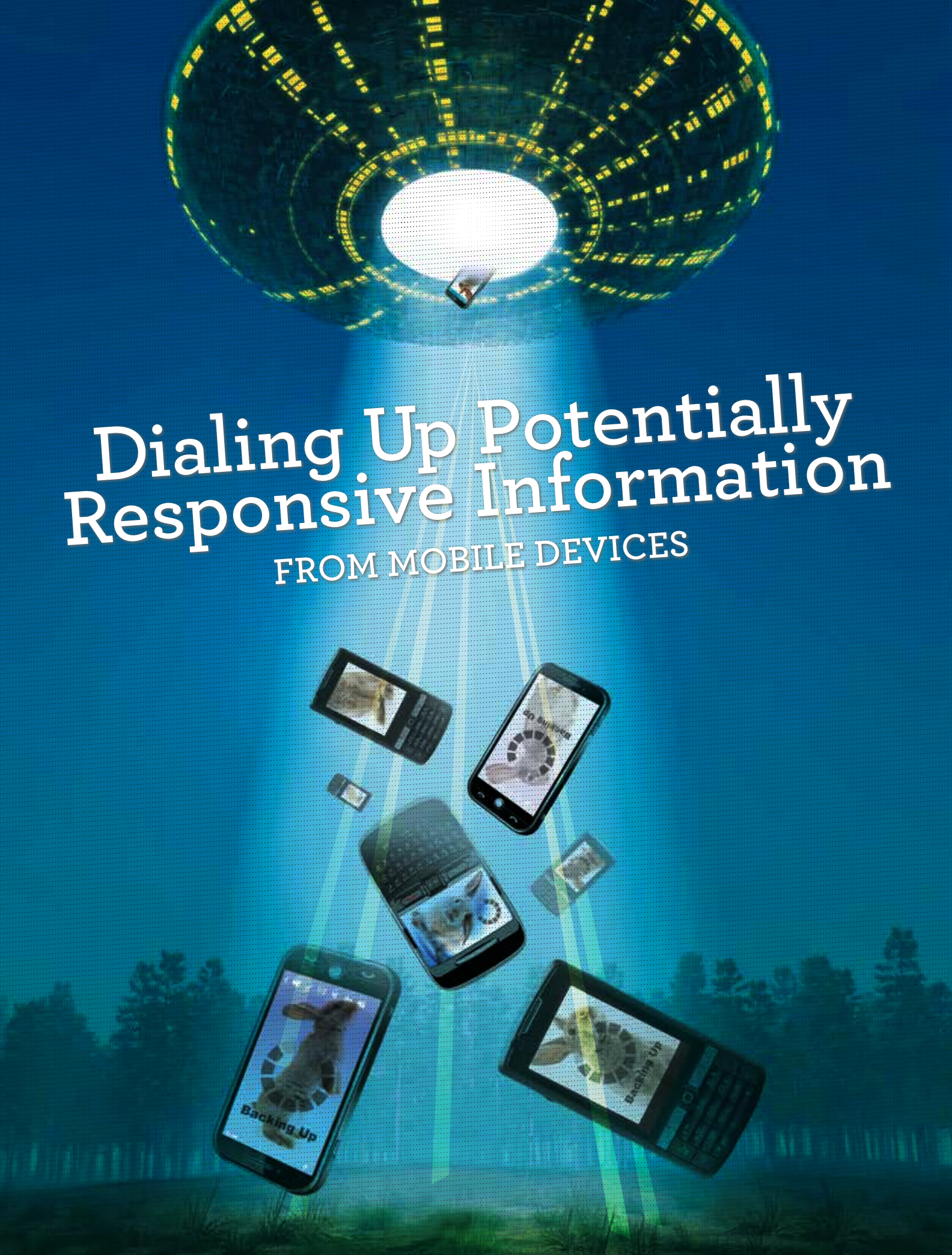

Dialing Up Potentially Responsive Information
FROM MOBILE DEVICES
Backing Up
Backing Up

