TEXT MESSAGES IN eDISCOVERY: RECOVERY, RETENTION AND PRESERVATION

As mobile device usage and capabilities increase, the importance of these gadgets as potential sources of electronically stored information (ESI) becomes undeniable. The more we rely on these accessories as vehicles for business communications and entertainment, the more data we create and consume. For every additional bit and byte that is born in the ether, there is a heightened chance that the information will become fodder for electronic discovery (eDiscovery).

powered by people D4

As mobile device usage and capabilities increase, the importance of the ever-slimmer gadgets as potential sources of electronically stored information (ESI) becomes undeniable. The more we rely on these accessories as vehicles for business communications and entertainment, the more data we create and consume. For every additional bit and byte that is born in the ether, there is a heightened chance that the information will become fodder for electronic discovery (eDiscovery). Despite this increasingly large amount of information, marooned mobile device data can provide a number of unique hurdles throughout the litigation lifecycle. Every step could potentially expose variables and scenarios that challenge even the most experienced eDiscovery counsel and technicians. The challenge is amplified by the sheer number of different device models available in today's competitive, lucrative, and growing mobile communication market. Each device, from pocket-sized mobile phones to tablets that range from the size of a paperback thriller to a traditional manila folder, can foster its own unique snowflake of devilish eDiscovery complications.

For law firms and corporations, the challenge is not to understand the technical architecture of each and every device, but rather how the devices utilized by your custodians generate and manage data. Once an organization maps an inventory of its own unique portfolio of cell phones and tablets, a consistent and repeatable process should be instituted in order to ensure data is properly identified, preserved, and considered for use in internal investigations, regulatory and law enforcement scenarios, and eDiscovery proceedings. Thankfully, enterprise technology usage policies and data retention schemes are more ubiquitous today than in years past, and the approach to information governance should be no different with mobile devices. In the same way that email evolved from a convenient way to conduct a conversation without involving the US Postal Service or a telephone, SMS messaging has become a more widely accepted and legitimate mode of communication for businesspeople and teenagers alike.

Early efforts at preserving and producing SMS messages from flip phones and Blackberries were commonly avoided through a facade of undue burden and cost. However, as mobile technology becomes cheaper, more ubiquitous, and even wearable, litigants who unilaterally determine that these short communications are inaccessible do so at their own peril. It's common knowledge that the best offense is a great defense, and

the same applies to governance of mobile communications. This guide will help you engineer proactive policies and preservations plans around SMS messaging, one of today's most popular ways to communicate.

Mobile Device Usage is Not a Fad

The continuing trend of growing mobile device usage is no secret and the metrics clearly support the essentially universal adoption we associate with traditional land-line telephones. In 2011, only 17% of the global population did not own at least a basic mobile phone; by 2013 the "off the grid" population fell to 9%. Furthermore, during the same period of time, the adoption of smartphones, which have features resembling a personal computer such as e-mail connectivity, digital cameras, and GPS location functionality, jumped from 35% in 2011 to 56% in 2013[1]. 2013 marked the first year where over half of the world's population owned a smartphone, a development that shows no sign of illness. By 2020, the total number of smartphone subscriptions is expected to reach an astonishing 6.1 billion.[2]

Combine email with SMS messaging and it becomes clear that mobile phones and tablets are thorny ESI caches that organizations need to be aware of in the event of litigation.

It should be no surprise that an increase in smartphone proliferation has led to a fundamental change in how people access and interact with their data and each other. A hearty 33.4% of

1. http://www.digitalbuzzblog.com/infographic-2013-mobile-growth-statistics/

2. http://techcrunch.com/2015/06/02/6-1b-smartphone-users-globally-by-2020-overtaking-basic-fixed-phone-subscriptions/

