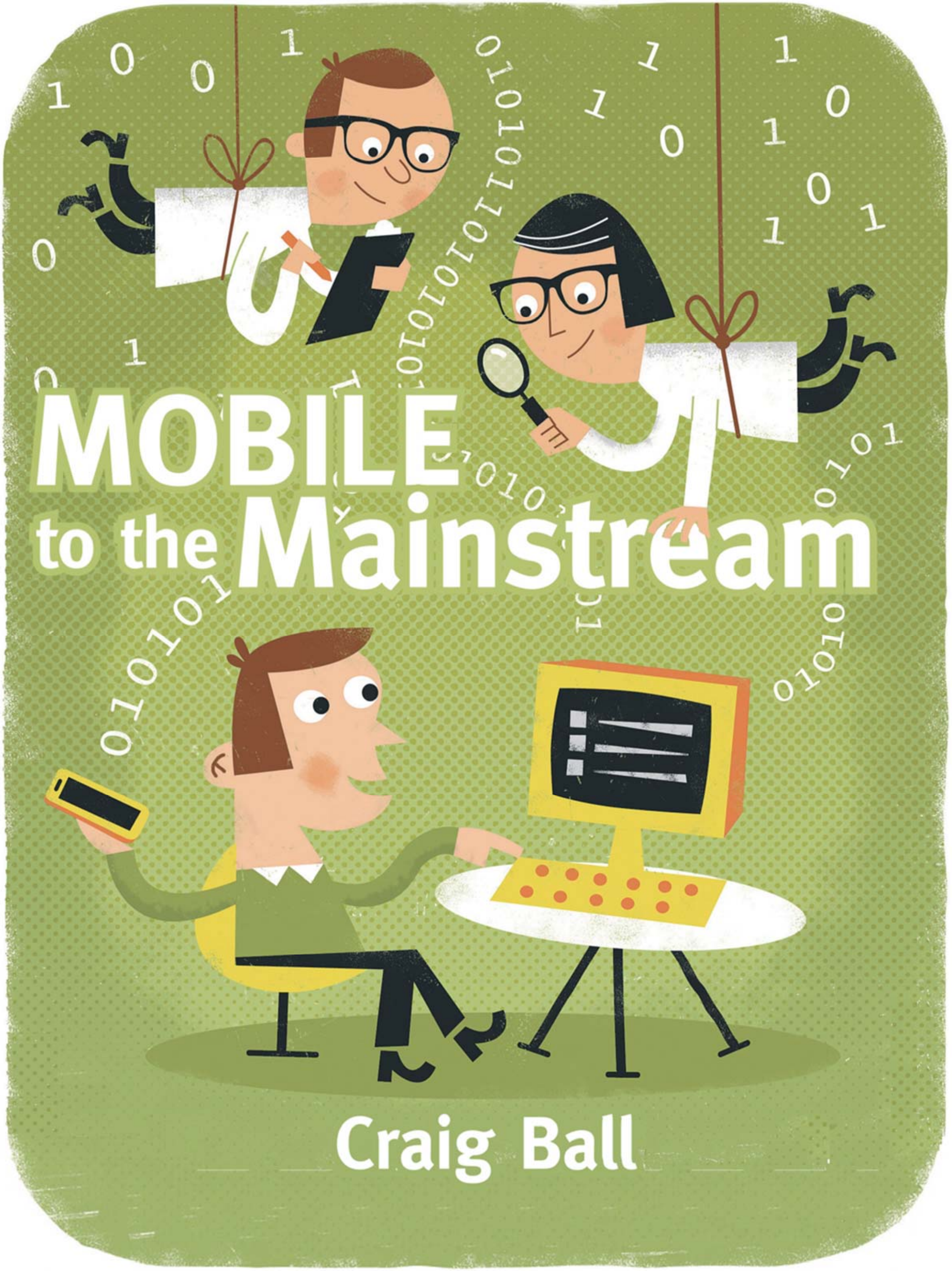


MOBILE to the Mainstream

Craig Ball

Mobile to the Mainstream

Craig Ball ©2018

Once you've preserved the contents of a mobile device, how do you extract responsive in forms that are searchable and amenable to review? Most information items on mobile devices aren't "documents" that can be printed to a static format for review. Instead, much mobile content is fielded data that must retain a measure of structural integrity for intelligibility. This article looks at simple, low-cost approaches to getting relevant and responsive mobile data into a standard e-discovery review workflow and offers a Mobile Evidence Scorecard designed to start a dialogue leading to a consensus about what forms of mobile content should be routinely collected and reviewed in e-discovery, without the need for digital forensic examination.

