Bloomberg BNA

Digital Discovery & e-Evidence®

TEXT MESSAGES

The authors explain why companies and their counsel must understand the unique challenges that the preservation and discovery of text messages pose compared to more traditional data sources, such as e-mail.

The Coming Storm: Companies Must Be Prepared to Deal With Text Messages on Employee Mobile Devices

BY GARETH EVANS AND VEERAL GOSALIA

Text messages have been playing an increasingly important role in high profile controversies. From the recent firing of police officers in San Francisco and the release of a senior executive at a large corporation for allegedly inappropriate text messages, to a defamation lawsuit in Hampton, New Jersey and other notable cases at universities and government offices, we are beginning to see text messages more frequently cited as evidence of wrongdoing.

It is now more important than ever that companies understand the challenges (and costs) involved in extracting text messages from mobile devices. It is also important that companies proactively manage text messaging data to reduce the risks of exploding litigation costs and spoliation sanctions that arise from the increasingly common use of text messaging for business purposes.

Text Messages as a Source of Evidence

In many respects, this new reliance on text messages as evidence is reminiscent of the early days of e-mail. In the early to mid-1990s, e-mail was a relatively new and informal means of communicating in business. That informality occasionally led to trouble, with e-mails often cited as key evidence in harassment and discrimination cases.

Over the past two and a half decades, etiquette in business e-mails has generally improved, along with a greater understanding by users that their e-mails on company accounts are accessible to IT and other personnel and are readily discoverable in litigation and investigations.

What Are Text Messages? Enter text messaging and its often highly casual banter. Text messages are often thought of in the form of Short Message Service (or

Gareth Evans is a litigation partner at Gibson, Dunn & Crutcher LLP, with 25 years of experience at the firm. His career has focused on complex business litigation, governmental investigations and data security, and has included matters in many different subject matter areas. He is co-chair of Gibson Dunn's Electronic Discovery and Information Governance Practice Group.

Veeral Gosalia is a senior managing director in the FTI Technology segment, where his areas of expertise include data preservation, data analysis, computer forensics and eDiscovery. He has assisted attorneys and corporations in understanding the issues surrounding electronic evidence—including the acquisition, analysis and production of data.

 ISSN 1941-3882

SMS) messages, which are limited to 160 characters and are sent across the mobile telephone communications network.

The term ''text message'' is also increasingly used to refer to messages sent across the Internet using instant messaging applications on mobile computing and phone devices. Examples include Apple iMessage, WhatsApp, BlackBerry Messenger, Snapchat, and Facebook Messenger.

As a medium, text messaging may encourage users to let their guard (and internal filters) down because of its direct mobile device-to-mobile device nature. As Internet-based text messaging does not go through a company server, and phone carriers usually retain SMS messages for only a few days, users may incorrectly assume that their text messages are ''off the radar.'' Many may also believe that text messages are more ephemeral than email and permanently removed once deleted in their messaging app. Text messaging apps often store messages in databases on the device, however, and ''deleted'' messages can sometimes still be extracted.

The Challenges. When viewed as a potential source of evidence, text messaging can pose significant challenges compared to e-mail. It can be difficult and very expensive to extract and collect text messages from mobile devices. E-mails can usually be obtained readily from company servers and archives, most often do not require extraction from the user's device and, if necessary, extraction is usually straightforward.

Text messages, by contrast, may require collecting the device from the employee—which can be challenging and can pose delicate privacy issues—as well as expensive forensic work, even for messages that have not been ''deleted.''

Additionally, when text messages do not go through company-managed enterprise servers or do not have any enterprise-based controls, companies may not be able to enforce records retention and legal hold policies for technical or logistical reasons.

Text messages may require collecting the device from the employee—which can be challenging and can pose delicate privacy issues—as well as expensive forensic work.

Lack of Preparation. Most companies are not prepared for the possibility that they may be required to preserve, extract and search text messages from their employees' mobile devices in litigation or an investigation. That possibility appears to be increasing.

A RingCentral survey[1] of more than 1,000 working adults in North America found that 79 percent of respondents use text messaging for business communications and, of those, 82 percent stated that they text more for business now than they did in the previous year. Separately, 32 percent claimed that they have closed a business deal via text message.