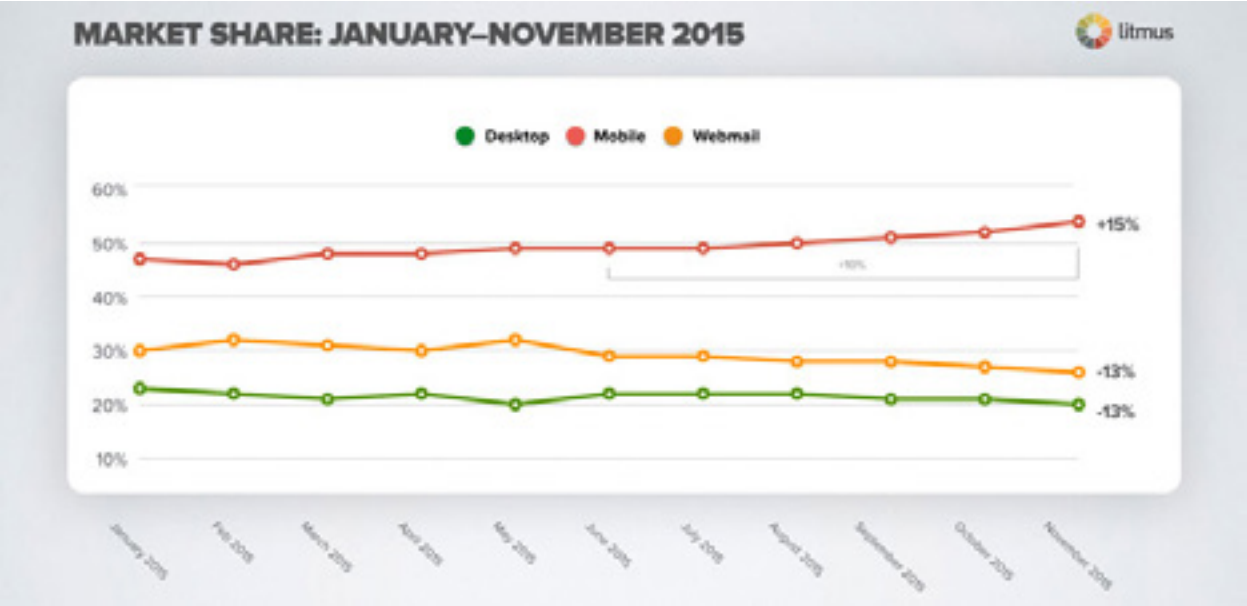

Figure 1

global web usage in 2015 came from mobile sources, up from 28.9% in 2014. [3] It would certainly not be a leap of faith to suggest that metric will continue to evolve as the global population continues its insatiable demand for smartphones and the always-connected lifestyle.

All of these trends provide an important bellwether for eDiscovery, which should closely trace the increase in mobile device usage to a corresponding increase in ESI generated from mobile sources. More business meetings and routine correspondence are being conducted on the go, the nearly permanent records of which are potentially relevant to any number of litigation scenarios. 54% of users open emails from their mobile devices, up from just 10% in 2011. That trend comes at the expense of email viewing on desktop computers, which is down from 58% in 2011 to only 22%[4]. (Figure 1)

Combine email with SMS messaging and it becomes clear that mobile phones and tablets are thorny ESI caches that organizations need to be aware of in the event of litigation. 92% of US smartphone owners use SMS messaging, and those users send an average of 111 messages per week. Corporations need to understand how these messages and emails are stored in order to institute appropriate usage, retention, and incident response policies.

Data Retention Issues and Recent Case Law

Recent judicial experiences are littered with Recent judicial experiences are littered with examples of litigants grappling with issues of mobile device preservation. For example, while allowing discovery of class members' social media, text messages, and email in *EEOC v. The Original Honey Baked Ham Company of Georgia Inc. (Feb. 27, 2013)*, Magistrate Judge Michael E. Hegarty opined that "If there are documents in this folder that contain information that is relevant or may lead to the discovery of admissible evidence relating to this lawsuit, the presumption is that it should be produced. The fact that it exists in cyberspace on an electronic device is a logistical and, perhaps, financial problem, but not a circumstance that removes the information from accessibility by a party opponent in litigation." It is clear that arguments around inaccessibility, burden, and even privacy will fall on deaf ears when it comes to preservation and collection of relevant ESI no matter where it resides.

Garcia v. City of Laredo (Dec. 12, 2012) saw The United States Court of Appeals for the Fifth Circuit confirm the Texas district court's opinion that mobile phones do not fall under the protections afforded by the Stored Communications Act (SCA) of 1986.