In the last decade, the iPhone and other smart mobile devices have tethered us to apps and networks in powerful, unprecedented ways. Daily, the average user spends four hours on her phone spread over seventy-six sessions. For most users, smartphones are the first thing picked up in the morning and the last set down at night. Even when we aren't looking at them, smartphones receive communications, push and pull data, record our activities and broadcast our locations. Two-thirds of e-mail communications are sent and received using phones.

Over the last fifteen years, litigants have made strides in establishing defensible, repeatable procedures for preserving, collecting, processing, culling, reviewing and producing legacy paper documents, e-mail and productivity files residing on personal computers and servers, to the point that these functions have been brought in-house at many corporations and a few law firms. By contrast, few corporations and firms have acted to systemize the preservation and production of data from smartphones. Despite being powerful, capacious computers, most lawyers and litigants treat mobile devices as if they only made phone calls. When addressed at all, smartphones are relegated to forensic examination by an expert rather than approached as a routine, repeatable process managed by e-discovery teams. Smartphones aren't "special" and, by virtue of enhanced security features on phones, there's little responsive content that can be collected through forensics that cannot also be gotten by e-discovery personnel. Smartphones are everyday tools that must be made a part of everyday, mainstream e-discovery.

Collection from computers could be routinized because there was consensus as to the types of information that should ordinarily be preserved, collected and reviewed. These included e-mail messages, photos, videos, and productivity formats like Word documents, Excel spreadsheets, PowerPoint presentations and PDFs. Contents of databases tended to be addressed on an *ad hoc* basis through negotiation between opposing parties.

No consensus exists as to what data must be routinely preserved and produced from mobile sources. Partly this stems from litigants' recalcitrance towards mobile evidence, and partly it's a consequence of the "special" forensic treatment accorded mobile sources. A forensic extraction seeks to recover everything: active data, latent data and deleted artifacts. "Get all you can get" is the *de facto* forensic standard, but often bears no proportionate relationship to the issues in the case. Forensic examiners endeavor to "get it all" because that's what we're trained to do, and what forensic tools are designed to do. Yet, "getting it all"—irrespective or relevance or materiality—is NOT what litigants or lawyers are obliged to do in e-discovery.

In the absence of circumstances prompting a need for digital forensics, e-discovery centers on active data, not latent artifacts. Forensically-sound techniques are routinely bought to bear on preservation; but, it's the rare matter that calls for forensic analyses of all sources. The cost would be unbearable were forensic analysis the norm for all matters.

So, what's our takeaway for smartphones? I'd argue that we must get the readily-accessible evidence on phones when it's relevant and responsive, but we must also strike a balance between what may be obtained through forensics versus what can be obtained using less-exacting but *reasonable and proportionate* methodologies. That is, not all we might want, but what's readily available, relevant and non-privileged considering the needs of the case.

Applying this principle, let's look at some of the data routinely found on a smartphone (and its backup) and consider potential relevance and burden issues. Note that all the extractions and exports I'm about to describe were accomplished with an easy-to-use, dirt cheap tool that runs on both Windows AND Mac--just one of several such inexpensive tools in the marketplace:

Files: Like a personal computer, phones hold word processed documents, spreadsheets, presentations and other files routinely responsive in e-discovery. Some of these items may be duplicative of other sources, but some may be unique to the phone. The burden of collecting files from mobile sources is not fundamentally different than collection from desktops, laptops, servers and cloud sources; so, unless it can be shown that documents on phones are merely duplicates of material collected elsewhere, there would seem to be no basis to eschew collection of files from mobile sources when potentially relevant.

