



## Smartphones and BYOD Impacts on Discovery

The importance and potential obligations attorneys face in including smartphones in discovery requests as well as the collection and analysis of these modern data sources.

---



Lauren Black  
BoyarMiller



John Myers  
Chorus Consulting



Richard Clark  
ESI Analyst

## Meet the Panel

# Modern Data Growth

1

Mobile device use is one of the primary factors expected to drive ediscovery through 2023 and beyond.

2

Smartphones account for 40% of global communications, the primary focus of both criminal and civil discovery.

3

Chat, messaging apps and collaboration tools account for over 18M messages being sent per minute every day.



<https://www.marketsandmarkets.com/Market-Reports/e-discovery-market-11881863.html>

[https://www.americanbar.org/groups/professional\\_responsibility/publications/professional\\_lawyer/2016/volume-24-number-1/forensic\\_examination\\_digital\\_devices\\_civil\\_litigation\\_legal\\_ethical\\_and\\_technical\\_traps/](https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/2016/volume-24-number-1/forensic_examination_digital_devices_civil_litigation_legal_ethical_and_technical_traps/)

# Modern Data Growth

## Messages Sent per Minute in 2019

SOCIAL MEDIA POSTS



SMS & MMS MESSAGES



COLLABORATION TOOLS



MESSAGING APPS



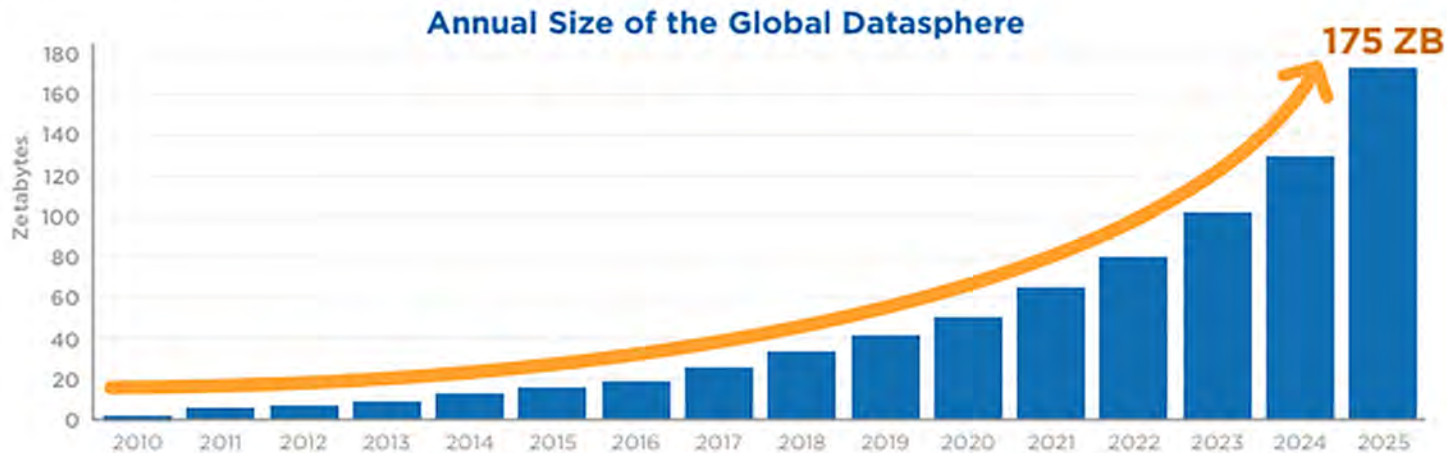
\*Sources: Slack and Collaboration tools estimated using 3 messages per minute average across 10 million users:  
Slack: <https://searchunifiedcommunications.techtarget.com/news/252456752/Number-of-daily-Slack-users-surpasses-10-million>  
Facebook: <https://zephoria.com/top-15-valuable-facebook-statistics/>  
Twitter: <https://www.dsayce.com/social-media/tweets-day/>  
LinkedIn: <https://blog.hootsuite.com/linkedin-statistics-business/>  
Internet Minute: <https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/>

# Modern Data Growth

150 billion devices will be connected across the globe in 2025, most will be creating real-time data.

This "always-on" and "sensorized" world is creating data 24x7, anticipated to reach 175 zeta bytes by 2025, **all of it subject to discovery!**

Figure 1 - Annual Size of the Global Datasphere



Source: Data Age 2025, sponsored by Seagate with data from IDC Global DataSphere, Nov 2018





*Perspectives from Counsel*



## Civil Litigation

- Labor and employment
  - Departures to competitors
  - Breach of fiduciary duty
  - Trade secrets misappropriation
  - Employment discrimination
  - Wrongful termination
  - Overtime, Fair Labor Standards Act issues
- Catastrophic personal injury
- Family law
- Contract cases and beyond



## Ethical Rules for Attorneys

- **Duty to be competent** in handling discovery of ESI
- Model Rules of Professional Conduct, Rule 1.1 (“Competence”), Comment 8:  
*To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.*
- Multiple areas where competence can be questioned





## Ethical Rules for Attorneys – cont'd

- **Supervisory responsibilities**—Model Rule of Professional Conduct 5.1, 5.2
  - *A **lawyer shall be responsible** for [another lawyer's or third party's] violation of the Rules of Professional Conduct if: . . . (2) the lawyer . . . has direct supervisory authority over [the other lawyer or third party], and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action*
- Also keep in mind . . .
  - Spoliation
  - Ethical collections
- Upshot? Stay current.