3. http://www.statista.com/statistics/241462/global-mobile-phone-website-traffic-share/

4. http://www.emailmonday.com/mobile-email-usage-statistics#growth

The SCA sought to extend fourth amendment rights to information carriers such as Internet Service Providers (ISPs) to protect them against unreasonable search and seizure. Plaintiff unsuccessfully argued that the City of Laredo violated the SCA by accessing information stored on her mobile phone without her permission. Circuit Judge W. Eugene Davis concluded that a mobile phone is not a *facility* through which an electronic communication service is provided and that only "electronic storage" that is provided by an electronic communication service is within the scope of the SCA. In other words, data stored on the physical device itself is not protected, but data hosted by or in transit through a communication provider such as Verizon or AT&T falls under the SCA's scope.

Prior to enacting a mobile device management policy, an organization must know exactly what devices it has, or will have, in order to better understand the hurdles unique to each manufacturer or operating system.

Case law about spoliation of workstations, e-mail, and accounting data is already well documented, but decisions around mobile device preservation are starting to take center stage. In the matter of *Christou v. Beatport, LLC (D. Colo. Jan. 23, 2013),* Defendant failed to preserve text messages on an iPhone that allegedly was lost or stolen approximately 8 months after preservation letters were exchanged. Defendant maintained that sanctions were not warranted because no relevant text messages existed on the device, a point which Plaintiff dismissed because there was no indication "… that defense counsel reviewed [Defendant's] text messages and determined that they contained nothing of relevance." Although Judge R. Brooke Jackson did not grant an adverse jury instruction, spoliation sanctions were warranted and Plaintiffs would be allowed to produce the legal hold letter at trial and argue "whatever inference they hope the jury will draw."

More recently, Judge Francisco A. Besosa delivered an adverse inference instruction in the matter of *Calderon v. Corporacion Puertorrique a de Salud (D.P.R. Jan. 16, 2014)* for the "conscious abandonment of potentially useful evidence." The evidence in question in this harassment and discrimination case was a series of SMS messages and e-mails between the plaintiff and the alleged harasser. Defendants argued that Plaintiff's admission that some of the communications had been deleted, and some preserved, warranted case dismissal. Defendants were able to preserve and produce communications among the parties that Plaintiffs should have preserved and produced, but failed to. Although Judge Besosa concluded that spoliation by Plaintiffs was not "particularly egregious or extreme," he did note that after spoliation is determined, "…the Court enjoys considerable discretion over whether to sanction the offending party."

Finally, as we witnessed in *Nuvasive, Inc. v.*

Madsen Med. Inc. (S.D. Cal. Jan. 26, 2016), even the recent updates to FRCP 37(e) that require proof of the "intent to deprive" a party of information in order to levy sanctions in the form of an adverse inference or, in extreme circumstances, case dismissal cannot shield an accused party of negative consequences for failure to preserve. The court granted Plaintiff's motion to reconsider a prior adverse inference instruction for failure to preserve and produce text message data, a decision the moving party claimed should be vacated due to the higher burden of proof required by the updated 37(e). Brushing aside arguments about whether the new rule can justly be applied to a previous instruction, the court decided to allow counsel on both sides to present the jury with further information about the missing data itself so that they, the jury, "may consider such evidence along with all other evidence in the case in making its decision."

Institutionalizing Mobile Device Management

These cases alone justify the creation of a mobile device management (MDM) policy and incident response plan well in advance of litigation or regulatory events. Together, they establish that electronic communications of all kinds are considered accessible by the courts and will not be afforded certain expectations of privacy. Prior to enacting a mobile device management policy, an organization must know exactly what devices it has, or will have, in order to better understand the hurdles unique to each manufacturer or operating system. Consider the following storage systems, retention schemes, deleted item recovery options, and preservation options for some of today's most popular mobile devices when formulating a mobile device management strategy or responding to a preservation trigger.

iPhone/iPad

Method of SMS/MMS/Chat Storage: Apple devices such as the iPhone and iPad employ variations of the Apple Darwin operating system which was later branded as the "iPhone OS" and ultimately shortened to simply "iOS." Apple devices currently store text message information inside a special-purpose SQLite database appropriately named "SMS.db." When iOS 5 emerged in 2011, Apple added a special iOS-to-iOS messaging feature called iMessage. Although iMessages do not transmit via the Short Message Service (SMS) protocol, iMessages are also stored within the SMS.db structure.

