OH, SNAP!

The State of Electronic Discovery Amid the Rise of Snapchat, WhatsApp, Kik, and Other Mobile Messaging Apps

SARA ANNE HOOK AND CORI FAKLARIS

Move over email, and take a back seat, text messages. Mobile apps such as Snapchat, WhatsApp and Kik Messenger are fast taking the lead role in electronic communications. This social media shift creates new issues in litigation related to electronically stored information just as the 2015 revisions to the Federal Rules of Civil Procedure promise to shake up the ever-evolving field of electronic discovery.

Introduction

Corporations spend considerable time and money preserving traditional electronic communications such as email, but the proliferation of Internet-enabled technologies and devices has added legal wrinkles to the preservation, discovery, and production of electronically stored information (ESI). While text messages were one of the focal points of the recent Deflategate controversy, which involved claims that Tom Brady, star quarterback of the National Football League's New England Patriots, took part in alleged football tampering during the January 2015 American Football Conference Championship game against the Indianapolis Colts, future inquiries may be determined by tweets, snaps, or some other app-based communication. In particular, new questions and issues in electronic discovery (e-discovery) have been sparked by the explosion in popularity of social networking services (SNS),[1] such as Facebook, that provide for a mix of public and private communications[2] across multiple devices and settings. Many cases already have revolved around the allowable scope of discovery for communications via social media and how to tailor that scope, such as whether to provide passwords for witnesses' social media accounts to trial teams, how to determine which members of the legal team are afforded access, and how long such access should be permitted.[3] Other cases have addressed, and will continue to address, the duty to preserve all relevant social media evidence and what that means in the ever-evolving social media landscape.[4]

In the past few years, a new breed of instant messaging apps,[5] such as Snapchat,[6] Kik Messenger, WhatsApp,[7] and many others, have rapidly been gaining popularity among users and attracting billion-dollar valuations from investors.[8] Among their most notable features are that the content (in theory) is not automatically archived—it disappears from view after a certain period of time—and that the apps' stand-alone nature keeps conversations relatively private as well as limits their "discovery" online in the broader sense. While conventional wisdom has been that such messages are often sexually oriented, research has shown that Snapchat adult users post about a variety of subjects that range far beyond the exchange of explicit photos or conversation about socially proscribed behavior, such as funny meme images or more stream-of-consciousness talk.[9] Messaging apps' more intimate feel and the restricted visibility of chats, photos, video clips, and other content have no doubt contributed to their popularity, and it should not be assumed that messages never deal with work or matters of more import than the latest viral video. Said one analyst: "It often feels like a more controlled, real-time replacement for email."[10]

On its face, the short-lived or ephemeral nature of such posts and the high walls around these services' communication systems seem to challenge the discoverability of information and imply the need for new spoliation standards for users and the services themselves. Legal professionals need further clarification of how and in what contexts the content on these messaging apps is discoverable as well as what duties exist to preserve information in these contexts and which dangers to watch out for. The following are among some of the questions this article will address: What are the most notable mobile messaging apps now in widespread use? How do they work? What issues in e-discovery arise from these apps? Can lessons be drawn from previous decisions regarding e-discovery for ESI in general and text-messaging and social media platforms in particular? What issues should lawyers be on the alert for?

While the main features of these SNS platforms seem to preclude many of the traditional methods of e-discovery, the evolution of their features and users' own behaviors do indicate some targets of opportunity for legal teams wishing to recover such communications. This article provides an overview of the case law and best practices for legal professionals seeking such data, and it notes where the law seems unclear or ripe for new interpretations. Certain trends in mobile technology are also noted, as are potential ramifications of the 2015 amendments to the Federal Rules of Civil Procedure, which may impact inquiries into SNS-related data.

History of the Existing Law on e-Discovery

Much of our current understanding of e-discovery can be traced back to the landmark *Zubulake v. UBS Warburg* case. After two years of discovery efforts following her initial filing of a 2001 Equal Employment Opportunity Commission claim of gender discrimination and her subsequent 2002 lawsuit, in 2004 plaintiff Laura Zubulake requested the court sanction UBS for failing to preserve relevant emails and for tardy production of other information critical to her claims.[11] Judge Shira Scheindlin agreed that sanctions, in the form of an adverse inference, were warranted based on the repeated failures of both UBS and its counsel.[12] Although this and related findings proved of little import to the case's ultimate outcome,[13] Scheindlin's rulings had a substantial impact on the legal profession, as she was the first judge to set forth sweeping guidance as to what e-discovery duties parties have when in litigation, to define e-discovery so as to encompass the full range of ESI in current usage, and to identify and impose sanctions for a party, and its counsel, failing to sufficiently fulfill their ESI-related duties.[14]

Scheindlin issued five groundbreaking opinions in 2003 and 2004 that set forth the following key e-discovery concepts, as elucidated here by the investigative and risk-consulting firm Kroll Ontrack:[15]

- The scope of a party's duty to preserve electronic evidence during the course of litigation;
- Lawyer's duty to monitor their clients' compliance with electronic data preservation and production;
- Data sampling;
- The ability for the disclosing party to shift the costs of restoring "inaccessible" backup tapes to the requesting party;
- The imposition of sanctions for the spoliation (or destruction) of electronic evidence.

Around the same time that the landmark *Zubulake* decisions were being issued, litigator George Socha and information technology (IT) consultant Tom Gelbmann were compiling what became the

Electronic Discovery Reference Model (EDRM) in response to their perception that no consensus existed among lawyers and vendors as to the best practices for e-discovery in an environment of rapid proliferation of such issues and explosion of potentially discoverable ESI.[16] To that end, Socha and Gelbmann established a coalition in May 2005 that now comprises some 401 organizations, including vendors, law firms, government and educational entities, and industry groups involved with e-discovery and information governance.[17] The EDRM, first published in 2006, introduced a conceptual and iterative framework for e-discovery that now has nine steps: information governance, identification, preservation, collection, processing, review, analysis, production, and presentation.[18]

Also in 2006, the Advisory Committee on Civil Rules (of which Scheindlin was a member) issued proposed revisions to the Federal Rules of Civil Procedure (FRCP) governing the discovery of ESI, which had been in the works since 2000. These revisions addressed the rapid proliferation of legal issues sparked by the 1990s-era revolution in IT.[19]

The revisions were ultimately adopted, and the amendment to FRCP Rule 26(a) recognized ESI as a separate object of discovery. Under the amendment, ESI was specifically defined as encompassing "all sorts of information stored in any medium including future developments in computer technology."[20] Furthermore, the amendments to FRCP Rules 16 and 26:

- Directed the parties to discuss issues involved with e-discovery;
- Addressed what forms the ESI should be produced in;
- Dealt with problems with the reasonable accessibility of some data;
- Directed the parties to discuss how to preserve ESI;
- Covered issues of privileged data and attorney product;
- Contained provisions for safe harbor from sanctions due to the loss of data from routine computer system operations if undertaken in good faith.[21]

The impact of the amendments to the FRCP on litigants was immediate. "The real genius behind the Amendments is that, when properly used, the responsibility rests upon the parties to consider the evidence they need, where it is located, and how to acquire it in a way that is fair and proportional to the needs of the case," wrote Bennett B. Borden et al. in "Four Years Later: How the 2006 Amendments to the Federal Rules Have Reshaped the E-Discovery Landscape and Are Revitalizing the Civil Justice System."[22] The U.S. Court of Appeals for the Seventh Circuit has built on FRCP Rule 26(f)(2) with its Discovery Pilot, which has published guidelines to streamline the electronic discovery process and resolve any disputes, including a model standing order for judges' use, as well as suggesting ideas such as designating a liaison for e-discovery issues.[23]

Nevertheless, the costs and logistical burdens of e-discovery continued to multiply. The escalation of these burdens amid an accompanying rise in the adversarial behavior of litigants led to the 2008 Sedona Conference Cooperation Proclamation.[24] This document asserted that cooperation in e-discovery was not incompatible with "zealous advocacy" or ethical representation. It set forth an agenda to seek commitment to cooperation from legal system stakeholders and to produce toolkits to assist and train them in "techniques of discovery cooperation, collaboration, and transparency."[25] Courts began to cite the Proclamation and embrace its tenets almost immediately, with the result that cooperation among parties during discovery is now the expectation rather than the exception.[26]

Such cooperation has become particularly important with the increase and near-ubiquity of Internet-connected computing devices and social media, which have vastly multiplied the amount of ESI that is potentially discoverable in a case and thus the burdens on all parties involved. Lessons in handling social media evidence can be derived from frameworks and best practices for e-discovery as well as relevant statutes and case law. As with earlier forms of ESI, evidence from SNS and from social media generally is discoverable and useful in all kinds of litigation, within some parameters.