Photos and Videos: Photographs and videos are some of the easiest items to collect from mobile sources, and phones have become the richest sources of photographic evidence. A phone may hold only a thumbnail-sized version of photos if the user, seeking to save space on the phone, configured the device to store photos in the cloud for download on demand. In that case, full resolution photos must either be downloaded to the phone before backup (if enough local storage is available) or independently collected from cloud storage. As iPhones now store photos in a High Efficiency Image File Format (with the file extension HEIC), parties collecting photos must weigh whether to collect in HEIC or convert to images JPEGs. Conversion entails loss of functionality for so-called "live" storing image sequences; but, many tools do not yet support the HEIC format.

Music and Ringtones: I've handled only two matters where a custodian's music collection was relevant to the issues in the case, and both were forensic investigations. Generally, music and ringtones won't be collected in e-discovery apart from the rare case where they have some unique relevance to the dispute. The burden to collect is small; but, the volume may be large, and music files are often rendered unusable by encryption.

Books: Like music, commercially-published books are rarely candidates for collection in discovery. Conceivably, references sources used by a key custodian and stored on the custodian's mobile device might be relevant, but that's not likely to occur with such frequency as to regard books as routine fodder for collection. Like music, books may be rendered unusable by encryption for copyright protection.

Messages: Messaging has eclipsed e-mail as the most common form of personal and business communication. Double-digit growth in messaging volume mirrors double-digit declines in e-mail usage. ***More than any other form of mobile evidence, messaging must become a source routinely scrutinized***

in e-discovery. The default message retention setting for the native messaging app on iPhones is to keep messages "forever;" so, it's common to encounter many thousands of messages and dozens or hundreds of message threads on each device.

Messages are threaded according to the participants in the thread; consequently, you may have multiple threads including the same person in different groups of recipients as well as separate threads for the same person communicating from different devices or under different aliases (that is, by phone number or by contact name or nickname). The threading issues don't complicate collection, but they make review challenging. E-discovery veterans may note that the same challenges existed with e-mail and were solved once tools were purpose-built to deal with e-mail in discovery. Demand drove innovation for e-mail in ways that have yet to emerge for messaging.

There is little burden to collect threaded messaging stored on mobile devices, and it's trivial to export messaging in delimited formats like CSV files that can be viewed as spreadsheets. Attachments to messages can also be exported with ease, although the tools to do so may not neatly pair the attachment with its transmitting message and emoji may render as cryptic characters unless you change the encoding to Unicode UTF-8 when loading the file. It's also easy to export the threads as a text or PDF file, though so doing will severely limit the utility of the data in terms of reordering the contents of columns for sender, date, etc. Delimited formats are preferable unless the reviewer cannot use a spreadsheet or intends to (*shudder*) print the messages out. All forms will facilitate text search when ingested by an e-discovery review tool, unless the tool requires load files be generated to support even rudimentary text searches.

That last point underscores why messaging can be so simple to collect yet daunting to review*: too many review tools have failed to keep pace with important sources of electronic evidence* (like messaging or collaboration tools like Slack). It's not a preservation or collection problem. It's not even a processing problem. *All these are cheap and easy tasks.* The problem lies with culling and review.

The other big challenge to messaging is the variety of messaging channels in the marketplace. Though most people message from the native messaging app on their phones, many use proprietary and cross-platform apps like WhatsApp, Facebook Messenger, WeChat or Skype. Even Words with Friends supports texting between players!

Some of the low-cost apps capable of exporting messaging don't support specialized messaging apps as capably as they support native messaging capabilities or may not support them at all. These shortcomings don't auger for continuing to ignore messaging in discovery; however, it does require that expectations be calibrated to the limitations of the tools at your disposal and, crucially, to the reasonable expectations of the Court and opposing parties. The inability to get all the messages that may exist isn't reason to collect none but may require the use of more sophisticated tools and expert assistance to achieve quality and completeness.