While mobile device technology may still be novel and nascent, the discovery-related legal issues are not. Mobile devices and mobile device data are subject to the same discovery and evidentiary rules that apply to other electronically stored information (ESI). Just as courts sanction parties for failing to preserve other forms of ESI, some courts are sanctioning parties for failing to preserve mobile device data. Managing mobile device data during the discovery process can be challenging due to the number of custodians and devices, and the variation of relevant data on those devices over time. Unlike conventional computer data that tends to remain static over the course of litigation, mobile data evolves and grows.

30-SECOND SUMMARY

By Mark Michels and Emily Soverel

"The cell phone is the most quickly adopted consumer technology in the history of the world."[1] Not surprisingly, 90 percent of full-time American workers use their personal smartphones for work purposes[2] — a fact that presents multi-faceted challenges for corporate counsel. This is particularly apparent in the context of employment-related disputes, which often center on employees' communications. A growing number of the most relevant communications among affected employees in employment-related disputes will likely reside on mobile devices.

Mobile devices offer a wide array of communication tools, such as text messages, group chats, video chats, photos, status updates, "likes" and voicemails. Identifying, preserving and collecting these communication data is complicated by the fact that mobile devices run on a number of operating systems, which are often customized by the carrier or the user, and may or may not have the latest updates to the operating system. If the mobile device data are potentially relevant in the litigation, they are subject to the same legal treatment as other electronic data involved in the litigation. However, the vagaries and complexities of mobile device data require careful consideration by counsel in discovery planning. Counsel will be well served to have technical advisors with expertise in mobile device forensics assisting them in discovery and litigation planning.

The legal context

While mobile device technology may still be novel and nascent, the discovery-related legal issues are not. Mobile devices and mobile device data are subject to the same discovery and evidentiary rules that apply to other electronically stored information (ESI) and other "tangible things" in federal civil litigation. Mobile device data are no different from other data types. The Advisory Committee notes to Federal Rules of Civil Procedure state that ESI includes "information 'stored in any medium' to encompass further developments in computer technology … [and] is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments."[3]

Just as courts sanction parties for failing to preserve other forms of ESI, some courts are sanctioning parties for failing to preserve mobile device data. In *Calderon v. Corporacion Puertorrique a de Salud*, 2014 WL 171599 (D.P.R. Jan. 16, 2014), the plaintiffs filed suit alleging discrimination under Title VII. Defendants served a subpoena on one of the plaintiff's mobile carriers. In their review of the phone and text message logs provided by the carrier, defendants determined that the individual plaintiff had not produced all of the text messages from the relevant time period. Ultimately, the facts demonstrated that plaintiff selectively saved text messages and deleted others. The court concluded that, when the plaintiff deleted the text messages, the plaintiff foresaw litigation and thus had a duty to preserve the text messages, and spoliation occurred. The court concluded that an adverse inference was the most appropriate sanction. The adverse inference would provide generally that "a trier of fact may (but need not) infer from a party's obliteration of a document relevant to the litigated issue that the contents of the document were unfavorable to the party."[4] See also, *Christou v. Beatport, LLC*, 2013 U.S. Dist. LEXIS 9034 (D. Colo. Jan. 23, 2013) (Defendant's failure to preserve mobile phone text messages was negligent, and spoliation sanctions were appropriate.).

