A Starting Point For Mobile Device Discovery

April 25, 2013

By: Greg Buckles

eDiscoveryJournal

This eDiscoverJournal research brief explores eDJ's survey results and market research into the current impact of mobile devices on civil corporate discovery. The brief is aimed at eDiscovery professionals seeking to understand the new challenges posed by these unique data sources and the general approaches for handling this new content. At least two more in depth research reports will follow this foundation to cover BYOD policies and preservation/collection technologies and approaches.

Table of Contents

Mobile Discovery: Soon To Be A Fact Of Life

The eDiscovery industry as it exists today was born out of a need to collect, preserve, process, review, and produce electronic information that was created and stored in an increasingly distributed fashion. First, there was the birth of client-server computing that put information out on local PCs. Next, the introduction of laptop computers made this distributed information much more portable. Combine that with the advent of high-volume user-generated collaboration tools such as email and the resulting information explosion creates eDiscovery challenges that most corporations still grapple with today.

Such eDiscovery challenges will only continue to grow as new forms of content gain mainstream traction and the variety of devices on which to create, store, manage, and share that content proliferate. If there is anything to be learned from the last decade of eDiscovery, it is that ignoring the challenges will only exacerbate them. One issue organizations cannot ignore is discovery of mobile device content.

Mobile devices are everywhere and touch everything

- 88% of Americans have cell phones and 46% own smartphones
- 63% of corporate devices are used for personal activities
- 65% of Fortune 100 are deploying/piloting iPads

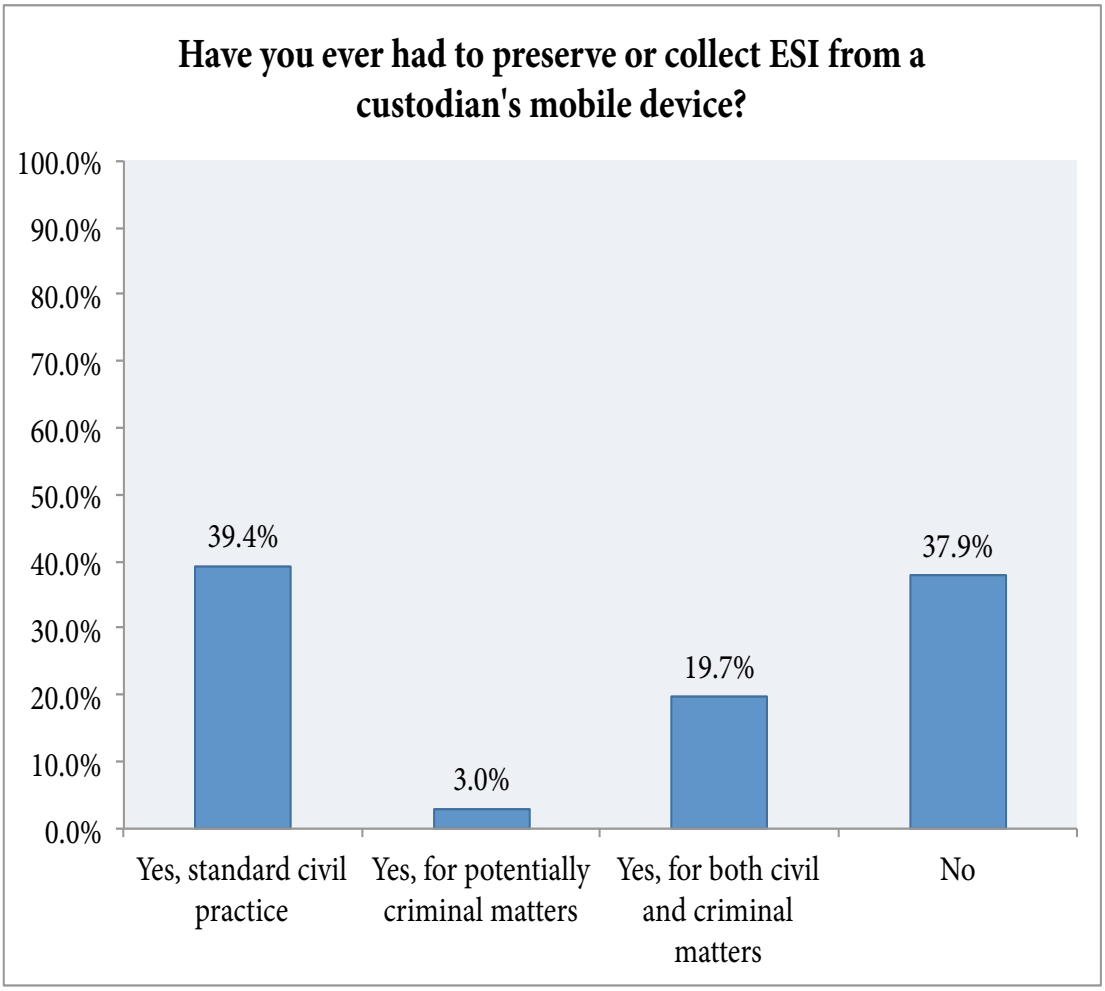
Sources:
Pew Internet and American life Project (http://pewinternet.org/Reports/2012/Smartphone-Update-2012/Findings.aspx)
Power, Richard. "*Mobility and Security: Dazzling Opportunities, Profound Challenges*" - See more at: http://www.cylab.cmu.edu/news_events/news/2011/mcafee-mobility-security-study.html#sthash.xgxvOYA8.dpuf; McAfee and Carnegie Mellon University Cylab