To the extent that senior company officers and executives, whose activities are at the highest risk of coming under the microscope in litigation or an investigation, may be using text messaging in this manner, this is a matter of even greater concern. Moreover, courts and governmental investigators may not appreciate the difficulties and costs of extracting text messages from mobile devices.

Emergence of Case Law

Not surprisingly, the courts have begun to grapple with the discovery of text messages.

Riley. The United States Supreme Court's landmark decision last year in *Riley v. California*[2] highlighted both the importance of mobile devices as a source of potentially relevant information—such as text messages—and the privacy interests that can be involved in discovery of the information from such devices. In *Riley*, the Court unanimously held that the Fourth Amendment generally requires law enforcement to obtain a warrant before reviewing digital information that is stored on a smart phone seized incident to arrest. Significantly, the Court observed that modern cell phones have the capacity to store ''millions of pages of text, thousands of pictures or hundreds of videos'' and thus ''implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.'' The privacy interests at issue in *Riley* highlight one of the challenges of dealing with mobile devices, whether individual- or company-owned, as they will likely contain both business-related and personal information.

Pradaxa. Because mobile devices hold such an immense volume of information, it is not surprising that data on such devices have become the subject of sanctions decisions regarding alleged failures to preserve relevant information. In 2014, the Seventh Circuit upheld sanctions imposed in *In re Pradaxa*.[3] The court held that the defendant had a duty to suspend an auto-delete function that operated on potentially relevant text messages. It imposed nearly $1 million in punitive sanctions for the defendant's failure to preserve the text messages, among other things. The court found that the plaintiffs, through their definition of ''document'' in their requests for production, had requested the text messages.

Calderon. In yet another recent example, *Calderon v. Corporacion Puertorrique de Salud*,[4] an employment discrimination case, the court held that an adverse inference instruction against the plaintiff was appropriate where the plaintiff had only selectively preserved relevant text messages between himself and a third-party. The court found that the plaintiff's failure to preserve more than 38 other text messages prejudiced the defendants by precluding a complete review of potentially

[1] RingCentral survey to 1,107 adults in North America conducted via social media (Facebook, LinkedIn, Twitter); Dec. 3 – 6, 2012

[2] *Riley v. California*, 134 S. Ct. 2473 (2014)

[3] *In re Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig.*, MDL No. 22385, 2013 BL 347278 (S.D. Ill. Dec. 9, 2013), aff'd, 745 F.3d 216, 218 (7th Cir. 2014)

[4] *Calderon v. Corporacion Puertorrique de Salud*, 992 F. Supp. 2d 48, 52-53 (D.P.R. 2014)

  DDEE ISSN 1941-3882

relevant conversations and pictures sent via text messages. The court viewed the plaintiff's actions as a ''conscious abandonment of potentially useful evidence,'' indicating that ''he believed those records would not help his side of the case.''

Hosch. Additionally, in *Hosch v. BAE Systems Information Solutions, Inc.*,[5] the district judge adopted the magistrate judge's findings that the plaintiff had engaged in a series of intentional and bad faith discovery violations, including the permanent deletion of all text messages and voicemails, by wiping his iPhone just two days before turning it over to counsel. The court dismissed the plaintiff's action with prejudice and awarded the defendant attorney's fees and costs incurred in bringing motions to compel and a motion for sanctions.

Technical Issues

The cases discussed above demonstrate that courts consider text messages to be subject to discovery. Increasingly, governmental and internal investigations also focus on examining text messages. It's important that companies and their counsel understand that the preservation and discovery of text messages poses unique challenges compared to more traditional data sources such as e-mail.

Technical Diversity and Rapid Innovation. The first issue to contend with is the technical diversity and rapid pace of innovation in the mobile device marketplace. The process for collecting data from a mobile device typically involves the use of forensic software to extract data from the device.

Unfortunately, there is no ''one size fits all'' forensic software. Rather, the forensic software generally has to be tailored to the specific device, including the various iterations of devices (*e.g.*, iPhone 5 versus iPhone 6), and the specific operating system used on the device.