The Stored Communications Act (SCA) of 1986,[27] which governs the circumstances under which electronic data services and storage

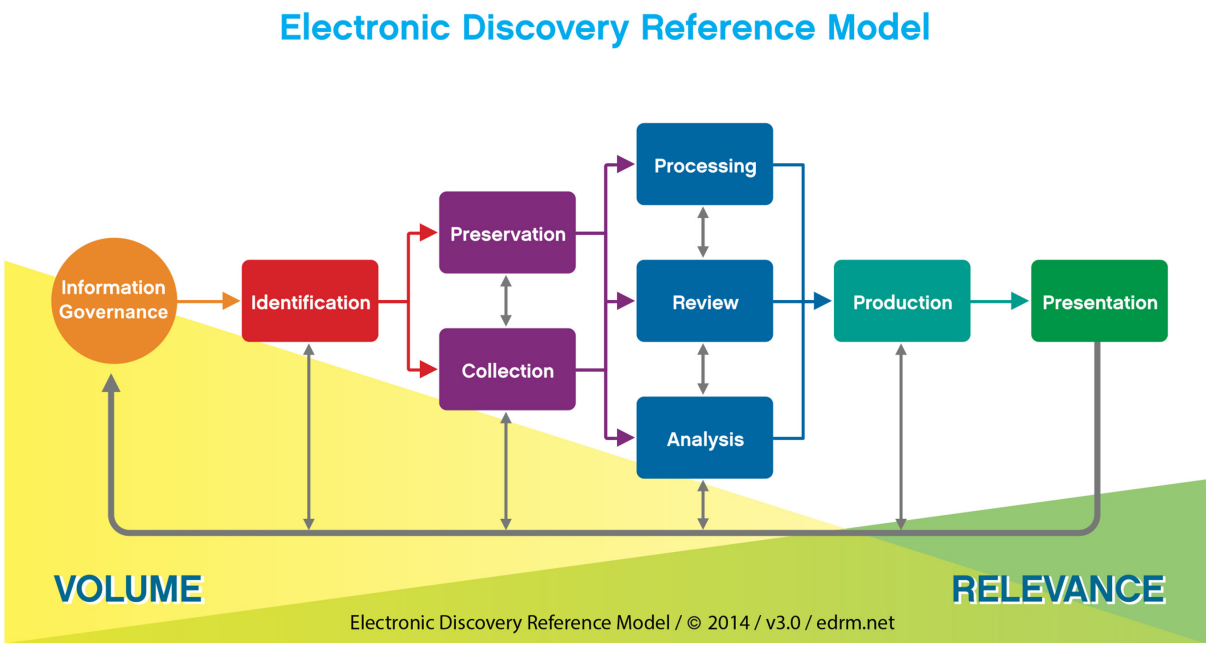

Figure 1: Diagram of the Electronic Discovery Reference Model

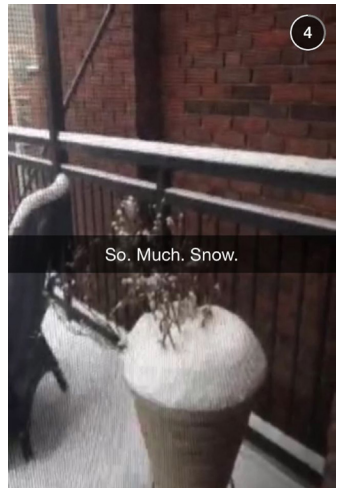

Figure 2: Screenshot of Snapchat "Friends" screen
Figure 3: A screenshot of one "Snap" posted by co-author

providers may disclose customers' data,[28] has generally been used to hold that Internet service providers (ISPs) and social media websites are not bound to produce postings in response to a civil subpoena.[29] Instead, the party seeking discovery must do so under FRCP Rules 34 and 36, with the best practice considered to be serving document requests and/or a subpoena on the opposing party or on a nonparty witness to the posting.[30] "With an executed authorization, a properly issued subpoena, and, in most cases, a reasonably small payment for associated costs, litigants can obtain all information related to a user's social media account," writes attorney Margaret DiBianca in her 2014 article for *Business Law Today*, "Discovery and Preservation of Social Media Evidence."[31]

DiBianca notes that social media content should be included in any litigation-hold notices requiring the preservation of evidence and stresses the critical importance of counsel taking steps to ensure such preservation, such as by hiring third-party vendors to assist with the tasks or instructing their clients of their duty to avoid evidence spoliation by deleting or "cleaning up" their accounts.[32] In addition, DiBianca observes that discovery of social media evidence merely requires the application of basic discovery principles in a new context. Parties should have no reasonable expectation of privacy given that social networking services' basic "sharing" functionality generally precludes a finding of such a privilege, even if the content was only shared with or visible to one or a limited number of others. "Courts generally find that 'private' is not the same as 'not public,'"[33] she observes, though courts also are not inclined to allow a "fishing expedition" through the entirety of a party's SNS accounts. According to DiBianca, the challenge in these cases for opposing counsel is identifying specific evidence showing the need for access to social media through discovery, which is only possible "if at least some part of [the] producing party's social media content is publicly available."[34]

An Overview of Notable Mobile Messaging Apps

Social networking services of concern to legal professionals have now advanced well beyond Facebook, Twitter, and other platform-based social media sites. The most buzzed-about SNS category in the past several months has been mobile messaging apps. According to data from the research firm comScore that was cited in early 2015 in *The New York Times*, "40 percent of mobile subscribers in the United States use an instant messaging app on their phones at least once a month."[35] The universe of such apps goes far beyond the standard short message service (SMS)[36] and multimedia messaging service (MMS)[37] functionality for texts, images, and videos that have been provided for years by cellphone carriers.

One of the fastest-growing apps is Snapchat. The free mobile app, which was founded by students at Stanford University in 2011 and now claims a user base of close to 100 million daily active users,[38] lets users snap and send "disappearing" photos and videos to friends from their smartphones.[39] This gives it a reputation as an app of choice for those sending sexually explicit or other sensitive content, although, as noted above, research has shown Snapchat users send a much wider variety of types of content. Once users take a photo or video (known as a Snap) using their mobile phones, they put a timer of one to 10 seconds on the content to control when these snaps disappear after being opened in the app.[40] However, several work-arounds exist for this "deletion by default." First of all, the app allows recipients to take and save screenshots of snaps, though it also alerts the sender that they have done so. Moreover, nothing stops a user from taking a photo of the screen with another phone's camera. The sender is also free to preserve the photo or video outside of Snapchat by saving the content to his or her phone.[41] Lastly, though Snapchat does not authorize them,[42] some third-party applications and plugins enable users to save their snaps.