Ignoring mobile discovery will undoubtedly lead organizations down a familiar path, one littered with sanctions, out-of-control eDiscovery costs, and myriad frustrations. The reality is that mobile device civil discovery is gaining speed. Organizations should prepare for the inevitable reality of mobile discovery and know their devices, data, usage, and policies. This report will show that mobile devices are already being requested in discovery and that they cannot be handled like a laptop or network share.

Mobile Discovery Today - Greater Than Might Be Expected

eDJ conducts an ongoing survey about mobile discovery experiences and has found that a majority of organizations have had to collect ESI from a mobile device.

More Than Half Of Respondents Conduct Mobile Discovery

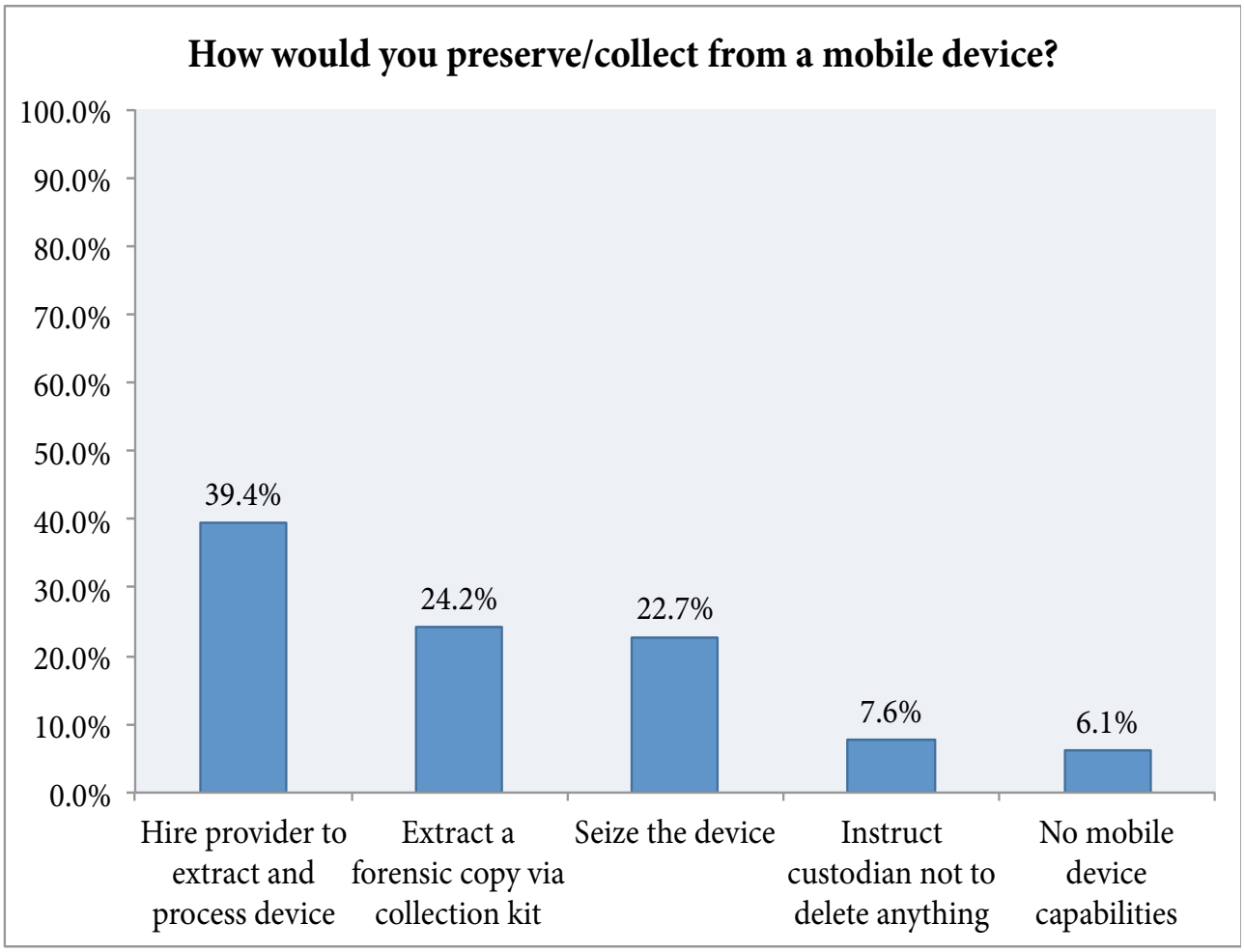


Source: eDiscoveryJournal Mobile Discovery Survey N = 66

Despite the fact that mobile discovery is required and organizations have had to collect ESI from mobile devices, there is not necessarily maturity in the approach to such collection. Many organizations – about 40% of respondents – hire a third-party provider to extract data from devices when faced with mobile discovery. Another 20% simply seize the actual devices for the purposes of discovery. Only about 20% of respondents in our survey report actually using a collection kit to obtain a forensic copy of ESI on devices.

In large part this reliance on third party forensic service providers is based on the complexity of the devices combined with the relatively specialized software required to collect that data. Until recently, collecting data from a mobile phone was the exclusive province of a forensic technical specialist. Although currently eDJ tracks thirteen providers of mobile device collection technology, only 4-5 of them are suitable for corporate use. Even these require training and constant updates to keep up with the rapidly evolving devices.