Retention Scheme: With IOS 5, Apple capped the messaging database to 15 megabytes, or approximately 75,000 text messages. Once the limit is reached, the user receives a warning that his or her "SMS mailbox is full" and the user would need to delete messages in order to free up space. More recent iOS versions have expanded storage limits and, as an added bonus for information governance

hawks, there is now an option available to automatically delete old messages after 30 days or one year. If a user opts instead to store messages "Forever," they are retained until the user deletes them manually or until the device's internal memory runs low, whereupon no additional messages can be stored (dependent again on the iOS version in use).

Deleted Item Recovery: When a user deletes a message, that message is simply flagged in the SMS database to be hidden from the user's view. There is no evidence to suggest that the iPhone or iPad will automatically delete or overwrite messages, although a periodic "vacuum" routine purges deleted records from the SMS database. The vacuum occurs at "page level" in digital storage terms and one page of storage space generally holds up to 4 kilobytes of data. If every single SMS record stored on a particular page of memory has been marked for deletion, the records are permanently deleted; if there is even one single "active" message on that page, the entire page will remain intact. This can result in an anomaly where relatively older deleted messages are forensically recoverable, but relatively more recent deleted messages are not recoverable because they happen to occupy the same memory page as one or more currently-active messages.

iOS also features device-wide indexing and searching. Users may find on occasion that previously-deleted text messages are still visible when performing a device-wide search with Spotlight because the content has not been fully purged from the Spotlight index. It is also possible to search unallocated space on an iOS device; however, if the device is equipped with file-level encryption, unallocated space may be completely inaccessible because the keys used to encrypt the data at the time it was created have been discarded.

Legal Hold & Preservation Options: Although Apple does not provide a central, enterprise-level Mobile Device Management (MDM) suite of tools, iOS comes equipped with an MDM programming interface which allows an organization to use 3rd party tools to manage the devices. The MDM interface can be used to enforce security, usage, and configuration policies on the devices. It cannot, however, be used to view calendar entries, contact information, SMS or iMessage content, photos, call logs, or GPS information. Currently, there are no central administrative tools that can force SMS messages to expire or be deleted from an iOS device; even if such a management tool existed, expired messages may still be recoverable using forensic tools.

If an organization wishes to catalog or retain the user-generated content of an iOS device, they must either obtain a backup of the device via iTunes (or a 3rd party alternative) or deploy a forensic tool to capture a physical, file system, or logical image. The level of extraction is dependent upon the model and

OS of the device. Alternatively, there are 3rd party applications that can be used to simply extract the SMS, iMessage, or other targeted data from the device when connected to a laptop or desktop computer. Although many of these tools are quite robust, they may fall short of a true enterprise solution and the demands of eDiscovery or law enforcement.

Another consideration for iPhone data retrieval is iCloud storage. With the continued integration between Apple's iCloud and iOS, users now may choose to use iCloud Backup to save their device data. iCloud automatically backs up a user's iOS device information daily over Wi-Fi when a device is turned on, locked, and connected to a power source[5] . With the user's AppleID and password, third-party tools like Elcomsoft Phone Breaker can access these backups. SMS or MMS messages that might have been deleted by the auto delete feature or by the end-user may still be accessible from those backups.

Andriod Devices
(Samsung Galaxy Family of Devices)

Method of SMS/MMS/Chat Storage: A recent Gartner study revealed that Google's Android operating system holds a hearty 84.7% share of the global mobile device operating system market[6]. The increasingly popular Samsung Galaxy S5, S6, Tab, and Note Android devices running the Lollipop operating system (versions 5.0 to 5.1.1) store message information in a dedicated SQLite database named "mmssms.db." This database is inaccessible outside of the Android application environment unless the user has obtained "root access" on the device, which would allow access to the system's privileged files.

Retention Scheme: By default, the S5 and S6 retain 1000 SMS and 100 MMS messages per conversation. Once these thresholds have been exceeded, the device's automatic deletion policy is activated to erase the oldest messages. However, these settings are configurable and can be controlled individually or by using a 3rd party MDM suite. The device will continue to operate up to these limits with each new conversation as long as storage is available. If the device's free storage space falls to 20 megabytes or less, depending on the particular device and Android version, the device will register a "full memory" notification and prompt the user to delete messages or other files.