Unopened or pending messages stay on Snapchat's servers for 30 days,[43] according to the company. Snapchat says that it does not retain users' data on its servers once these messages are opened. Nevertheless, the Oct. 28, 2015, update to its privacy policy notes:

> We can't guarantee that messages and corresponding metadata will be deleted within a specific timeframe. Keep in mind that we may also retain certain information in backup for a limited period of time or as required by law. This is true even after we've deleted messages and corresponding metadata from our servers. We also sometimes receive requests from law enforcement requiring us by law to suspend our ordinary server-deletion practices for specific information. Finally, of course, as with any digital information, there may be ways to access messages while still in temporary storage on recipients' devices or, forensically, even after they are deleted.[44]

Snapchat now also offers three notable functions through which a user can preserve content, at least within the app, for a certain period of time. First of all, the Replay feature allows users to replay a Snap once a day for free and, as of September 2015, up to 20 times for an additional charge.[45] Secondly, inside the Chat function, a user now can press and hold on a chat message to save the content at no charge.[46] Thirdly, a user can save a photo or video to Stories, which are curated clips of events uploaded and selected by users. Depending on the user's privacy settings and selection options, the photo or video may be included in his or her personal network (the option labeled My Story) and viewable for up to 24 hours[47] or as part of the Live Stories collections selected by the app from users who are at the same public event or notable location.[48]

These features—as well as Snapcash, a method for transmitting money through the service,[49] and Discover, a page where multimedia clips can be posted by media brands—are part of the app's attempts

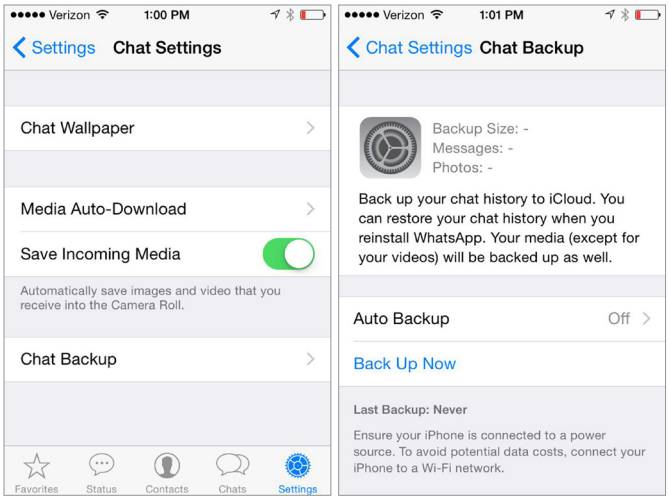

Figure 4: A screenshot of WhatsApp's Chat Settings showing the option to Save Incoming Media and for Chat Backup

Figure 5: A screenshot of the WhatsApp Chat Settings showing where to toggle Auto Backup and detailing the iCloud backup

to boost the engagement of its large user base and to correspondingly monetize that audience, the potential for which reportedly spurred a $3 billion acquisition offer from Facebook.[50] The new features led the company to revamp and expand its support pages, terms of service, and privacy policy at the end of October 2015 to clarify its use of content in plainer language. This caused a stir when actor and former White House staffer Kal Penn tweeted a section of the new terms of service[51] that reads, in part, "We may access, review, screen, and delete your content at any time and for any reason."[52] Snapchat later clarified in a blog post that "Snapchat is not—and never has been—stockpiling your private snaps or chats."[53]

Snapchat is not the only mobile messaging app gaining rapid adoption. An even more popular (if less talked-about) messaging app is WhatsApp. In fact, some data analysts rank this platform as the most popular messaging app in the world. WhatsApp, which was founded in 2009, proudly touts its base of active, as opposed to merely registered, users: a whopping 1 billion as of 2016.[54] This app, once installed, can read the user's existing database of phone contacts and be used to send messages such as texts, photos, video, or even audio messages via SMS to any other device that has the app installed. WhatsApp has settings to both save incoming media on its users' mobile devices and to back up chats, for example to iCloud for iOS users, and send chat histories for the past seven days to email. It also displays when the message or chat is viewed by the recipient.

Until this year, WhatsApp's only charge for Wi-Fi users was a $1 yearly renewal fee or for data usage for those connected to a carrier's network; now even that fee is being scrapped, as the service experiments with charging businesses to connect with customers.[55] One source summarized WhatsApp's appeal and disruption in the mobile space as doing "to SMS on mobile phones what Skype did to international calling on landlines."[56]

Another leading mobile app is Kik Messenger, modeled on a popular previous-generation app, BlackBerry Messenger. Kik has the distinction of identifying users not by phone number but by username, which makes it attractive to those seeking some degree of anonymity or who do not have a cell phone. This app also allows users to access mobile websites offering games, memes, stranger connections, and other content from within the app as part of its chat feature[57] and to share videos, photos, sketches, and other content via Wi-Fi, as well as to take screenshots. With close to 40 percent of its more than 200 million registered users between 13 and 18 years old[58] and with its ease of masking identity, Kik has reportedly become an app of choice for pedophiles.[59] This led the company in March 2015 to adopt Microsoft's PhotoDNA technology[60] to detect and delete any child pornography and to join the Virtual Global Taskforce[61] to combat child abuse.[62]

Besides Snapchat, WhatsApp, and Kik, literally dozens of other messaging apps are available for mobile devices, with millennial favorites Instagram, Skype, Tinder, and YikYak among 2015's most-downloaded in the iOS App Store and Android apps section of Google Play. Among other apps rated most popular globally according to their active users are China-based Tencent QQ[63] and WeChat,[64] South Korea-based KakaoTalk,[65] Cyprus-based Viber,[66] and Japanese app LINE,[67] each of which utilize some of the same features and processes as Snapchat and WhatsApp. Moreover, a market has also grown for many enterprise and otherwise "secure" mobile-friendly apps for messaging, such as Symphony,[68] Slack,[69] Yammer, Wickr, Lua, Confide, Vaporstream, and TigerText.[70] With the global proliferation of SNS apps, a litigator would be wise to inquire if a party to U.S. litigation has used or is using one of the apps referenced in this article, or any other SNS apps, and to start the process of ESI preservation and production early. This is particularly important if the party has ties to individuals outside the United States. These apps might also contain relevant communications for parties to cross-border or multinational litigation.

Examination of e-Discovery Issues Posed by These Apps

Based on the above descriptions, it is reasonable to assume that a party to a civil lawsuit may be using or have used one of these mobile messaging apps during the period in question. Lawyers and their teams should be thinking about ESI from these apps when developing case strategy, creating a discovery plan, and drafting requests for production. Among the questions that may arise:

Does a permanent archive of such data exist?

The answer is likely yes. The user-generated content (UGC),[71] such as photos that are shared within the app, may be held on the app's remote servers. In the case of Snapchat, the Federal Trade Commission (FTC) forced the company to modify its terms of service[72] to clarify that unopened posts may be retained for 30 days and that other data may be recoverable through backups or other means.[73] The FTC approved a final order on Dec. 31, 2014, settling charges that "Snapchat deceived consumers with promises about the disappearing nature of messages sent through the service" and also "deceived consumers over the amount of personal data it collected and the security measures taken to protect that data from misuse and unauthorized disclosure."[74]

UGC may also be stored within the app itself locally on the user's mobile device and/or as a screenshot in the mobile device's camera roll or other image archive and thus could be discoverable via a civil subpoena. In addition, because third-party apps can be used to either save or upload content to the service, these should also be considered a possible source of archived ESI. In the case of Snapchat, a quick search of the App Store for iOS in 2015 revealed

the apps SaveSnap, Snap Keeper, Snap Sender, and SnapBox among dozens of other third-party apps available to archive and upload Snapchat posts. The popular Android app SnapSave and the Web client SnapSaved.com were said to be the vehicle for a hack known as "The Snappening" (as it was nicknamed in the online forum 4chan), which resulted in the 2014 release of a database of at least 100,000 user images, including underage nude photos.[75] However, in response to this privacy breach and others, the ability to recover saved snaps via these third-party apps has been curtailed by Snapchat, which moved in 2015 to lock out third-party apps' access to its application programming interface (API) and advised users to upgrade to the latest Snapchat version incorporating the changes.[76] Notwithstanding the guidance from providers like Snapchat, it is important to find out if a client or the opposing party has upgraded his or her phone or apps to reflect these changes, as that may impact the scope of discovery.

In the case of WhatsApp, identifying the app's archive of chat histories, incoming media, and deleted messages appears even easier. The mobile app has provided extensive documentation on its website under the FAQ tab, which has entries for recovering UGC from Android devices, iPhones, Windows phones, Nokia S40 and S60 devices, and BlackBerry and BlackBerry 10 devices. For example, under the Android FAQ for "How do I restore my messages?" WhatsApp notes that its software backs up chats every day at 3 a.m. by default. However, the app notes the following caveats: The FAQ says that it only retains a seven-day chat history, either on the device's SD card or its internal memory; also, WhatsApp warns that any backup will overwrite the current chat history file unless the user creates a manual backup. The app FAQ provides directions for performing such a manual backup and recommends a list of file managers for locating and managing such backups.[77]

In addition to the content that is transmitted via mobile messaging apps, metadata such as the places, days, and times when the app was used or when content was uploaded, created, or shared may be available in archive form or in the mobile device's memory. Such data is likely relevant to the case, along with any relevant UGC created or shared via mobile messaging apps, and should also be included in e-discovery requests. Getting the timestamp for an uploaded video, for instance, may be critical to proving its admissibility. Finding the date, time, and sender GPS location for a text message sent inside one of these apps may help prove charges of texting while driving, regardless of the message's content.[78] This information could also be used to corroborate testimony from a witness, such as to verify a party's whereabouts at a time in question.