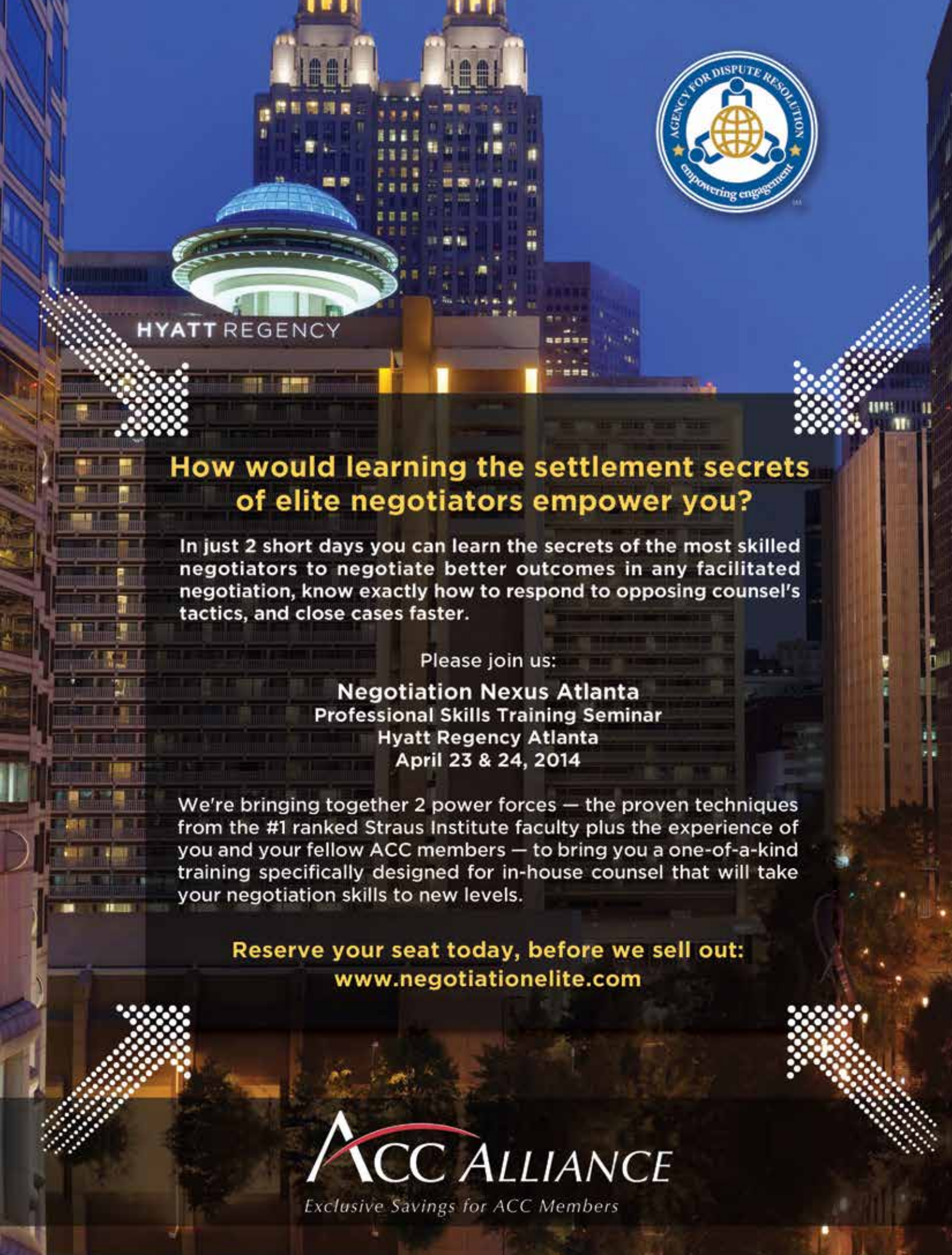
Preservation must be thought about in the context of proportionality; this is as true for mobile devices as it is for other discovery data. Failing to preserve may not result in sanctions if there is a proportionality argument to be made. *The Sedona Conference Commentary on Proportionality in Electronic Discovery* (January 2013) traces the development of the "proportionality" principle in the Federal Rules of Civil Procedure, culminating in the current version of Rule 26(c)(1), which permits a party to resist discovery if the cost of obtaining the data outweighs the benefit of the data in the specific matter. In the case of *PTSI, Inc. v. Haley*, 2013 PA Super 130 (Pa. Super. Ct. 2013), the defendants routinely deleted text messages "so as not to unduly encumber" their smartphones.[5] They did this due to the volume of text messages and the limited storage capabilities of their smartphones. "[I]t would be very difficult, if not impossible, to save all text messages and to continue to use the phone for messaging."[6] "[T]he obligation to preserve electronic data and documents requires reasonable and good faith efforts … [but] it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data."[7]