Mobile Discovery Collection Practices Still Immature



Source: eDiscoveryJournal Mobile Discovery Survey N = 66

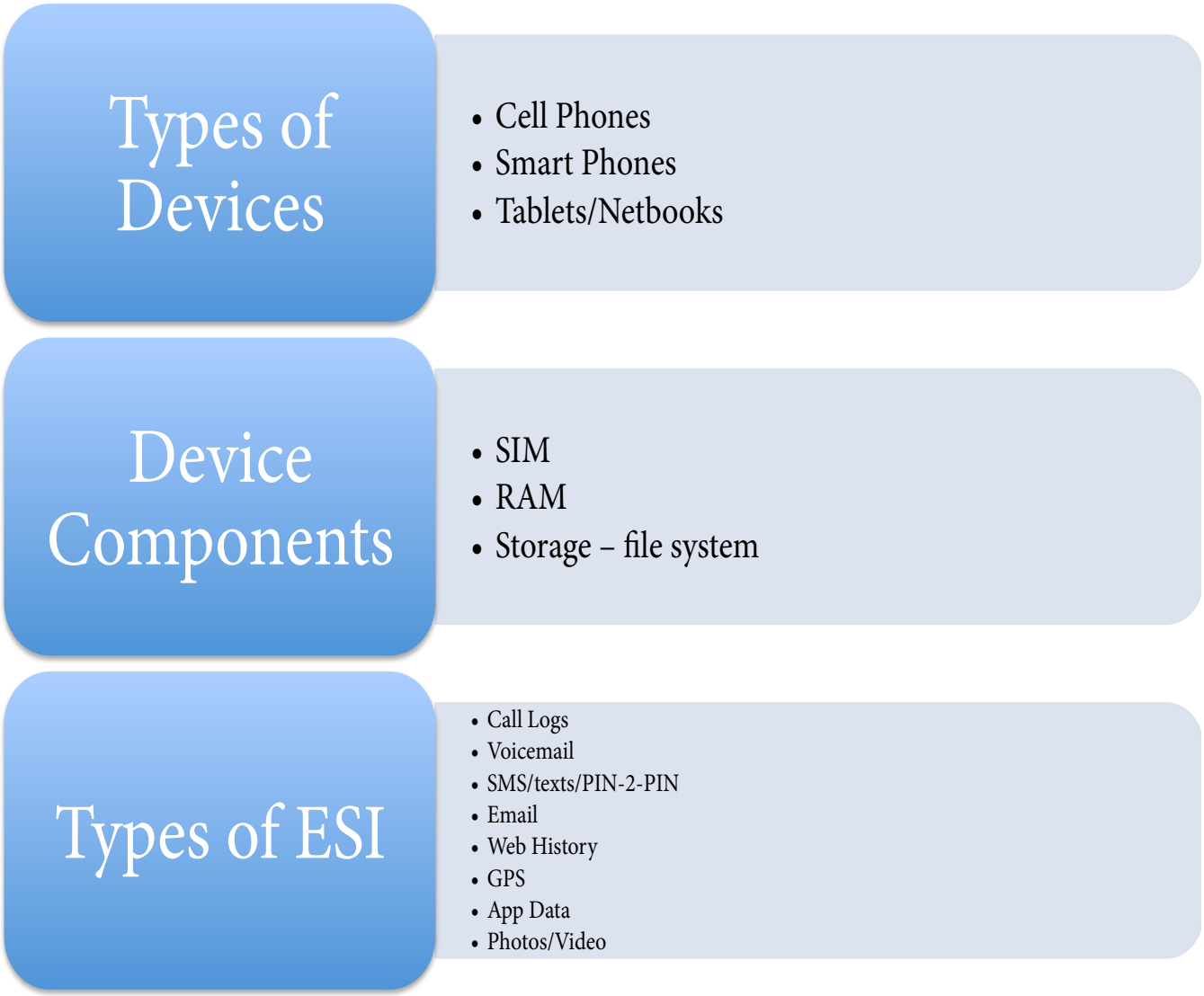
How to Prepare For Mobile Discovery

In order to be ready for mobile discovery, it is critical to know what types of data are housed on mobile devices, how to acquire and process that data when necessary, and how to export and produce that data if required.

Understanding Mobile Device Content

A Smart phone is not just a hard drive. There are a variety of mobile devices and a diverse set of information that each type of device stores. The figure below shows the types of devices and components that exist and the types of information that may be stored. You may have to perform collections on each device component, which increases the complexity of data processing and review.

Understanding Mobile ESI



Understanding the types of data that exist on mobile devices will allow you to best determine approaches for collecting and processing that data when needed for litigation, regulatory action, or internal investigations. The important point here is to identify truly unique, relevant ESI that is not already replicated on your enterprise systems. Many corporate litigants already have archives that collect all corporate email, voicemail and instant messaging. Counsel will have to understand the unique mobile content and make a make a call as to preservation requirements and techniques, and, potentially to collection, processing and production. As to preservation decisions, documented custodian questionnaires and interviews can help to exclude text messages, photos, videos, location information, call logs and other mobile app content.

Preserving Mobile Content

Creating an effective, defensible legal hold strategy for mobile devices is especially challenging due to their dynamic storage management. Unlike laptops and network shares, mobile devices are designed to manage and expire inactive texts, call logs and other volatile ESI. Custodians under legal hold may refrain from deleting files and other static content, but preservation collections or backups may be required if more dynamic content is