Phone Call History: It's just a click or two to export a delimited file of an iPhone's call history, including contacts/phone numbers, call times, call directions (incoming/outgoing) and call durations. It's considerably less burdensome than it was to pull a paper phone call detail from a file, back when phone companies routinely supplied call details. It's far easier than logging into a cell provider's website and downloading a call history. Yet in e-discovery practice, phone call histories were only sought and produced when the call record was pertinent to a claim or defense in the cause; they weren't routinely sought simply because the information existed. Accordingly, mobile phone call history records aren't likely to be scrutinized absent a specific request and a plausible nexus between the data and the issues.

Voice Mail: Voice mail can be easily exported as a delimited CSV file showing time of call, duration, caller, number and, in some instances, a transcript of the message. The audio files for each message can also be exported in the .amr audio format, playable via QuickTime or iTunes. Unfortunately, the CSV file doesn't hyperlink to the audio files, making review a tedious process. Comparing mobile voicemail to its e-discovery antecedents, it's considerably easier to collect mobile voicemail, but it's just as challenging to review absent costly processing for message transcription or phonemic search.

Browser History and Bookmarks: Exporting browser history and bookmarks is far simpler for a mobile device as the task usually required expert assistance to collect from a personal computer but can be achieved with a few clicks from a phone backup. But, even if the data doesn't require expert intervention, is it likely to be relevant in enough matters to require routine collection? The jury is out on that, but the better approach is probably to require a specific request before routinely collecting and reviewing browser histories.

Calendar: Calendar entries for any selected interval can be exported to an iCal or CSV file format. If paper or Outlook calendars would have been reviewed in the past, then this data is easier to collect and ingest than processing a PST or photocopying years of paper calendars. The mobile calendar data is also much easier to redact.

Contacts: Another case- and custodian-specific determination as to collection and processing. All contacts or just selected contacts can be exported as a CSV file or as discrete VCards. Rudimentary text filtering before export is feasible, such as by including only contacts that include a relevant area- or zip code.

Notes: On iPhones, Notes is a no-frills word processing application akin to Windows Notepad. Some use it extensively; some not at all; but whether it holds user-generated documents relevant to the case should be routinely assessed. Single notes documents can be exported to PDF. Selected items or all Notes documents can be exported as discrete plain text files for each document, files named by date, time and first eight words of the Notes entry.

Voice Memos: As the name implies, the built-in Voice Memos app lets users record any audio to the iPhone. These can be exported, singly or collectively, as .M4A audio files and the exported files will retain the names of the source recordings. Like Voice Mail, Voice Memos are challenging to review without transcription or processing the audio for phonemic search; otherwise, there's no clear reason to distinguish a custodian's potentially responsive voice memos from memos made with Notes or other word processor in terms of preservation and collection.

Apps: Evidence that can be exported from individual apps varies as widely as the apps themselves. Although the data collected from apps comprise the customary JSON, PLIST and SQLITE files familiar to forensic examiners, apps also yield photos and documents in familiar productivity formats; the same files customarily collected when found on a user's laptop, desktop or network share. Any file can be exported easily; but, it's a manual process unaided by search or filtering features. As such, parsing all apps in this manner approaches the burden of a forensic examination without the benefit of an examiner's expertise. If a handful of apps are known to hold responsive files in intelligible formats, it's feasible and cost-effective to export potentially-responsive files one-by-one; else, it's not a scalable workflow.

File System: Though it’s feasible to export most of the thousands of data and configuration files that make up the phone’s file system, little of that data would be intelligible to counsel without further processing, expert assistance and, sometimes, decryption of contents. As such, file system artifacts are probably best left to forensic investigations and won’t be routinely collected and reviewed as part of routine e-discovery.

Geolocation Data: Geolocation data is relevant in many cases, even dispositive in some. Geolocation data is one of those peculiar sources of powerfully probative evidence (like e-mail stored on iPhones) that is readily accessible to a user via a few screen taps but enormously difficult to collect and review efficiently. By U.S. Federal law, any cell phone capable of making or receiving calls must broadcast its location in order to support 911 emergency response services. By default, an iPhone closely tracks a user’s movements for months, recording locations visited and the times and durations of visits in its Significant Locations database. The latest version even records the length of the drive prior to arrival.