The producing party in *PTSI* convinced the court that the monetary cost of preserving the text messages outweighed the benefit of producing them in the matter. However, defendants in employment-related cases may face non-monetary factors in the court's cost-benefit balancing, notably, the public interest. The Federal Rules of Civil Procedure Advisory Committee stated that "Rule 26(b)(2)(C)(iii) recognizes that many cases in

Mark Michels is a director in the Discovery practice of Deloitte Financial Advisory Services LLP. As a former in-house counsel, Michels specializes in advising on electronic discovery management related to complex litigation, patent litigation, class actions, commercial disputes, pre-merger reviews and internal investigations. *mmichels@deloitte.com*

Emily Soverel is a Discovery staff attorney at Google. As case specialist, she leads ediscovery matters from collections to production. She also serves as a tech POC for the Google team and helps colleagues troubleshoot difficulties and challenges with the ediscovery platforms. *soverel@gmail.com*

The authors would like to thank John Medeiros and Brian Rydstrom from Deloitte for their considerable contributions to this article.



How would learning the settlement secrets of elite negotiators empower you?

In just 2 short days you can learn the secrets of the most skilled negotiators to negotiate better outcomes in any facilitated negotiation, know exactly how to respond to opposing counsel's tactics, and close cases faster.

Please join us:

Negotiation Nexus Atlanta
Professional Skills Training Seminar
Hyatt Regency Atlanta
April 23 & 24, 2014

We're bringing together 2 power forces — the proven techniques from the #1 ranked Straus Institute faculty plus the experience of you and your fellow ACC members — to bring you a one-of-a-kind training specifically designed for in-house counsel that will take your negotiation skills to new levels.

Reserve your seat today, before we sell out:
www.negotiationelite.com

ACC ALLIANCE
Exclusive Savings for ACC Members

Mobile data types

UNFAMILIAR MOBILE DATA TYPES MAY INCLUDE:

- Call logs: a history, with dates and times, of calls made, received and missed
- Chat: a generic name for SMS and MMS type communications, often referring to messaging via third-party applications
- Contacts: the phonebook on the device, which may contain photographs, URLs, email addresses, date of birth and other information, in addition to phone numbers and addresses
- Device information: information about the device, including make, model, serial number, IMEI or other communications information
- Device settings: all of the user configurable settings, including time zone, language, Roll Off settings, Do Not Disturb, etc.
- Device voicemail: voice mail recordings
- Locations: refers to both operating system captured geolocation data, such as Access Points, as well as coordinates embedded in photographs, such as longitude, latitude and altitude found in mobile device camera files
- Memory card content: removable storage memory modules that operate similar to an external hard drive and may contain photographs, movies, music, sound recordings, text messages, files, etc.
- Multi-media messaging system (MMS): a protocol that facilitates the inclusion of an attachment with a text message, allowing the text message to exceed 160 characters
- Short message system (SMS): commonly referred to as a text message and is limited to 160 characters of text
- Tasks: a type of calendar entry, also referred to as a "to-do" list, but is linked to a date and time

public policy spheres, such as employment practices, free speech, and other matters, may have importance far beyond the monetary amount involved."[8]

In discovery planning, in-house counsel are faced with applying preservation, production and evidentiary principles in a mobile device environment that is substantially different than the typical personal computer and enterprise data environment. However, the same concepts of reasonableness and proportionality that apply in traditional discovery also apply to mobile device data discovery.