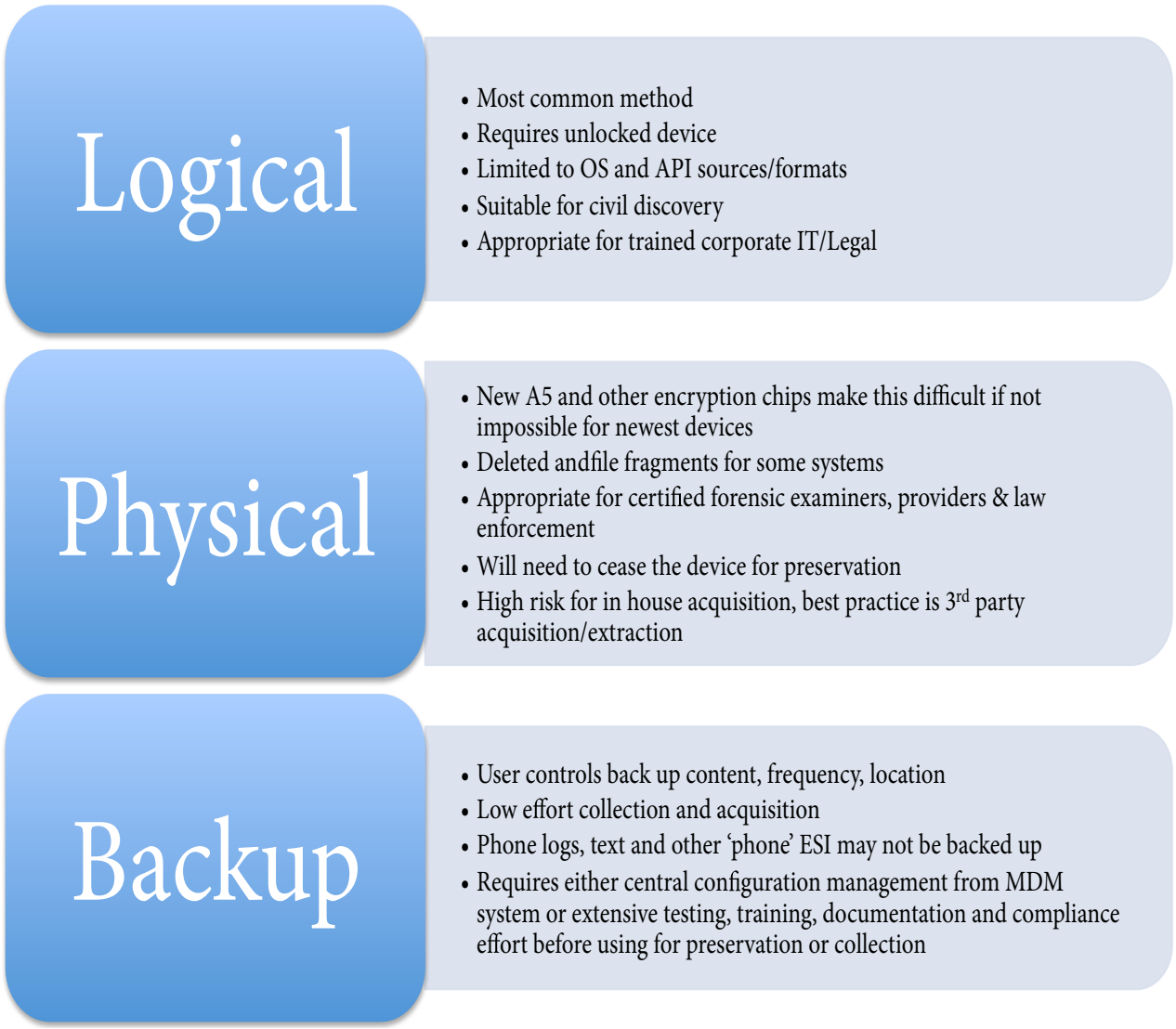
potentially relevant.

Collecting Mobile Device Content

The proliferation of mobile devices has occurred very quickly. The existence of these devices is still relatively new. With several major device providers and fast release cycles, there are numerous devices types and a plethora of collection mechanisms. The security on most recent generation of devices (iPhone 4s+, Android & Blackberry) requires that the device be unlocked for collection. Even when unlocked, most software can only collect the 'logical' data from the device operating system instead of a true 'physical' bit-by-bit copy of the storage components. Luckily, most user deleted content is still accessible from the logical collection. Device backups are relatively easy to collect and process, but they may not preserve critical content without changes to the configuration settings. They also pose a hidden risk when custodians backup corporate ESI onto their home computers.

The table below outlines the major ESI acquisition methods for mobile device content.