Deleted Item Recovery: Currently, there are several 3rd party programs that offer deleted item recovery, available both as Android applications and desktop software. Due to the wide variety of Android devices and marketing-focused software modifications by wireless carriers, these applications are device-specific and the results vary greatly depending on the version of the operating

5. https://support.apple.com/kb/PH12520?locale=en_US&viewlocale=en_US

6. http://www.gartner.com/newsroom/id/3169417

system, how much storage is remaining, and the time that has elapsed since deletion of the items occurred. As free storage becomes re-allocated to new data, the remnants of these deleted files are over-written. Forensic tools are also available to attempt recovery of items from within the device's various SQLite databases, similar to widely used methods to recover corrupt or deleted data from Microsoft SQL Server running on physical Windows servers.

Legal Hold & Preservation Options: Samsung and, by extension, the family of Galaxy devices, have deployed a bundled set of corporate-friendly features such as device encryption, VPN access, and a secure implementation of Microsoft Exchange ActiveSync. Known as Samsung Approved For Enterprise (SAFE), the MDM toolkit allows enterprise security officers to rest assured that their users' Samsung devices are "enterprise ready." This designation allows for enterprise-level MDM through one of Samsung's 3rd party software partners, which include Mobile Iron, SAP, and AirWatch. Accordingly, a "sandbox" can be established on the device using the pre-installed Samsung KNOX security environment which provides enterprise administrators with secure, IT-compliant access to large numbers of devices including bring-your-own-device (BYOD) participants. In fact, early in 2013, the US Department of Defense approved the use of Android devices that are managed under the KNOX umbrella.

After configuring the KNOX sandbox environment, enterprise-level policies can be translated into globally-applied email, application, SMS, and Internet browsing configurations. These policies can be used to establish application requirements or restrictions along with the same type of controls that already exist for operating system and software updates. Although devices can be wiped, tracked, or powered down from a central management console in the event of loss or theft, current MDM solutions do not provide the ability to remotely collect or preserve text message content to respond to a legal or compliance request.

BlackBerry Devices / BES

Method of SMS/MMS/Chat Storage: Like many other mobile devices, Blackberry smartphones store data within multiple special-purpose databases on the device's storage system. In fact, there are over 120 databases on the latest Blackberry models that store everything from the Address Book to Internet browsing history and GPS coordinates. The Blackberry also stores its messaging data in such databases, including PIN, SMS, MMS, and RIM's proprietary Blackberry Messenger (BBM) messages. Much of this data can be logged, archived, or both from the Blackberry Enterprise Server (BES) management environment.

Retention Scheme: By default, most Blackberry messages including email and

SMS messages are retained on the device for up to 30 days depending on the device's model number. In an enterprise environment, email retention is governed by the policies set forth on the Exchange or Lotus Domino servers; therefore, an email purged from the device after 30 days will likely remain in the user's mailbox on the e-mail server or within the company's e-mail archive system. However, SMS messages that are deleted by the user or auto-deleted based on their age are likely not present in any other storage system and, as a result, they present a unique ESI preservation challenge. Once they are purged from the device, SMS messages are potentially only recoverable by use of mobile device forensic software. To prevent auto-deletion, the user or administrator may set the message retention period to "forever," however large SMS, MMS, and BBM databases can result in a slower user interface experience.

Deleted Item Recovery: Because SMS and other messaging data are stored within multi-purpose databases on the Blackberry device and pressing the "delete" button simply "hides" the messages from the user's view, there exists a potential for recovery of deleted items. The only theoretical limit on the number of messages stored in the SMS database is derived from the storage capacity of the device and the relative size of the messaging database. The Blackberry operating system decides when previously-deleted data will be over-written with new data, including within the SMS database. In a data preservation or recovery scenario, the quicker the device is acquired the better the chances of recovering previously-deleted messages.

Legal Hold & Preservation Options: The Blackberry Enterprise Server is capable of logging and archiving PIN, SMS, MMS, and BBM messages. The administrator can configure the system to capture both the metadata for each message (sender, recipient, date/time, etc.) and the actual content. Under no circumstances, however, will the BES server record or capture pictures sent via any of these protocols. Options for ongoing retention include logging, content archiving, or both. The organization can then set policies around how long, and under what conditions, those logs and content will be kept. GPS information can also be cataloged, but the managing organization must evaluate the potential benefits (asset loss prevention, safety of personnel) against the potential risks (personal privacy.)