How can legal professionals identify the scope of discovery and tailor it appropriately?

As with social media evidence in general, the challenge for lawyers and their clients will be in identifying the need for access to nonparties' mobile messaging apps' content and metadata. Looking for publicly visible information on the sites may prove challenging, unless the parties involved have a relationship as mutual users of the apps and/or have shared or alluded to their use in other forums, such as on their Facebook walls, in emails or during real-time conversations. Nevertheless, it can be surprising how often users of these apps either post messages, videos, or other data for public or otherwise unrestricted access that makes the data visible to anyone who searches for their accounts. Therefore, one of the best methods for finding relevant messages may be to look to see what is there.

A second method for identifying the existence of such ESI is to ask. When making their lists of potentially relevant materials to request during discovery, lawyers and their clients should include posts on Snapchat, Kik, WhatsApp, and other mobile messaging apps along with social media such as Facebook and Twitter, as well as SMS text messages, emails, and other electronic forms of communication. This puts the opposing party on notice to check these accounts for information relevant to the lawsuit, which they may not realize could exist on these services. It also serves as an early alert that they should take steps to safeguard any relevant ESI, such as preventing routine expiration of the messages or delaying app updates.

In a 2015 interview with *Indiana Lawyer*, Indianapolis attorney Marc Quigley suggested another avenue for identifying messages sent via an app on a mobile device: depositions. "I have witnessed and been involved in depositions where someone asks someone else to take a cell phone out and read a series of messages," he said. "What it did was ultimately preserve the fact that there were these communications."[79]

Employers also should be able to access any messages sent and received via these apps on employees' work-issued mobile devices, as set forth in *City of Ontario v. Quon*. Notably, the city in this 2010 case had the foresight to publish and record employees' consent to a "Computer Usage, Internet, and Email Policy" that specified that the city "reserves the right to monitor and log all network activity, including email and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources."[80] Such a policy would also be a reasonable justification for searches of employees' work-issued mobile phones for messages sent via Snapchat, WhatsApp, and enterprise mobile messaging apps such as Slack, Yammer, and the like, all of which rely on cellular network data as well as Wi-Fi Internet connections for use.

In terms of mobile messaging apps, it is notable that enterprise-focused apps such as Slack[81] and others cited above could be used by an employer that has entered into a paid contract for their services, as the paid versions usually offer better features and functionality than do the free versions of these apps. In this situation, it may be possible to use the SCA to compel production of these messaging apps' archives of relevant employee communications, as established in 2008's *Flagg v. City of Detroit*.[82] In that case, the court made an exception to the general finding that the SCA prevents civil subpoenas of ISPs and social-media websites to compel production of UGC stored on their own servers. The city of Detroit had entered into a contract with SkyTel to provide text-messaging capability to its employees. Upon learning that the company had retained some messages even after the contract was canceled, the city moved to subpoena SkyTel for the records. The court "reasoned that nothing in the plain language of the SCA requires a sweeping prohibition against civil discovery of electronic communication, especially if the communication was created by and maintained within the control of the City."[83]

Attorneys and their clients may have more trouble arguing to expand the scope of discovery beyond the immediate parties in the case by requesting access to or materials from accounts on mobile messaging apps that do not belong to but are used by the parties to the lawsuit, barring clear evidence that this would produce relevant information. In the 2014 decision in the employment discrimination lawsuit *Finkle v. Howard County*,[84] the U.S. District Court in Maryland denied the plaintiff's request to identify account data for

"all email accounts, social media services, Internet discussion groups or pages, and cellular telephone or text messaging services" used by nonparty employees, reasoning that "there is no reason to invite an unfettered 'fishing expedition' … without a viable reason to believe that relevant information would be accessible to the Plaintiff or would be contained therein."[85] This decision relied on language in FRCP Rule 26 that has since been amended to further limit the scope of discovery by its proportionality, "considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit."[86]

How can this data be preserved and collected?

The content on mobile messaging apps, any backups that may exist, and the metadata for both should be included in any litigation holds requiring the preservation of evidence. Lawyers should direct their clients not to delete the apps or the posts on these apps, as well as their SMS messages, email, social media, and other services. Even in cases of workplace lawsuits, lawyers should not overlook employees' personal mobile devices because many users mix personal and professional communications. In fact, lawyers should explicitly warn their clients not to destroy or trade in any of their mobile devices, not to download and install upgrades for the apps on these devices, and not to delete or overwrite the existing local backups for these apps' data. Such actions could expose them to sanctions for spoliation or claims of acting in bad faith. A notable example in 2015 arose in the Deflategate controversy involving Tom Brady, a quarterback for the New England Patriots. Brady destroyed his cell phone shortly before meeting with investigators who had sought access to his text messages and to other data stored on the device. The National Football League's decision in July 2015 to uphold Brady's four-game suspension for the start of the 2015–16 season largely hinged on Brady's destruction of the phone, with NFL Commissioner Roger Goodell citing this action as the principal factor in his finding that "Mr. Brady had failed to cooperate with the investigation."[87]

In cases that may involve a large amount of data, the parties may wish to negotiate and implement a protocol for the handling of ESI. This protocol should be extended to determine how to account for ESI from any mobile messaging apps used for personal (Snapchat, WhatsApp, etc.) or professional (Slack, Wickr, etc.) communication.

Lawyers should be prepared for arguments that ESI from a mobile messaging app such as Snapchat is presumptively, not reasonably, accessible. The Seventh Circuit Discovery Pilot Program Model Standing Order,[88] for example, includes the following in that category:

- Deleted, slack, fragmented, or unallocated data on hard drives;
- Random access memory (RAM) or other ephemeral data;
- Online access data, such as temporary Internet files, history, cache, cookies, etc;
- Data in metadata fields that are frequently updated automatically, such as last-opened dates;
- Backup data that is substantially duplicative of data that is more accessible elsewhere;
- Other forms of ESI whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary course of business.

Someone unfamiliar with end-user recovery methods or details of the Snapchat terms of service cited above, for example, may claim that all snaps by definition are "ephemeral data."[89] However, refuting such arguments may not be difficult, depending on the claims and defenses involved in the lawsuit and the amount of knowledge of the current state of IT.

In that regard, it may be helpful to hire a third-party vendor to assist in the preservation and collection of data from any mobile device and from any mobile messaging accounts belonging to the opposing party or to a nonparty witness. The vendor should be knowledgeable about how to freeze or stop automatic backups, such as WhatsApp's daily backup, that may overwrite relevant and discoverable content or metadata. Some vendors have developed expertise related to mobile messaging apps, such as Decipher Forensics of Utah. In a blog post from 2013, this firm said that it had devised a method for recovering supposedly deleted Snapchat images from Android devices[90] using Access Data's Forensic Toolkit software.

Recovering ESI from iOS devices belonging to the opposing party or to a nonparty witness may be possible via the same or similar forensic software, though Decipher Forensics has not posted any similar research. However, the same result might be accomplished through the use of widely available third-party apps for browsing an iPhone or iPad's files and folders. BuzzFeed in 2012 posted a method for accessing the Snapchat application's "tmp" folder on an iPhone connected to a desktop Mac via the iFunBox app, a free file- and folder-manager for iOS devices that uses a classic Windows-style user interface.[91] Photographer and tech enthusiast Nick Keck posted a YouTube video in 2013[92] to prove that expired Snapchat videos could be recovered on iPhone and iPads using Cydia's iFile app, which functions as a jailbroken iOS device's file and folder browser under the root user.[93]

Of particular note with mobile devices is that it is not possible to generate a true forensic image of the device, as an investigator would with a traditional personal computer.[94] "Because the device must be powered on to perform the extraction, mobile forensics processes make changes to the evidence device," writes Brendan Morgan in *The Federal Lawyer*. "Although the process doesn't change user data, it does alter the information within the device's operating system."[95] Morgan cautions that ignorance or inexperience by the computer forensics examiner of the proper processes and methodologies could lead to damaging or altering ESI, missing other data that is potentially relevant and discoverable, misinterpreting the data that is found, and preparing an inaccurate report of the findings.[96] Thus, finding the right vendor is an important step in preserving and collecting the right data from the opposing party or nonparty witness.