While a company may have general uniformity in the computers provided to employees, and may also use a single enterprise-wide e-mail platform, the mobile devices employees use can vary significantly. This is especially true if a company has a Bring Your Own Device (or ''BYOD'') policy permitting employees to use the device of their choice.

If you consider the vast number of different makes, models and versions of mobile devices, operating systems, and carriers in the marketplace, these different combinations can make predicting what type of device one might expect to encounter for forensic extraction rather difficult.

Further, the pace at which new mobile device models are released is only surpassed by that of the pace at which operating systems are updated. These variations in mobile device hardware and software make it difficult for the forensic software to keep pace for support. Certain forensic software has better success with certain devices than others, requiring frequent monitoring of the latest technologies available for this purpose.

Security and Encryption. Data security and encryption also pose significant challenges to extracting data—including text messages—from mobile devices. With data security and breaches often in the headlines, it's not surprising that mobile device manufacturers are increasingly including data encryption and security capabilities in their products. In fact, manufacturers often tout the strength of the security features on their devices and their ability to prevent data access.

While there are methods to bypass data security on mobile devices, the success rate is largely dependent upon the make and model of the device, the version of the operating system, and whether the device has been ''jail broken'' or ''rooted'' (i.e., where the user has altered the operating system to bypass certain restrictions on the device's functionality). The simplest way to bypass mobile device security is through the user's cooperation in disabling encryption or ''unlocking'' the device so that the forensic software can access the contents.

Plan to Control Text Messaging Risks

1) Include mobile device usage as part of the corporation's IT usage policies, including a BYOD policy if employees are permitted to use personal devices. This should state the company's position on the use of text messages for business purposes and the company's potential need to collect text messages from the device.

2) Educate employees regarding appropriate text messaging usage, including that text messaging is subject to discovery in litigation and investigations.

3) Educate employees on litigation hold to understand that their text messages are subject to the same hold requirements as other documents.

4) Rather than permitting employees to use a mobile IM messaging system of their choice, offer a specific service that allows for logging and central collection.

5) Consider the use of ''sandboxes'' or separate spaces for work and personal app usage on mobile devices. Products are now available that enforce separation between personal and work data, which can help address privacy concerns when collecting data from mobile devices.

6) Partner with IT to utilize Mobile Device Management (''MDM'') software to help monitor and track mobile device usage, including information regarding the make/model, operating system, and other information related to mobile device usage in the enterprise.

7) Ensure your data collection teams or vendors are fully equipped to handle mobile devices and have the appropriate resources available to successfully extract text messages from the mobile devices in use at the company.

[5] *Hosch v. BAE Systems Information Solutions, Inc.*, No. 1:13-cv-00825 (AJT/TCP), 2014 BL 114226 at *2 (E.D. Va. Apr. 24, 2014)

Battening Down the Hatches

Ultimately, getting ahead of the litigation risks imposed by text messaging starts with proactive management integrated into the company's information governance strategy. With text messaging, companies are dealing with a situation where business communications may be taking place without company control over how long messages are retained, or whether they are retained at all, posing risks for records retention (both under- and over-retention) and legal holds.

Legal and IT teams need to ensure that employees are not retaining communications for longer or shorter than provided by company policy and, very importantly, that employees on legal hold are retaining messages subject to the hold. In the end, this is an information governance issue—and it's an important one.

Unfortunately, most information governance projects never get off the ground, despite the fact that they are driven by acutely felt pain points. Many information governance projects take time for benefits to materialize, and may not offer immediate rewards that can discourage adoption.

Legal departments have the opportunity to play a critical role in this process, however, and should understand that it should address both issues of broad scope (e.g., general records retention and defensible deletion) and more specific issues such as text messaging.

Working with key stakeholders to develop policies, educational and enforcement programs, and to implement appropriate technologies, is a critical step in reigning in employee communications—including texting—and protecting the company against risk.

Very soon, demands for the search of employee text messages will likely be common in litigation and investigations. Developing a well-thought out plan and implementing appropriate technology before the coming storm can save companies from being faced with enormous litigation expenses and potentially disastrous sanctions arising out of executive and employee text messaging.

  DDEE ISSN 1941-3882