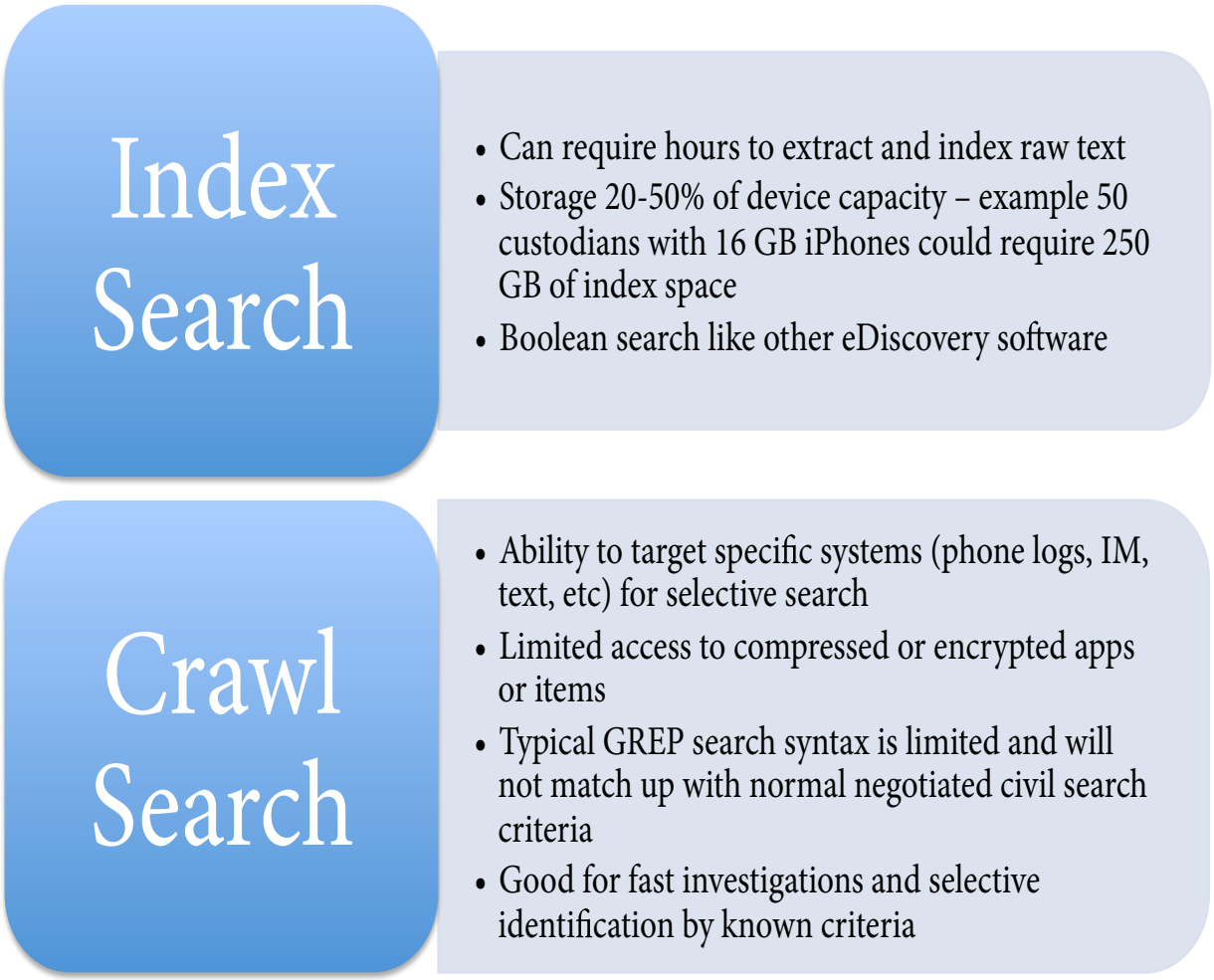
Mobile ESI Acquisition Methods



Working With Mobile Device ESI

Once mobile device content is collected, the next step is to use the information for its intended purpose, e.g. review for legal responsiveness or privilege, or find information related to regulatory or internal investigations. Most collection software creates one or more forensic container files that must be processed to extract tables and file objects such as photos, emails and more. A very few mainstream eDiscovery platforms (AccessData, Guidance, Nuix and Clearwell to date) have built connectors to directly ingest these packages for search and review. The majority of users extract selective ESI from individual mobile devices container files using either full index or live crawl searches. A crawl type search usually targets specific tables or files and attempts a pattern match to specific names, numbers or single terms.