What does evidence spoliation mean in this context?

The landmark *Zubulake* opinions put lawyers on notice more than 10 years ago of their duty to preserve any ESI once litigation is anticipated. This obligation was reiterated by Scheindlin in her 2013 ruling in *Sekisui v. Hart*,[97] in which she reversed the decision of a lower court and imposed sanctions for willfully and permanently destroying the ESI of two key parties for failing to impose a litigation hold for more than a year to preserve critical emails and for failing to advise its IT vendor for nearly six months of the litigation hold. Scheindlin granted the plaintiffs' request for an adverse inference jury instruction as well as monetary sanctions.

As has been reiterated in numerous other cases, other forms

of ESI beyond emails, such as text messages, are included under the same duty to preserve. In 2014's *Calderon v. Corporacion Puertorriqueña de Salud*,[98] the defendants demonstrated (via records obtained with an ex parte subpoena from T-Mobile) that the plaintiff had received 38 relevant text messages and sent numerous additional messages in response but then failed to produce any of them during discovery. As a result, the court sanctioned one of the plaintiffs for spoliation for failing to preserve the text messages sent and received by him and said that it would give an adverse inference at trial.

One of the most notable such spoliation examples of the past few years is *Small vs. University Medical Center of Southern Nevada*.[99] In the lengthy and fairly blistering report of Aug. 18, 2014, the Special Master recommended sanctioning the defense for "extraordinary misconduct and substantial and willful spoliation of relevant ESI"[100] from a spectrum of sources, including laptops, personal mobile devices, and BlackBerry and SMS messaging apps, during a two-year period. To remedy the prejudice to plaintiff, the Special Master recommended approving certification of the class alleging that employees were deprived of appropriate wages and overtime compensation and "a presumption in the plaintiffs' favor on a range of issues"[101] as well as monetary sanctions. "Today, ignorance of technology is simply an inadequate excuse for failure to properly carry out discovery obligations."[102]

Just in the past several months, several cases have appeared dealing with e-discovery and WhatsApp. In *Brady v. Grendene USA Inc.,* the plaintiffs said they were unable to locate any emails responsive to defense counsel's request because they spoke mostly through regular text messages and WhatsApp—and then asserted that they were unable to retrieve those messages because their mobile phones had since been destroyed, lost, or stolen.[103] *Moulton v. Bane*[104] is among the first cases to address spoliation in the context of mobile messaging apps. It was discovered that David Bane had discarded more than 1,600 WhatsApp messages upon replacing his mobile phone in late 2014. The court found that the spoliation was not willful and was the result of "routine, good-faith operation of an electronic information system," because Bane said that he had asked Verizon staff to transfer everything from his old phone to his new phone and thought that this would include his WhatsApp archive. Bane was ordered to reimburse the opposing parties for the cost of retrieving these messages, but the judge noted, "Communication among counsel might have allowed a resolution of the issue without court action."[104]

Until more disputes and/or requests for sanctions come before a court regarding ESI from Snapchat, WhatsApp, or other such sources, a prudent litigator should heed the overarching obligation on parties and their counsel to preserve potentially relevant ESI once litigation is reasonably anticipated and to follow current best practices for the preservation, maintenance, and production of ESI from mobile device sources so as not to become infamous for having the first case to establish the precedent.

Looking Ahead

Despite the challenges, the above information should establish that at least some mobile messaging data may be discoverable. Will it continue to be?

As noted, it is likely that Snapchat and other mobile messaging apps will continue to tighten security and privacy controls on users' data in response to breaches and negative publicity, such as "The Snappening" hacking incident, which led Snapchat to recently clamp down on third-party apps' access to its API. "Deletion by default is the core of the company," noted a Snapchat spokesperson.[105] This may curtail the ability of computer forensics investigators to continue accessing and recovering ESI from users' devices, third-party apps, or the developers' servers.

Apple moved with its iOS 8 update of 2014 to make it possible for iPhone and iPad users to more easily delete and set expirations for some messages, including audio and video files. While this functionality is in large part a response to users' need to keep such messages from consuming their storage capacity, the more robust expiration options also seem aimed at competing with Snapchat's and WhatsApp's consumer-friendly deletion features.[106]

As horror stories mount about photos, videos, and other content coming back to haunt their subjects on social media, it is reasonable to assume that more app developers will be spurred to add automatic expiration of UGC to their products' options and thus shorten the time frame in which ESI is in existence and discoverable. Under these circumstances, it will be even more important for lawyers and parties to act swiftly to freeze or stop such expiration or overwrites of relevant ESI. It also suggests that some of the conventional wisdom among computer forensics experts regarding the existence and preservation of messages, even from older technologies such as emails and SMS texts, may be upended as that software continues to evolve—unless the industry or Congress moves to address e-discovery issues that would arise. For instance, the SCA could be amended to explicitly allow access to user data backups that may be accessible on tech firms' servers but which have already expired or were no longer saved on users' client devices, and/or to compel parties to carve out exceptions to automatic expiration of files for enterprise users regarding spoliation concerns in workplace lawsuits.

As lawyers grapple with the issues raised by mobile messaging apps, it is worth looking to how they could inform the next frontier of electronic discovery: ESI from wearable technology, such as Fitbit wristbands that monitor a person's physical activity or the new Apple Watch.[107] The issues arising from mobile messaging apps should also have parallels with those involving wearable tech, given several similarities:

- The software and their devices are increasingly popular;
- As with mobile phones and associated cloud backup services, they may be creating data archives either locally or on a device or server to which they are tethered or otherwise linked;
- Their electronic data content, such as health metrics, may be highly relevant to certain lawsuits, such as personal-injury cases and malpractice;
- Given that they also travel with their users and are sending information "on the go," their metadata such as timestamps and location data can be potentially as valuable as admissible evidence as the content itself, if it is necessary to prove users' whereabouts and what they were doing at the time and place in question.

Such devices are already prompting concerns about privacy, including whether the Health Insurance Portability and Accountability Act protections apply, and about the ownership and (particularly with biometric information) reliability of their data. At least one legal expert recently quoted in the *ABA Journal* noted that even if the

substantive content of such data proves to be unusable, the metadata could be used to corroborate testimony from an expert witness, such as a physician.[108]

Impacts of the Latest FRCP Amendments

Finally, the newest FRCP amendments, effective Dec. 1, 2015, are likely to impact various aspects of e-discovery. Some other changes may also be of note regarding ESI from mobile messaging apps specifically:[109]

FRCP Rule 26(c)(1)'s new language will expressly acknowledge the court's authority to allocate the expenses of discovery, including electronic discovery, to the requesting party. These expenses could become prohibitive for the discovery of ESI from mobile messaging apps if it becomes necessary to hire a forensics investigator with sufficiently sophisticated tools and know-how to preserve, collect, and analyze data from a cell phone or locally stored cache of mobile messaging data without altering or damaging the ESI in the process.

FRCP Rule 26(d)(2) will allow a party to serve a Rule 34 document request prior to a FRCP Rule 26(d)(f) meeting between the parties, with the date of service calculated to the date of the first such meeting. This change, as well as rewording of FRCP Rule 16(b)(3)(B)(iii) to specify that a court may address the preservation of ESI, may encourage additional and earlier use of preservation holds, which is particularly valuable for discovery of ESIs in regard to mobile messaging apps from opposing parties and nonparty witnesses. Time can be of the essence in tracking down and securing data from mobile devices and apps such as Snapchat and WhatsApp that are often subject to regular background updates of the software and overwrites and expirations of cached data and chat backups.

FRCP Rule 34 includes several changes that could impact production of mobile messaging ESI, which could be both voluminous and emotionally significant to the opposing party. First, an objection to mass production of ESI, such as an employee's message archive on Symphony or Slack, must now be much more specific as to why the request is unreasonable; and second, such an objection must specify the part and allow inspection of the remainder to avoid withholding the entire document, which in this case could be part of all of a message chain found elsewhere in the archive. Third, the revised rule allows a responding party to state that it will produce copies of documents or ESI in lieu of permitting inspection, which could ease concerns about or even hostility to providing access to ESI on mobile devices or apps, often considered among a person's most valuable and intimate possessions and communications.