Another option for Blackberry devices is the use of the Blackberry Desktop Manager (BDM) or Blackberry Link depending on the version of the device. This is the primary method by which a user or administrator can create either a full, or selective, backup of the device. Under a full backup, the entire device is captured to a file on a PC or MAC; with a selective backup, the user can be more surgical about which data is captured in the backup. Although the SMS and other messages captured in the backup are not viewable

Operating System	SMS/MMS Deletion Policy	MDM Program(s)	Enterprise SMS/ MMS Collection?	Local Back-Up
Apple iPhone/iPad	Message retention set to "Forever" by default, but can be shortened to 30 days or one year.	Air Watch and various 3rd party solutions only. No proprietary MDM solution.	No remote SMS/ MMS collection or retention capabilities. Only administrative device security. Backup to personal Cloud.	Devices can be individually backed up through Apple iTunes desktop software.
Android Samsung Galaxy Devices	Auto-deletion default is triggered after 1000 SMS and 100 MMS per conversation.	Samsung SAFE devices can use one of their 3rd partners: Air Watch, Mobile Iron, SAP, others.	No remote SMS collection. Retention policies can be set through 3rd MDM software.	Devices can be individually backed up through Samsung Kies desktop software..
BlackBerry BlackBerry Enterprise Server	Default message retention is set at 30 days. Configurable time periods including "forever."	BlackBerry Enterprise Server (BES) and BlackBerry Desktop Manager (BDM).	Yes, PIN, SMS, MMS, BBM collection and archiving through BES.	Devices can be individually backed up through BlackBerry Desktop Manager software.
Windows Phone 8	No default message expiration.	Air Watch and various 3rd solutions only. No proprietary MDM solution.	No central repository for SMS/ MMS, but remote backup possible through SkyDrive.	Devices can be individually backed up and synced with Windows 8 & 10. External SD storage possible.

directly from the BDM or Link interface, there are several 3rd party applications that can access and extract individual content types as well as attempt to recover previously-deleted items.

An organization may choose to have users or local IT administrators perform BDM or Link backups of devices in a regulatory, audit, or litigation scenario. Such backups can be copied to a central location from the user or administrator's PC and retained for the necessary legal hold duration. A more defensible, but more costly, option is to acquire a physical or logical forensic image of the target devices and extract the required data using industry standard forensic toolkits.

Windows Phone 8

Method of SMS/MMS/Chat Storage: Messages on Windows mobile devices are stored within a Microsoft Embedded Database (EDB) labeled "CEMAIL.VOL" which is the same

method of storage implemented for email messages within the Microsoft device. SMS messages also reside in a more familiar folder structure at Windows\Messaging. However, both of these databases are inaccessible by the user outside of the Windows application environment, as the operating system prevents read access rights by utilizing a layer of hardware abstraction.

As consumer technology becomes increasingly present in the corporate environment, a proper information governance strategy is paramount to ensure valuable business information is retained while stale data is purged to reduce legal and regulatory risk exposure.

Retention Scheme: By default, messages are stored until the device falls short of free storage space. To prevent data loss and storage issues, users can deploy their cloud-based Microsoft SkyDrive account as an on-demand backup solution. Once a user links their SkyDrive account to the device, the default configuration backs up all current and future text messages in a manner similar to email journaling. Message databases can be moved to external SD cards, which allows for a potentially large volume of messaging information to be stored on a removable piece of media. "Low memory" notifications occur once the device reaches a critically low level of available storage. The exact threshold of storage needed to trigger this notification depends on native device storage, SkyDrive syncing, and SD card storage. Once the phone and its accompanying alternative storage options are full, the device will be unable to receive or send messages until storage space is freed up.

Deleted Item Recovery: Currently, 3rd party tools for recovering deleted messages from Windows Phone 8 have limited utility. Although the names of deleted files are fairly easy to recover, difficulty is encountered in actually recovering the contents of such files which the operating system has back-filled with meaningless binary codes. Windows Mobile creates temporary files in various locations throughout the device that can provide useful information regarding deleted files, but the only way to examine these files is through the use of specialty forensic tools. Although there are limited deleted item recovery options, SkyDrive can be set to sync all messages to a user's account if they have linked their account with their Windows Phone. If this function has been enabled, old messages deleted locally on the device may still be available via SkyDrive. Messages are generally stored as text files and can be viewed with any text editor, MS Word, and in some cases directly online via Office 365.

