it is not always easy to avoid comingling personal and employment-related files because mobile devices and desktop computers are so interconnected. This situation is particularly acute with small companies that may not be able to afford multiple accounts and hardware. If one device is compromised, they both are and so is the data stored on them. Moreover, any litigation holds would apply to both devices.

The authors discuss some emerging trends on page 231, stating that new technology can often affect people's right to privacy. They give the example of event data recorders (EDRs) that can capture information about vehicles, such as seatbelt use, airbag deployment, use of brakes, etc. For example, a party requested a pickup truck as evidence because there was interest in the data about its airbag system. Of course, other kinds of technology have implications for e-discovery, such as wearable technology, the Internet of Things and increasingly ephemeral and transient communications methods. The authors give 3D printing technology as another example. Although there have been a number of articles addressing the intellectual property issues with 3D printing, the memory of 3D printers and the software that is used with them may contain discoverable and potentially relevant electronic evidence. The authors cite Recommind (now part of OpenText - <https://www.recommind.com/>) as one product that uses predictive coding to sift through huge amounts of data in e-discovery.

The next two sections of Chapter 9 are devoted to what the authors refer to as anti-forensics. Note that although most lawyers who handle civil cases may believe that the opposing party has provided everything that they have asked for with nothing deliberately concealed or deleted, this is not so with prosecutors or law enforcement officers working on criminal cases. Although I think most lawyers in civil cases now understand that discovery involves dealing with electronic evidence in various forms and formats, they may not think about inappropriate actions of employees who might accidentally – or even intentionally - remove relevant evidence without the company's knowledge. Anti-forensics is defined as any measure that is used to defeat or obstruct a forensics examination (also recall our discussion of steganography from a previous Module). During civil litigation, evidence of anti-forensics activity is usually deemed spoliation by the courts and subject to sanctions. In criminal cases, evidence of anti-forensics is usually used to support the prosecution's claims of criminal activity. The authors provide an example of the *Kolon* case, which concerned corporate espionage and had both criminal and civil aspects to it.

Anti-forensics methods are covered on pages 232-233. As the authors observe on page

232, there are numerous methods for hiding or destroying digital information or interfering with a forensics examination, from something as simple as emptying the Recycle bin to using command-line scripts or specialized software. For example, as indicted in the note at the bottom of page 232, the Remove Hidden Data feature in Microsoft Office and Adobe Acrobat could be considered an anti-forensics method if used outside the course of normal business activities. Traces of most anti-forensics activities are stored in the Registry or other areas of the OS. If the original hard drive or a bit-by-bit copy is not available, you can examine only the data or metadata that remains embedded in native files, which is why you want to be able to obtain forensic images of the hard drive. Reviewing how a file is deleted in Windows can be helpful in understanding anti-forensics. Recall from a previous Module that we may be able to look at the Master File Table (MFT) or the File Allocation Table (older Windows operating systems), which is a database of information about files and is stored in a part of the hard drive that users do not typically see or know about. PST and OST email files have similar structures. As the authors note, the act of deleting an email message changes only the email markers stored in the database; it does not delete the email itself. The authors describe a way to look at an email file in PST format at the binary level and how to recover a deleted email by restoring altered bits. They state that reviewing these concepts with employees who do not have forensics or IT expertise is important to make sure that correct files are being produced in response to discovery requests (and to work with a qualified digital forensics expert if tampering or deletion is suspected).

Chapter 9 of *E-Discovery: An Introduction to Digital Evidence* concludes with a chapter summary and a glossary of key terms.

Some materials from Exterro are provided as part of Module 16 in Canvas. Note particularly the white paper from Exterro titled *6 Tips for Successfully Adopting E-Discovery Technology*. Note from the article from *The Indiana Lawyer* that even lawyers who should know better have been known to engage in behaviors that put the attorney-client privilege at risk and that also make them subject to some significant disciplinary action, in this situation, a four-year suspension.

I am so pleased that you enrolled in this course! The career opportunities in e-discovery will continue to increase, as will positions in related fields like digital forensics and information governance. You have been a TERRIFIC group of students and have made this semester especially rewarding for me!

Please let me know if you have questions about Module 16 or the reading assignment.

Congratulations on completing the course! Have a wonderful holiday break! If you are graduating in December, congratulations and best of luck as you move forward in your life and career!"