Of the changes, FRCP Rule 37's amendments seem most directly the result of the ever-ballooning complexity of preserving ESI as technologies such as mobile messaging apps appear and proliferate. The new Rule 37 does not create an explicit duty to preserve ESI in all circumstances, instead yielding to existing case law that the obligation to preserve such data begins once litigation is reasonably anticipated. It seems reasonable to conclude from the changes themselves as the committee notes on the 2015 amendments[110] that they should constitute a true safe harbor for many unsophisticated parties or nonparty witnesses who lose relevant ESI from mobile messaging apps, especially when acting in the moment with limited-to-nonexistent information about possible litigation. For example, a teenager using Snapchat at a concert likely would not be legally liable for failing to retain her snaps simply because a lawsuit followed from a car accident outside the venue that she may not have known was in the background of something else she recorded.

As to what can be done in the event of such loss, FRCP Rule 37(e)(1) focuses on the remedies available to the parties. These include "curative measures," such as allowing additional discovery and ordering the offending party to pay reasonable expenses incurred by the ESI's loss, and providing for punitive sanctions "only where the party's actions either (1) caused substantial prejudice and were willful or in bad faith or (2) irreparably deprived a part of a meaningful opportunity to present or defend against the claims made in the litigation."[111] This should help ease the risk of sanctions for unsophisticated parties or nonparty witnesses in the event that they failed to take "reasonable steps" to preserve ESI from mobile messaging apps that fall short of "willful or in bad faith," such as thoughtlessly clicking "Yes" to a push notification of a software update that causes damage to or deletion of any sought content, backups, or metadata.

This safe harbor, however, could give false comfort to IT and legal departments for businesses grappling with the spread of "deletion by default" messaging apps among enterprise mobile users. These entities are both sophisticated and nearly certain to be targets of litigation. It seems a mistake to think that courts will apply the same standards for determining spoliation in context of their lawsuits as with those involving unsophisticated parties or witnesses. Thus, it may be more critical than ever that IT and legal professionals take steps to obtain control over and centrally archive ESI from mobile messaging apps used by employees on any devices or accounts for work purposes, similar to other forms of electronics communication, such as email, that are now subject to their protocols for document retention and preservation. In the "Bring Your Own Device" era, this could involve requiring employees to allow IT departments to access and archive data from messaging apps that are held on or transmitted through their personal mobile devices as a condition of using them for work purposes. It may be prudent to educate employees about what they can and cannot use their personal devices or apps to talk about regarding work matters.

Parties would be well advised to be on guard and proactive in seeking preservation holds for ESI from mobile messaging apps as early as possible, per FRCP Rule 26. Attorneys should also pursue discovery of their opponents' ESI retention protocols to investigate whether any conduct that leads to a loss of relevant ESI from such apps could be construed as an abuse of the amended rules. Given the rapid growth in the use and popularity of mobile messaging apps, it is increasingly likely that this form of ESI will be critical to a case, and thus proper planning for addressing these issues is paramount. ⊙

Sara Anne Hook, MBA, J.D., is a professor at the Indiana University School of Informatics and Computing, where she has developed a suite of online courses in the emerging field of legal informatics. She is also adjunct professor in the Robert H. McKinney School of Law. Cori Faklaris is a longtime U.S. journalist and communications professional who is researching legal and communications issues involving mobile messaging apps for a master's degree in informatics from Indiana University-Purdue University Indianapolis, where she works as a research assistant for Professor Hook.

Endnotes

[1]A social networking service (alternately, social network site) is a platform for building and maintaining social relationships through the sharing of profile information, connections, messages and other content. Researcher Danah Boyd has noted that defining an SNS has become increasingly challenging as features, opportunities for interaction, practices and norms evolve and proliferate. *See* Nicole B. Ellison & Danah Boyd, Sociality Through Social Network Sites (Oxford University Press 2013).

[2]Adam Cohen, "Social Media and eDiscovery: Emerging Issues," 32 Pace L. Rev. 289 (Spring 2012).

[3]Allyson Haynes Stuart, "Finding Privacy in a Sea of Social Media and Other E-Discovery," 12 NW. J. Tech. & Intell. Prop. 149 (Spring 2013).

[4]Margaret (Molly) DiBianca, *Discovery and Preservation of Social Media Evidence*, Bus. L Today, A.B.A. (January 2014), *available at* www.americanbar.org/publications/blt/2014/01/02_dibianca.html.

[5]These apps are sometimes referred to as "over the top," or OTT, apps because they transmit information on top of the user's Internet or cellular network. *See* Dan York, "What is an Over-The-Top (OTT) Application or Service? A Brief Explanation," Disruptive Telephony, July 10, 2012, *available at* www.disruptivetelephony.com/2012/07/what-is-an-over-the-top-ott-application-or-service-a-brief-explanation.html (last visited Dec. 22, 2015).

[6]Andrew Lipsman, "Does Snapchat's Strength Among Millennials Predict Eventual Mainstream Success?" comScore Insights Blog, Aug. 8, 2014, *at* www.comscore.com/Insights/Blog/Does-Snapchats-Strength-Among-Millennials-Predict-Eventual-Mainstream-Success (last visited Dec. 22, 2015).

[7]*See* Statista, "Most Popular Global Mobile Messenger Apps as of March 2015, Based on Number of Monthly Active Users (in Millions)," *available at* www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps (last visited April 18, 2015).

[8]John Shinal, "More Big Money Pours Into Messaging," USA Today, Feb. 18, 2015, *available at* www.usatoday.com/story/tech/2015/02/18/new-tech-economy-john-shinal/23263625 (last visited April 18, 2015).

[9]Franziska Roesner, Brian T. Gill, and Tadayoshi Kohno, "Sex, Lies, or Kittens? Investigating the Use of Snapchat's Self-Destructing Messages," Financial Cryptography and Data Security Conference (2014) (pre-proceedings version), University of Washington, Computer Science & Engineering; Seattle Pacific University, Mathematics; *available at* homes.cs.washington.edu/~yoshi/papers/snapchat-FC2014.pdf.

[10]Mike Isaac and Michael J. de la Merced, "Why Apps for Messaging Are Trending," The N.Y. Times, Jan. 25, 2015, *at* www.nytimes.com/2015/01/26/technology/why-apps-for-messaging-are-trending.html.

[11]*Zubulake v. UBS Warburg*, 229 F.R.D. 422 (S.D.N.Y. 2004).

[12]*Id.*

[13]Victor Li, "*Zubulake* 10 Years After: Landmark Case Created An Industry—And Still Stirs Debate," A.B.A. J. (September 2014), *at* www.abajournal.com/magazine/article/looking_back_on_zubulake_10_years_later (last visited Sept. 2, 2015).

[14]*Id.*

[15]Kroll Ontrack, *Zubulake vs. UBS Warburg*, *available at* www.krollontrack.co.uk/zubulake (last visited April 18, 2015).

[16]Li, *supra* note 13.

[17]Electronic Discovery Reference Model coalition, website, EDRM LLC (2005–15), www.edrm.net [hereinafter EDRM].

[18]*See id.* at *EDRM stages,* www.edrm.net/resources/edrm-stages-explained (last accessed April 27, 2016).

[19]Richard L. Marcus, "The 2006 Amendments to the Federal Rules of Civil Procedure Governing Discovery of Electronically Stored Information: Fitting Electronic Discovery Into the Overall Discovery Mix," introduction to Shira A. Scheindlin & Daniel J. Capra, Electronic Discovery and Digital Evidence: Cases and Materials, 1-15 (The Sedona Conference, American Casebook Series, Thomson/Reuters 2009).

[20]*Id.* at 6.

[21]*Id*. at 5-13.

[22]Bennett B. Borden, Monica McCarroll, Brian C. Vick & Lauren M. Wheeling, "Four Years Later: How the 2006 Amendments to the Federal Rules Have Reshaped the E-Discovery Landscape and are Revitalizing the Civil Justice System," XVII Rich. J.L. & Tech. 10, 4 (2011), *available at* jolt.richmond.edu/v17i3/article10.pdf.

[23]Seventh Circuit Electronic Discovery Pilot Program, *Seventh Circuit Pilot Project Model Standing Order* (proposed) at 5, *available at* www.DiscoveryPilot.com/sites/default/files/StandingOrde8_10.pdf (last accessed April 27, 2016) [hereinafter E-Discovery Pilot Program].