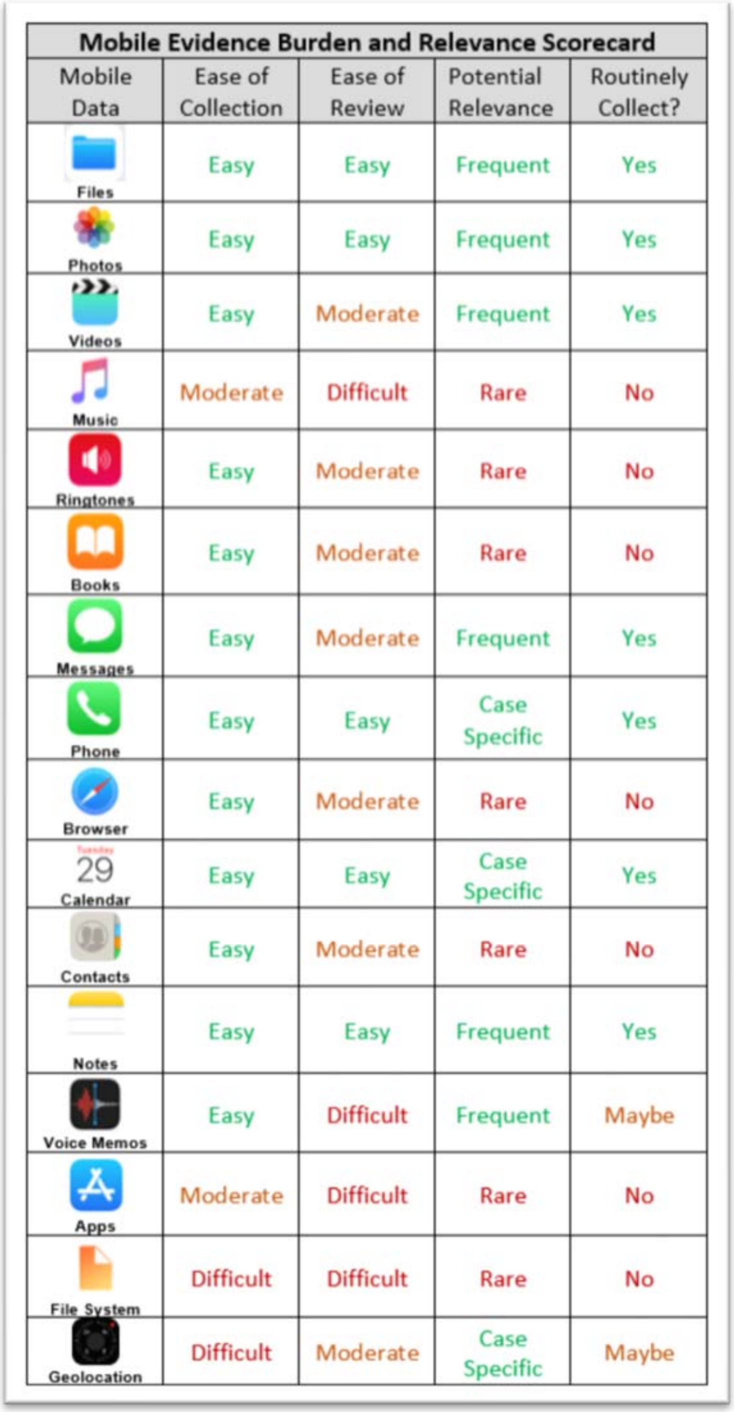
Any iPhone user can readily access their geolocation history via *Settings>Privacy>Location Services>System Services>Significant Locations.* It’s trivial. But, the only way to collect this data without jailbreaking the phone and using specialized forensics software is to grab screenshots of the Significant Locations screens. That’s because Apple protects this data and won’t allow it to be exported. It’s not backed up nor is it stored in iCloud. It’s not difficult to acquire geolocation data by screenshots; it’s just tedious, and data acquired by screenshots won’t be text searchable or capable of being exported to mapping tools that would enhance its utility. To accomplish that, you need a digital forensics expert to acquire the recorded coordinates in a standard file format suited to geospatial data (*e.g.*, Keyhole Markup or JSON files).