Legal Hold & Preservation Options: Windows mobile devices are easily deployed and managed through a number of 3rd party MDM suites such as AirWatch and Sophos Mobile Control. However, like the iOS platform, the Windows MDM API does not allow administrative access to personal information such as SMS messages and

pictures, leaving administrators and legal teams with few options to enact a legal hold. If the user chooses to backup their personal data to SkyDrive, remote preservation and collection are possible from the cloud with user consent. Backups of the physical device can be made through Microsoft's Zune software and a number of 3rd party desktop tools; however, these tools may not be as defensible as a forensic collection suite such as the Cellebrite UFED Touch, which is the same device used by law enforcement and the military to extract data from mobile devices. The time it takes to acquire a physical device and capture a backup or image leaves the organization at risk of spoliation due to the fact that mobile devices are easily broken, lost, or stolen before acquisition occurs.

Planning for SMS Discovery

As consumer technology continues to infiltrate the corporate working environment, a proper information governance strategy is paramount to ensure that valuable business information is retained while stale data is purged to reduce legal and regulatory risk exposure. Today's always-connected, mobile information worker generates an ocean of discoverable ESI that is essentially stored in their pocket or purse and likely falls just outside the sphere of administrative control. Initially a communication tool popular with teenagers and college students, SMS messaging is now a mature and ubiquitous collaboration channel. Recent case law suggests that this data, and SMS messages in particular, is no longer unduly burdensome to preserve and collect. Although the number of devices, operating systems, and 3rd party tools present a dizzying array of consumer and business options, a careful examination of the intersection of governance policy and MDM options is a necessary exercise for organizations of all sizes.

Author Biography

Joshua Headley

Josh is the Director of Litigation Support Analysts and Application Development, and has nearly 10 years of experience in systems analysis and engineering. He joins D4 from Nixon Peabody LLP, where he applied his analytic and programming skills to the growing field of electronic discovery.

A go-to resource for managing large-scale collection and review efforts, Joshua has also become an expert at guiding clients large and small through the discovery of ESI through in-depth dialogs with information technology personnel, senior management, legal counsel, and forensic experts. He has demonstrable expertise in many eDiscovery applications in use today including LAW, Relativity, FTK, MS SQL Server, and DT Search.

About D4

D4 is a national provider of electronic discovery, computer forensics, information security and management, and deposition services to law firms and corporations, and has been instrumental in helping customers realize up to a 70% cost reduction over previous eDiscovery solutions. At D4, we focus on technology and process to streamline the discovery life-cycle in the most defensible, practical and cost-effective manner possible. We believe that eDiscovery doesn't have to break the bank – and we make that belief a reality for clients every day.

Founded in 1997 in Upstate New York, D4 has grown to a national presence. With over 160 employees, D4 has offices in Buffalo, Chicago, Detroit, Grand Rapids, Lincoln, New York City, Omaha, Orlando, Phoenix, Rochester, San Francisco, San Diego and Tampa. D4's state-of-the-art Tier 3 data center and operations in Rochester are complemented by electronic discovery, litigation support and paper document services in other offices across the country. D4 has been recognized by Inc. Magazine as one of the fastest-growing private companies in the US, and is a fourtime Inc. 500/5000 honoree.

There is a reason why hundreds of AMLAW 200 firms and Fortune 1000 companies choose D4. Our unprecedented customer service, coupled with our industry experts and bestof- breed technology, is why the D4 way is the better way.

How D4 Can Help

Are you tasked with collecting and producing SMS messages or overwhelmed by the logistics of creating a mobile device management (MDM) policy?

Schedule a complimentary consultation with a D4 subject matter expert (SME) today. We can assist you in managing the preservation process and recommend the best approach to take for your unique situation.

D4 Can Assist You With:

- Developing a preservation plan for ESI from mobile devices and the cloud.
- Executing on that plan to preserve data in a defensible and timely fashion.
- The creation of a BYOD policy and selection of an MDM policy.

SCHEDULE A COMPLEMENTARY CONSULTATION TODAY

www.d4discovery.com
marketing@d4discovery.com
800.710.4066