[24]The Sedona Conference, *The Sedona Conference Cooperation Proclamation*, The Sedona Conference Working Group Series (2008), *available at* thesedonaconference.org/download-pub/3802.

[25]*Id.*

[26]Jonathan M. Redgrave and Peter C. Hennigan, "Learning to Cooperate," E-Discovery Bull. (November 2013), 26-30, *available at* www.redgravellp.com/sites/default/files/Article-Learning-to-Cooperate.pdf.

[27]Stored Communications Act, 18 U.S.C. §§ 2701–2712 (1986), *available at* www.law.cornell.edu/uscode/text/18/part-I/chapter-121 (last visited April 18, 2015).

[28]ABA Section of Litigation, 2013 ABA Annual Meeting, Aug. 8-12, 2013: *Social Media Evidence—How To Find It and How To Use It*, at 5, *available at* www.americanbar.org/content/dam/aba/administrative/litigation/materials/aba-annual-2013/written_materials/15_1_social_media_evidence.authcheckdam.pdf.

[29]*Id*. at 6.

[30]*Id.* Commentators have noted that seeking a release authorizing disclosure by the ISP or social media website is not the best practice in civil litigation. Instead, since the opposing party or a nonparty witness should have "control" over the posting if it is discoverable, as noted in *Flagg v. City of Detroit* in 2008, they should be able to produce it under subpoena without involving the ISP or website using commonplace methods. For example, if I am tagged on Facebook in a photo and caption and am then subpoenaed for it, I should be able to directly provide the information by hitting Command-P to print the webpage to PDF, and/or creating a screenshot of the image of the posting in my browser or phone app, and/or copying the permalink to the posting, and/or providing my username and password for an in camera review of my Facebook account limited to the view of that post only.

[31]DiBianca, *supra* note 4.

[32]*Id.*

[33]*Id.*

[34]*Id.*

[35]Mike Isaac and Michael J. de la Merced, "Why Apps for Messaging Are Trending," The N.Y. Times, Jan. 25, 2015, *available at* www.nytimes.com/2015/01/26/technology/why-apps-for-messaging-are-trending.html.

[36]Short messaging service is a standardized telecommunications protocol for sending text messages of up to 160 characters in length as well as ringtones and small graphics among cell phones and other mobile and Internet-connected devices. *See* Ofir Turel et al., "User Acceptance of Wireless Short Messaging Services: Deconstructing Perceived Value," 44 Information & Mgmt. (2007).

[37]Multimedia messaging service is a telecommunications protocol that extends SMS functionality beyond text messages, ringtones, and small graphics to large color images, extended text messages, music files, video clips, voice memos, email, and more. *See, e.g.* Stéphane Coulombe & Guido Grassel, "Multimedia Adaptation for the Multimedia Messaging Service," 7 IEEE Comms. Mag. (2004).

[38]Dylan Tweney, "Engagement To Die For: Snapchat Has 100M Daily Users, 65% of Whom Upload Photos," Venture Beat, May. 26, 2015, *available at* venturebeat.com/2015/05/26/snapchat-has-100m-daily-users-65-of-whom-upload-photos.

[39]"A Snapchat Explainer for Non-Millennials," Re/Code, Aug. 18, 2014, *available at* recode.net/2014/08/18/a-snapchat-explainer-for-non-millennials.

[40]Snapchat.com, "Snapchat Law Enforcement Guide," Oct. 16, 2015, *available at* www.snapchat.com/static_files/lawenforcement.pdf?version=20150604.

[41]*Id*. at 4.

[42]Snapchat.com, "Snapchat Support: Third-Party Applications and Plugins" (2015), *available at* support.snapchat.com/a/third-party.

[43]Snapchat.com, "Snapchat Law Enforcement Guide," *supra* note 40, at 6.

[44]Snapchat.com, "Privacy Policy," Oct. 28, 2015, *available at* www.snapchat.com/privacy.

[45]Snapchat.com, "Snapchat Support: Replay" (2015), *available at* support.snapchat.com/ca/replay (last visited Dec. 15, 2015).

[46]Snapchat.com, "Snapchat Support: Chat" (2015), *available at* support.snapchat.com/ca/chat (last visited Dec. 15, 2015).

[47]Snapchat.com, "Snapchat Support: Stories" (2015), *available at* support.snapchat.com/ca/stories (last visited Dec. 15, 2015).

[48]Snapchat.com, "Snapchat Support: Live Stories" (2015), *available at* support.snapchat.com/ca/live-stories (last visited Dec. 15, 2015).

[49]Josh Constine, "Snapchat Now Lets You Send Money To Friends Through Snapcash Deal With Square Cash," TechCrunch, Nov. 17, 2014, *available at* techcrunch.com/2014/11/17/snapcash.

[50]Evelyn M. Rusli and Douglas MacMillan, "Snapchat Spurned $3 Billion Acquisition Offer from Facebook," WSJ Digits Blog, Nov. 13, 2013, *available at* blogs.wsj.com/digits/2013/11/13/snapchat-spurned-3-billion-acquisition-offer-from-facebook.

[51]Andrea Peterson, "Snapchat's New Terms of Service Freaked People Out Because No One Reads Them," Wash. Post, Nov. 2, 2015, *available at* www.washingtonpost.com/news/the-switch/wp/2015/11/02/snapchats-new-terms-of-service-freaked-people-out-because-no-one-reads-them (last visited Dec. 15, 2015).

[52]Snapchat.com, "Terms of Service" (effective Oct. 28, 2015), *available at* www.snapchat.com/terms.

[53]Snapchat.com, "Protecting Your Privacy" *(*Nov. 1, 2015), *available at* blog.snapchat.com/post/132379796495/protecting-your-privacy.

[54]Ken Yeung, "WhatsApp Passes 1 Billion Monthly Active Users," VENTUREBEAT, Feb. 1, 2016, *available at* venturebeat.com/2016/02/01/whatsapp-passes-1-billion-monthly-active-users/.

[55]Natalia Drozdiak, "WhatsApp To Drop Yearly Subscription Fee," Wall St. J., Jan. 18, 2016, *available at* www.wsj.com/articles/whatsapp-to-drop-subscription-fee-1453115467.

[56]Tim Bradshaw, "WhatsApp Users Get the Message," Fin. Times, Nov. 14, 2011, *available at* www.ft.com/cms/s/2/30fd99a2-0c60-11e1-88c6-00144feabdc0.html#axzz3V8IfdvFg.

[57]Kit Eaton, "Messaging Services Bypass the Old SMS Route," N.Y. Times, March 25, 2014, *available at* www.nytimes.com/2014/03/27/technology/personaltech/messaging-services-bypass-the-old-sms-route.html?_r=0.

[58]Sarah Frier, "Kik Adds Tools To Prevent Child Exploitation on Messaging App," Bloomberg, March 10, 2015, *available at* www.bloomberg.com/news/articles/2015-03-10/kik-adds-tools-to-prevent-child-exploitation-on-messaging-app.

[59]David Foster, "Pedophile on Kik App: 'It Is Well Known in Our Industry,'" The Trentonian, July 28, 2014, *available at* www.trentonian.com/general-news/20140728/pedophile-on-kik-app-its-well-known-in-our-industry.

[60]Microsoft, "PhotoDNA Cloud Service," www.microsoft.com/en-us/photodna (last visited March 21, 2015).

[61]Virtual Global Taskforce, website, www.virtualglobaltaskforce.com (last visited March 21, 2015).

[62]Frier, *supra* note 58.

[63]Tencent.com, "About Tencent" (2016), *available at* www.tencent.com/en-us/at/abouttencent.shtml (last visited April 19, 2016).

[64]Steven Milward, "WeChat Now Has 500 Million Monthly Active Users," Tech in ASIA, March 18, 2015, *available at* www.techinasia.com/wechat-500-million-active-users-q4-2014.

[65]Willis Wee, "KakaoTalk Reveals It Has 140 Million Users, Made $203 Million in Revenue Last Year," Tech in Asia, April 19, 2014, *available at* www.techinasia.com/kakao-2013-203m-revenue-59m-profit-140m-users.