Scalability and Workflow Integration: An advantage of forensic tools is their scalability. Using X-Ways Forensics, Encase, FTK or one of the other tool suites, I can filter and search the data from dozens of hard- and thumb drive images in a single operation. I can export from some or all the images as easily and deliver the data in forms more-or-less suited for ingestion into a review platform. But, phone forensics has never been scalable. I don't know of a production tool that's designed to manage simultaneous processing and analysis of dozens of phone images. If it exists, I doubt it's within the tool budgets of most forensic examiners.

The forty- or fifty buck consumer grade tools that accomplish the tasks I've just described do a mighty good job against a handful of phones and pads; but, they don't scale--hardly a criticism considering that six-figure phone forensics tools don't either. As mobile enters mainstream discovery, the tools we employ must scale to support, not one or two devices, but dozens or hundreds of phones and pads. Still, we cannot wait for the perfect tool set to emerge. The evidence is here now, and no party should imagine a court will accept the excuse, "I didn't deal with any mobile evidence because I couldn't deal with all of it." Lawyers don't eliminate risk; we manage it. So, manage it.

The Mobile Evidence Scorecard: The information just shared are my opinions; however, they’re based on experience and testing for each form of evidence listed. In my latest testing, I used a $50.00 tool called iMazing (www.imazing.com) that runs on both Windows and Mac machines. I like iMazing for these tasks, but there are other low-cost tools that perform admirably.

In an effort to distill these observations into a lay roadmap for collection and review of mobile content in e-discovery, I prepared the Mobile Evidence Scorecard. In it, I assess the burdens attendant to collection and review and the potential relevance of each source based upon existing standards in e-discovery and my years as a trial lawyer, e-discovery special master and forensic examiner. I invite different views of the criteria I used for the scorecard and conclusions I reached, asking only that the rationale for a different conclusion be shared, too. Please share better, cheaper and faster ways.



Mobile Evidence Burden and Relevance Scorecard

Mobile Data	Ease of Collection	Ease of Review	Potential Relevance	Routinely Collect?
Files	Easy	Easy	Frequent	Yes
Photos	Easy	Easy	Frequent	Yes
Videos	Easy	Moderate	Frequent	Yes
Music	Moderate	Difficult	Rare	No
Ringtones	Easy	Moderate	Rare	No
Books	Easy	Moderate	Rare	No
Messages	Easy	Moderate	Frequent	Yes
Phone	Easy	Easy	Case Specific	Yes
Browser	Easy	Moderate	Rare	No
Calendar	Easy	Easy	Case Specific	Yes
Contacts	Easy	Moderate	Rare	No
Notes	Easy	Easy	Frequent	Yes
Voice Memos	Easy	Difficult	Frequent	Maybe
Apps	Moderate	Difficult	Rare	No
File System	Difficult	Difficult	Rare	No
Geolocation	Difficult	Moderate	Case Specific	Maybe

My goal is to foster consensus as to what data must be routinely preserved and produced from mobile sources. Messaging (be it called SMS, MMS, texting or instant messaging) must be every bit as mainstream and obligatory as e-mail. Mobile photos and video must be considered in appropriate cases for both the probative value of the images and that of the embedded EXIF time and geolocation data.

We can't keep our heads in the sand on mobile simply because we've grown complacent with e-mail and documents. Evidence isn't documents anymore; it's data, and much of that evidence resides in those tiny, powerful computers in our pockets and purses. Notes content should be given a measure of the same scrutiny we devote to Word documents. Call logs, voice mail and calendar entries should all be collected and processed when they may bear on the issues. Relevant files are no less relevant because they've been stored in a pocket instead of on a server. If such evidence can be made ready for review with little skill and a fifty-dollar tool, where is the burden?

We've only to look around to see the changes wrought by mobile devices and the compelling reasons to move mobile to the mainstream of e-discovery. But honestly, who looks around anymore? We're all so busy staring at our phones. 😉