Mobile Device ESI Extraction



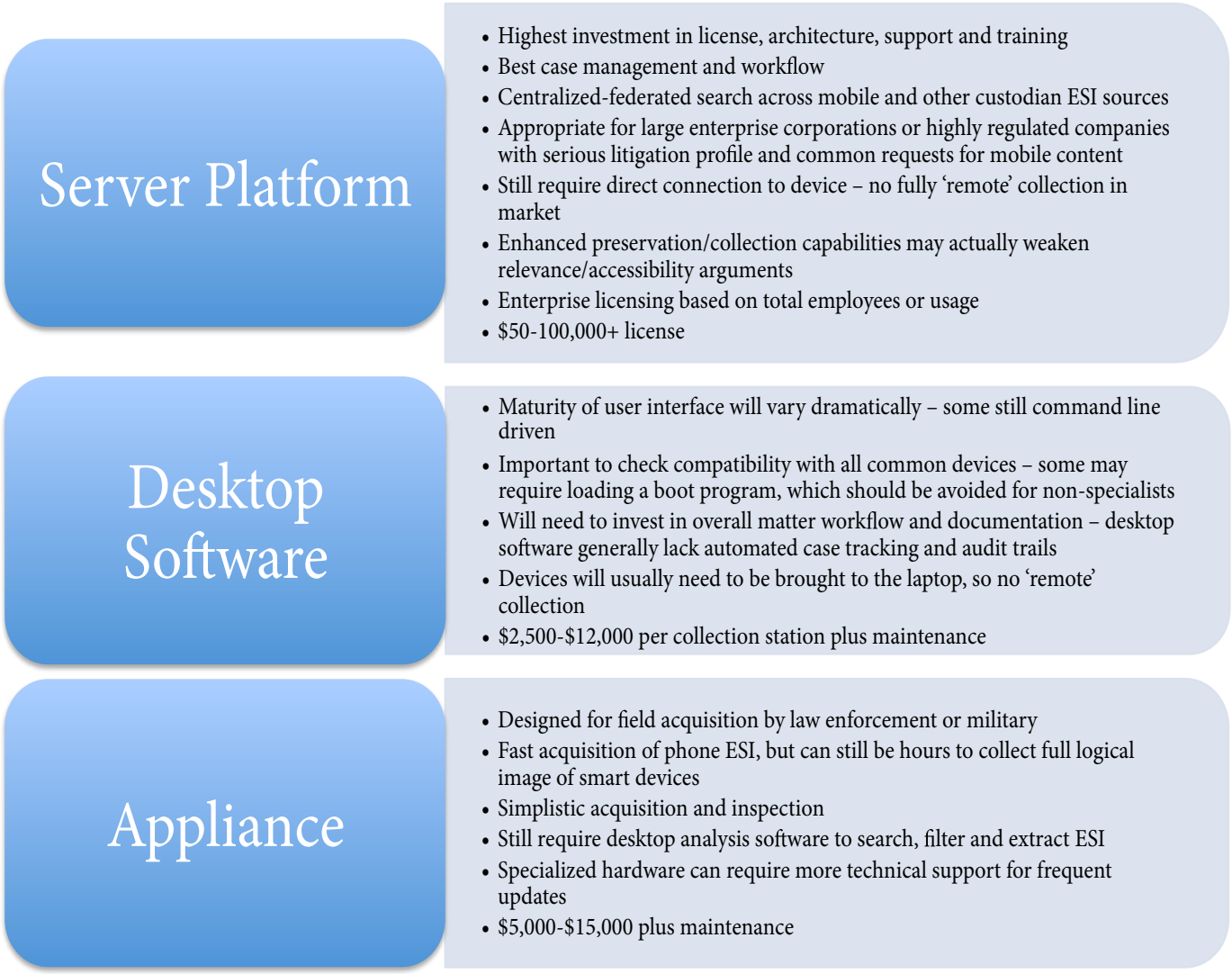
Mobile Device Collection Tool Approaches

There are three main types of tools for collecting mobile device content – server platform, desktop software, and appliances. Each approach has unique considerations that any organization should consider before making a decision. As with any technology investment, you should first calculate your current or potential costs and time attributed to mobile device discovery.

Example: If your average matter has 10 custodians, then you could incur $5,000-7,500 for a service provider to perform collections that will result in 160-640 GB of container files for processing and review.