[66]Steve Costello, "Viber User Base Tops 600 Million," Mobile World Live, Aug. 5, 2014, *available at* www.mobileworldlive.com/viber-user-base-tops-600-million.

[67]Josh Horwitz, "Line Finally Reveals Its Monthly Active User Count," Tech in Asia, Oct. 9, 2014, *available at* www.techinasia.com/line-japanese-messaging-app-has-170-million-monthly-active-users.

[68]Kieren McCarthy, "Bubble? LMAO—YOLO! Wall St. Gets New Instant Messaging Service," *available at* www.theregister.co.uk/2015/09/14/wall_street_gets_new_instant_messaging (last accessed April 27, 2016).

[69]Owen Williams, "Slack Doubles in Size in Four Months to 1.1 Million Daily Active Users," TNW, June 24, 2015, *available at* thenextweb.com/insider/2015/06/24/slack-doubles-in-size-in-four-months-to-1-1-million-daily-active-users/.

[70]Ryan G. Ganzenmuller, "Snap and Destroy: Preservation Issues for Ephemeral Communications," 62 Buff. L. Rev. (2014).

[71]User-generated content is defined as content such as written posts, images, videos and audio files that are published on the social Web and are publicly available to a set of users or circle of friends, show some creative input, and are generated outside of professional routines and practices. *See* Marie-Francine Moens, et al., Mining User-Generated Content (CRC Press 2014).

[72]Charlie Osborne, "FTC Finalizes Charges Against Snapchat Over User Privacy," ZDNet.com, Jan. 2, 2015, *available at* www.zdnet.com/article/ftc-finalizes-charges-against-snapchat-over-user-privacy.

[73]Danielle Young, "Now You See It, Now You Don't … Or Do You?: Snapchat's Deceptive Promotion of Vanishing Messages Violates Federal Trade Commission Regulations," 30 J. Marshall J. Info. Tech.

and Privacy L. 827 (2014).
[74]News release, "FTC Approves Final Order Settling Charges Against Snapchat," Dec. 31, 2014, *available at* www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat.
[75]James Cook, "Hackers Access at Least 100,000 Snapchat Photos and Prepare To Leak Them, Including Underage Nude Pictures," Business Insider, Oct. 10, 2014, *available at* www.businessinsider.com/snapchat-hacked-the-snappening-2014-10#ixzz3VF9GdoiD.
[76]Eric Zeman, "Snapchat Lays Down the Law on Third-Party Apps," Programmable Web, April 7, 2015, *available at* www.programmableweb.com/news/snapchat-lays-down-law-third-party-apps/2015/04/07.
[77]WhatsApp.com, "Android: How Do I Restore My Messages?" *available at* www.whatsapp.com/faq/en/android/20887921 (last visited Sept. 2, 2015).
[78]Dave Stafford, "Texts Present Unique Challenges in Evidence Preservation and Admission," The Ind. Lawyer, Feb. 11, 2015, *at* 8-9, *available at* www.theindianalawyer.com/texts-present-unique-challenges-in-evidence-preservation-and-admission/PARAMS/article/36325.
[79]*Id.*
[80]*City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).
[81]"The Message Is the Medium: Messaging Services Are Rapidly Growing Beyond Online Chat," The Economist, March 28, 2015, *available at* www.economist.com/news/business/21647317-messaging-services-are-rapidly-growing-beyond-online-chat-message-medium.
[82]*Flagg v. City of Detroit*, 2008 WL 787061 (E.D. Mich. Mar. 20, 2008).
[83]Joo Y. Park, "Obtaining Stored Wire and Electronic Communications and Transactional Records Why Is It So Difficult? Helpful Tips on Getting It Done," High Swartz LLP, *available at* www.highswartz.com/blog/articles-white-papers/obtaining-stored-wire-electronic-communications-transactional-records-difficult-helpful-tips-getting-done (last accessed in 2015 but no longer available at the URL).
[84]*Finkle v. Howard Cnty., Md.*, No. SAG-13-3236, 2014 WL 6835628, (D. Md. Dec. 2, 2014).
[85]*Id.*
[86]Fed. R. Civ. P. 26(b)(1).
[87]*See* Ken Belson, "N.F.L. Upholds Tom Brady's Ban; Cellphone's Fate Helped Make the Call," N.Y. Times, July 28, 2015, *available at* www.nytimes.com/2015/07/29/sports/football/tom-bradys-four-game-suspension-is-upheld.html. Goodell's action was later vacated by U.S. District Judge Richard Berman due to violations of the players' collective bargaining agreement, per *National Football League Management Council v. National Football League Players Assn.,* Civil No. 15-5916 and 15-5982 (RMB/JCF) (S.D.N.Y., Sept. 3, 2015).
[88]E-Discovery Pilot Program, *supra* note 23, at 5.
[89]*See* Ganzenmuller, *supra* note 70, for a more in-depth discussion of the difference between "incidentally ephemeral" data, such as RAM, and "designedly ephemeral" data, such as Snapchat's "snaps."
[90]Decipher Forensics, "Snapchat Unveiled: An Examination of Snapchat on Android Devices," Jan. 23, 2014, www.decipherforensics.com/snapchat/
[91]Katie Notopoluos, "The Snapchat Feature That Will Ruin Your Life," BuzzFeed, Dec. 5, 2012, *available at* www.buzzfeed.com/katienotopoulos/the-snapchat-feature-that-will-ruin-your-life.
[92]YouTube video, "Proof Snapchat Doesn't Delete Your Photos/Videos After They Expire," posted by username "chromalux," May 17, 2013, *available at* www.youtube.com/watch?v=xPHsM9gXOnY.
[93]Molly McHugh, "Yes, You Can Recover Dead Snapchats — And Here's the Video Proof," Digital Trends, May 19, 2013, *available at* www.digitaltrends.com/social-media/yes-you-can-recover-dead-snapchats-and-heres-the-video-proof.
[94]Brendan Morgan, "Ensuring Admissibility of Mobile Evidence in Court," 62 The Fed. Lawyer 2, 66-69 (March 2015).
[95]*Id.*
[96]*Id.*
[97]*Sekisui v. Hart*, 945 F. Supp. 2d 494 (S.D.N.Y. 2013) (No. 12 Civ. 3479).
[98]*Polo-Calderon v. Corporacion Puertorriqueña de Salud*, No. 12-1006 (D.P.R. Jan. 16, 2014).
[99]*Small v. Univ. Med. Ctr. of S. Nev.*, No. 2:13-cv-00298-APG-PAL (D. Nev. Aug. 18, 2014) (report and recommendation and final findings of fact and conclusions of law of special master Daniel B. Garrie).
[100]*Id.*
[101]*Id.*
[102]*Id*.
[103]*Brady v. Grendene USA Inc.,* No. 12cv604-GPC (KSC) (S.D. Cal. July 24, 2015).
[104]*Moulton v. Bane,* Civil No. 14-cv-265-JD (D.N.H. Dec. 2, 2015).
[105]Steven Levy, "Snapchat's Non-Vanishing Message: You Can Trust Us," Medium, April 2, 2015, *available at* medium.com/backchannel/snapchat-s-non-vanishing-message-you-can-trust-us-6606e6774b8b.
[106]Thorin Klosowski, "How To Use All of Messages' New Features in iOS 8," Lifehacker, Sept. 17, 2014, *available at* lifehacker.com/how-to-use-all-of-messages-new-features-in-ios-8-1635030388.
[107]Margaret Littman, "What Everyone Is Wearing: Data From Wearable Devices Is Being Eyed as Evidence in the Courtroom," A.B.A. J., (April 2015), at 12.
[108]*See id.*
[109]*See* Jordan D. Maglich, *Major Changes Coming to the Rules of Civil Procedure.* 62 The Fed. Lawyer 2 37-45 (March 2015); *see also* K&L Gates, "Federal Rules Changes Affecting E-Discovery Are Almost Here—Are You Ready This Time? An Overview of the Rules, History, and Commentary," Oct. 1, 2015, *available at* www.ediscoverylaw.com/wp-content/uploads/2015/10/Rules-Amendment-Alert-100115.pdf.
[110]Fed. R. Civ. P. 37 Committee Notes on Rules—2015 Amendment, *available at* www.law.cornell.edu/rules/frcp/rule_37.
[111]Maglich, *supra* note 109, at 38.