Mobile device litigation hold and preservation

At first blush, preserving mobile device data raises exactly the same issues as preserving other forms of ESI. Counsel typically asks: In this particular case, will an instruction to the employees suffice? Alternatively, does collecting the device from the employee make the most sense under those particular circumstances? Is the right approach to collect the data off the device and preserve it now? Counsel's answers to these questions often differ under the specific case circumstances and may even change during the course of the matter.

A threshold level of inquiry in discovery planning is to determine whether the corporation has "possession, custody or control" of the device, the data or both. This inquiry may be more complicated when an employee's personal device contains both personal and corporate data. The specific nuances of this issue are beyond the scope of this article; however, this issue must be addressed by counsel under the specific circumstances of the matter. Assuming that the company determines the device is within its possession, custody or control, it may be obligated to issue a litigation hold if relevant data are determined to reside on the mobile device.

Developing the preservation strategy requires counsel to understand where potentially responsive data are stored. There may be data types that only exist on the mobile device, including certain application data, draft messages and draft emails. As is true with other devices, the corporate IT organization may have information, such as billing records, logs and purchase records, from which counsel may determine whether custodians have mobile devices. However, these sources are often insufficient, and counsel may need to develop questionnaires and conduct interviews with each custodian to ensure an understanding of the number of devices and the potential storage locations of the desired data types associated with the mobile device.

Relying exclusively on employees to preserve mobile device data, especially because of the dynamic nature of the data, requires considerable oversight to ensure that they preserve the required data. Some even maintain that relying on employees to preserve the data is problematic. "[M]any commentators have reported strong judicial disapproval of 'self-collection' and have concluded … that the approach is simply far too dangerous for most enterprises, except perhaps those that are extremely risk tolerant."[9]

Assuming that the company determines the device is within its possession, custody or control, it may be obligated to issue a litigation hold if relevant data are determined to reside on the mobile device.

Due to these constant changes, the methods used to image and interpret data from a specific phone may not be possible at the time of release or even for a time after the initial release.

If counsel's preservation strategy is to take physical custody of the device, it is important to maintain proper chain-of-custody practices so that the device can be tracked back to the individual. In one instance, a company instructed employees who had just been laid off to place their phones in a box as they exited the building. Litigation over this layoff or reduction in force (RIF) then ensued, and the poorly collected phones presented a host of problems when provided to the forensics team for processing. Many of the devices required a password or specific chargers that were not collected during the RIF. This hindered, and in some cases even prevented, the data collection from some of these devices. The lesson here is that when collecting the mobile devices, parties must ensure that the devices can be linked to their owner later in the litigation. Furthermore, collecting passwords and chargers are examples of two other actions counsel should take when the preservation strategy is to collect and hold the device.

If counsel choose to collect mobile device data as a preservation strategy, then counsel must address mobile device data collection complexities in their planning. For example, if counsel decides that the circumstances of the case require preserving the data directly from the mobile device, the tools currently available typically preserve all data of each type selected, as there is currently no cost effective way to preserve only selected data types on a mobile device. This potential over-collection can be very costly and may result in collecting personal employee data, creating potential privacy concerns among employees.

As with all discovery preservation issues, counsel ought to be mindful of proportionality issues and determine whether the mobile device data are duplicative of other data, and whether the duplicative data are more accessible elsewhere (e.g., on a computer backup or server backup). If counsel can determine that the mobile device data themselves are redundant, that information may factor into the preservation calculus. In crafting a preservation strategy, counsel should discuss their specific requirements with experts on their team who have requisite technical knowledge to determine the most effective and efficient method of preserving mobile device data.

Mobile device collection

Mobile device data collection and the associated forensics are evolving rapidly. Maintaining data collection quality and efficiency is one significant challenge that sets mobile device forensics apart from personal computer forensics. Unlike traditional personal computer forensics, mobile device forensics must not only address the changes in capacity, but also a plethora of changing configurations that lack industry standards and a short development cycle for updated operating systems. Many devices use customized or proprietary mobile variations of the original operating systems, resulting in added complexity when compared to the traditional operating system used on a computer.