With these kinds of outsourced costs, it is little wonder that corporations are evaluating technology, staff and process to manage this in-house. Mobile devices are still a relatively new discovery target and many counsel will ignore them or agree that they are not relevant to avoid the complexity and cost. With more and more unique content residing on these devices, it is only a matter of time before they must be handled as a normal part of a mature discovery workflow.

Mobile ESI Acquisition Tools



In thinking about how to collect mobile device content, do not overlook the human element of mobile discovery. As the eDJ data showed, many organizations simply bring in a third party expert to conduct mobile discovery. There are certain technical skills that will be required and there will be training and education needs. Not every organization will have the wherewithal to employ that expertise internally.

Processing Mobile Device ESI

Once all or selective data is extracted from the collection container files, it will need to be manually reviewed or processed for loading into a review platform. The discovery team should evaluate the relevance scope to determine what can be excluded or included by type, identity or other criteria. For smaller collections, processing and review may be more efficient using investigative software directly on the forensic containers. Conversion of larger collections into more traditional load files with attached files may be more efficient.

Review and Production of Mobile Device ESI

Most review platforms do a relatively poor job of presenting mobile content compared to more traditional email and files. Much of the unique mobile content is stored in tables or logs. Just like databases, these content types may be better handled by a technical specialist who can craft searches or reports that retain the context of entries. Analytics such as chronology, social networking and time/location mapping can be exceptionally useful in extracting key evidence, but they will require specialized tools and support.

As you might imagine, traditional production of mobile content in load file, TIFF images and text may not be acceptable for requesting parties. eDJ strongly recommends early discussions to agree upon a production format, whether extracted-selective forensic containers, native files or hybrid native-image productions.

Mobile Device Discovery Requirements In The Modern Corporation

The ability to conduct mobile device discovery is certainly a requirement for any organization that wants to be litigation ready. What this report has described so far gives you a primer on what kinds of data you might encounter and how to collect, process, and produce that data.

Mobile device data, though, exists in a corporate environment where there are many other types of data scatter across diverse systems. Many organizations struggle with information governance initiatives because of the boil-the-ocean nature of such a broad topic. Future eDJ reports will examine how to manage mobile device content within the context of the BYOD (bring your own device) paradigm, the world of apps and email, and increase in social media usage. We will examine the mix of policies, processes, and technologies required to make information governance of mobile device content a reality.

In the meantime, if you are considering conducting some or all of your mobile device discovery in-house, the following are some minimum requirements for the typical corporate discovery lifecycle.

- Ability to collect unique mobile device ESI from dominant three OS platforms
  - iOS – Apple – iPhones, iPads
  - Android – phones and tablets
  - Blackberry – if still in use
- Ability to acquire logical image of device in 2-4 hour period - minimize custodian impact
- Minimal user training or software certification for device collection – authentication of evidence
- Search and inspection of device image/container files – in-house investigation and ECA capabilities are criti-

cal to relevance decisions and scope management
- Filter by type/date/names – the vast majority of devices are user owned and personal data should be filtered out of collections as early as possible
- Extraction of ESI – metadata, content items, chain of custody information on collection

This report provides an overview of the challenges to mobile device discovery and a framework for addresses these challenges. The next eDJ reports in this series will focus on managing mobile content at the enterprise level and deeper dives into implementation of in-house discovery solutions.

About The eDJ Group

eDJ Group offers unbiased information and pragmatic advice, based on years of experience and proven industry best practices. Whether researching a technology or service solution, conducting an eDiscovery Bootcamp or finding the right expertise to answer your specific questions, eDJ Group is the source for all eDiscovery professionals.

We are committed to helping eDiscovery professionals get the information necessary to excel in their professions, rather than offering legal advice or counsel. We operate with the utmost integrity and commitment to our clients on these guiding principles:

- Independence – All research, reports, advice and services are agnostic and conducted independently without influence by sponsors.
- Highest Ethical standards – All content is honest perspective based on real experience and interactions with thousands of practitioners; detailing both successes and failures without favoritism.
- Pragmatic, Experienced Expertise – All services are conducted by industry experts with decades of experience in eDiscovery and strictly vetted by the eDJ Group founders.

For further information about the eDJ Group and their research, please contact Barry Murphy (barry@edjgroupinc.com) or Jason Velasco (jason@edjgroupinc.com).