There are thousands of different mobile devices, each of which may have a slightly different operating system. Additionally, there are new mobile devices and operating systems released to the marketplace on a weekly or monthly basis. Many of the manufacturers do not release the technical details and specifications of the operating systems or new devices to the mobile vendors prior to the public release of the device. Despite the mobile forensic tool developers' best efforts, they are still forced to play "catch-up" to identify a forensic method for extraction of these new devices and operating systems. Due to these constant changes, the methods used to image and interpret data from a specific phone may not be possible at the time of release or even for a time after the initial release.

The leading industry standard mobile forensics tools have the ability to create their own images or use the backup file created by the mobile

Glossary of mobile device terminology

- Access Points: refers to Wi-Fi routers through which a device may connect to the internet
- Chat: a common term encompassing multiple messaging standards
- International mobile equipment identifier (IMEI): a unique number used as part of the identification of a mobile device on a cellular network
- Locations: refers to both operating system captured geolocation data, such as Access Points, as well as coordinates embedded in photographs, such as longitude, latitude and altitude found in mobile device camera files
- Multimedia messaging service (MMS): a protocol that provides for transmission of messages of greater length than SMS, as well as the ability to transmit an attachment
- Short message service (SMS): a protocol that provides for transmission of text messages up to 160 characters
- Wi-Fi: refers to the IEEE standard for wireless communication under section 802.11

ACC EXTRAS ON… Mobile device data

ACC Docket
New Technology, New Traps — How Advancing Technology Advances Litigation (Apr. 2010). *www.acc.com/docket/tech-lit_apr10*

Top Tens
B-Y-OMG: Top Ten Considerations When Creating a Bring-Your-Own-Device (BYOD) Company Policy (Oct. 2013). *www.acc.com/topten/byod_oct13*

Top Ten BYOD Policy Concerns (Jan. 2014). www.acc.com/topten/byod_jan14 *http://www.acc.com/legalresources/publications/topten/ttbyod.cfm*

Presentation
Your Mobile Workforce — What You Should Know About BYOD and COPE (Oct. 2013). *www.acc.com/mobile-workforce_oct13*

InfoPAKs℠
Cloud-Based vs. On-Premise eDiscovery and Information Governance Under US and EU Law (Aug. 2011). *www.acc.com/infopaks/cloud-ediscovery_aug11*

Workplace Information Risk in the Digital Age: Monitoring Employees, Social Media Challenges, Managing Access to Data and Optimizing Flexibility (Jan. 2011). *www.acc.com/infopaks/info-risk_jan11*

Practice Resource
If you need additional expert consultation on your discovery-related challenges, ACC Alliance partner Modus eDiscovery is ready to help. Modus assesses organizations' litigation readiness, applies best practices and provides business intelligence throughout the entire discovery process to help organizations monitor and control costs. Find out more at *www.acc.com/alliance*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

device's backup utility to extract active (or logical) and previously deleted (recovered) data that would have once resided on the mobile device. It may be necessary to use multiple tools or even perform multiple preservations in order to obtain all possible information from a mobile device. In some cases, the only option is to manually preserve data through static screenshots or video. This is heavily dependent on the specific make and model, the version of the operating system, and the potential acquisition method.

Traditionally, forensically collecting mobile device data was the only option due to the complexity of the devices, the variables of collection and the diverse data types to be handled. This may no longer be true in certain enterprises, which may now have a range of other collection options available. Mobile device management (MDM) collections and corporate application data repositories may account for a part of the solution, which may significantly lower litigation costs. Many of the device types and MDM utilities allow for data backup from the device and even to a remote repository. However, these backups are not the equivalent of a physical image from a traditional hard drive and do not encompass all available data. Therefore, these may not be adequate in the particular litigation at issue.

Due to the lack of standards, the ability to collect all potentially relevant data from a mobile device may not always be possible due to the proprietary operating systems, varying interfaces and ever-changing landscape, including the release of new applications that may store data differently in each operating system. In addition, the techniques used to collect all data may be very time consuming and could potentially be considered "unreasonable." It is critical to identify the data that needs to be preserved and the methods that need to be employed. There are a number of factors in determining the image and collection method that is appropriate for a specific matter. The main factor is to preserve all data while considering and weighing the risk factors with the benefits. Counsel's collection planning is yet another area where counsel should consult with mobile device forensics experts to understand the specific data collection issues involved in the specific case.

Mobile device processing, review and production

One challenge counsel face when processing mobile data is extracting data from the device in a way that enables review in a manner consistent with other data. Loading mobile data into the review platforms, while preserving associated metadata, enables the data to be handled as single unique items, providing for improved review, searching, privilege management and production. For example, an investigation timeline consisting of multiple data types (i.e., emails, documents, text messages, etc.) is easier to construct and potentially richer when all data are organized in one location in a consistent form. Most mobile forensic tools generally lack the ability to extract this data into a generic format that can be loaded into the majority of discovery review tools. Some service providers have solutions designed to normalize mobile phone data so that it can be concurrently reviewed.

Another challenge to mobile device data review is normalizing dates and times. Not only do text messages have the same challenges as email — requiring the conversion of all messages to a common time zone to correctly display threads of messages across custodians — but mobile device text message times may also differ significantly between the sending device and the receiving device. The providers handle text messages as a "store and forward" service. When sent, the message receives a timestamp on the sending device based on the time currently held by the device. However, since these are "store and forward" messages, they are stamped with the server time on the receiving device when delivered. This can be additionally complicated

because mobile devices may be out of contact with the provider's text messaging server for extended periods of time, such as when the custodian is on an aircraft. Unlike emails, which have extensive headers that contain dates and times of each mail server processing the message, no similar record is included with text messages.

Here again, counsel's planning should consider how mobile device data are to be managed for investigations, review and production.

Challenging but manageable

Essential to any discovery matter or investigation is the involvement of all parties in advance planning, including management, legal and technical personnel. Managing mobile device data during the discovery process can be challenging due to the number of custodians, the number of devices, the variation of relevant data on those devices over time and the variations of data among devices. In discovery planning, counsel's communications with key personnel is critical. Once the data types of interest and their potential locations are mapped, counsel, working with their mobile forensics experts, should develop a preservation strategy that is consistent with the needs of the litigation. Counsel must work closely with the team that controls the corporate MDM solution to identify devices, corporate applications and data types that may be responsive in the litigation. Unlike conventional computer data types that tend to remain static over the course of the litigation, mobile data types continue to evolve and grow, requiring repeated touch points over time to ensure a complete understanding of both the data to be collected and the potential locations from which to preserve that data. **ACC**

NOTES

1 *www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.*
2 *www.structuredweb.com/sw/swchannel/CustomerCenter/documents/8523/22089/Cisco_mCon_BYOD_Insights_2013.pdf.*
3 Fed. R. Civ. p. 34 Advisory Committee notes (2006 Amendment).
4 *Calderon* at 5.
5 *PTSI, Inc. v. Haley*, 2013 PA Super 130 (Pa. Super. Ct. 2013).
6 Id.
7 The Sedona Conference, "The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production" (2005).
8 Fed. R. Civ. p. 26 Advisory Committee note (1983 Amendment).
9 Jeffrey C. Sharer, Colleen M. Kenney & Sheila A.G. Armbrust, "*Taming the Fox in the Henhouse: Defensible "Self-Collection" in E-Discovery," The Computer & Internet Law*, Vol. 30, No. 3 (March 2013).