## What CAN Employers Do?

- Employers have a right to establish as **conditions of employment** . . .
  - No privacy as to communications on the employer's network
  - Return devices upon termination
  - Searches of devices upon termination
  - **Both personal and private?**
- Other security protocols:
  - Acceptable use policies
  - Password protection requirements



## Discovery into Cellphones—Do Courts Allow It?

- **Proportionality** is the overarching theme.
- Federal Rule of Civil Procedure 26(b)(1) (as amended on December 1, 2015)
  - *Parties may obtain discovery regarding information that is relevant to a party's claim or defense and proportional to the needs of the case . . . .*
- Factors:
  - Importance of the **issues at stake** in the action
  - **Amount** in controversy
  - Parties' relative **access to relevant information**
  - Parties' **resources**,
  - **Importance** of the discovery in resolving the issues, and
  - Whether the burden or expense of the proposed discovery **outweighs its likely benefit**

## Discovery into Cellphones—Do Courts Allow It?

### Car Accident

#### YES –

- Specific testimony regarding use.
- Limited inspection.

148 So. 3d 163(Fla. App. 2014)

#### NO –

- Mere possession insufficient.
- Nothing unique in bare argument that driver was distracted.

5 Pa. D. & C.5th 1, 7 (C.P. 2012)

### Trade Secret Misappropriation

#### YES –

- Plaintiff testified he accessed confidential info.
- Neutral third party.
- Protective Order.

2020 U.S. Dist. LEXIS 62200 (E.D. Pa. 2020)

#### NO –

- Rejected argument that Protective Order guarded data.
- No relevancy evidence.
- Narrower means available.

5 Pa. D. & C.5th 1, 7 (C.P. 2012)

## Tips Regarding Cell Phone Discovery

- Make sure to exhaust all “less intrusive” means
  - Interrogatories
  - Deposition questions
  - Information, not devices
- Keep critical limitations intact
  - Custodian
  - Recipients
  - Time frame
  - Subject matter
- Don’t necessarily start with subpoenas



Chorus Consulting LLC

*Forensic Collection Perspective*





1

More volatile than a computer hard drive

2

Ability to recover and extract information that is not readily available

3

Expert review may determine potential relevance data associated with personal information vs company information

## Mobile Device Evidence



## Information of Interest

- Text Messages
- Chats
- Call logs
- Contacts/address books
- Photos
- Videos
- Notes
- Recorder memos
- Saved documents



- Voicemails
- GPS Locations (geolocation)
- Calendars
- Internet history
- Search engine history
- Social media artifacts
- Device logs
- User activity metadata
- Third-party applications

## Collection In Person or Remote

### Physical Collection

Project need or requirement

Device limitations

Potential Additional Cost

Deferred analysis



### Remote Collection

Coordinated from Lab

Social Distancing Era - provides protection to investigator and the custodian (Health Conscious)

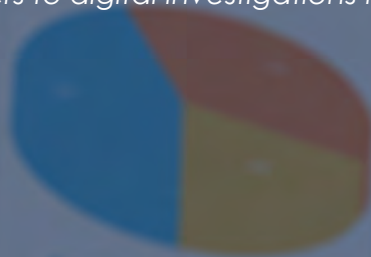
Cost Effective

- Expert/Professional Consultants
  - Solidify results
  - Methodology
  - Testifying / Declaration
- Assessment
  - Content
  - Reporting
- Data
  - Securing / Acquisition
  - Protection
  - Recovery
  - Remediation



# esi<sup>i</sup>analyst™

*Lowering the barriers to digital investigations for modern data*





- **General Litigation:** Internal chat and collaboration like #Slack, Teams etc.
- **Employment Litigation:** Computer activity, communications and geolocation can tell the story of employee activity.
- **White Collar:** Stack together all available data to create the timeline
- **Financial Investigation:** Analyze all financial records to follow the transactions.
- **IP Theft or Phishing Scams:** Computer activity and geolocation can pinpoint originations of nefarious activity.







- **Cyber Attack:** Analyze all computer activities, communications around the incident.
- **Product Liability:** Compare internal communications with structured data reports for fast analysis around product development and creation.
- **Insurance Claims:** Compare claims to plaintiff activity with geolocations, social media etc.
- **Internal Investigations:** Stack all data for the key players to identify communications and activity.



# Bios

## Panelist

### Lauren Black

Skilled Litigation Associate with 8+ years experience representing clients in both state and federal court proceedings, arbitrations, mediations, contract negotiations, and informal settlement negotiations. By working in a firm environment, I have become well-versed in all matters of Business Litigation, including specialized experience in Labor and Employment Litigation, as well as contract disputes. I am a persuasive and strong advocate in and out of the courtroom. Doctor of Law (J.D.) from Georgetown University Law Center, BA from Duke University. Dedicated Houstonian, global traveler, and sports enthusiast.

[LBlack@boyarmiller.com](mailto:LBlack@boyarmiller.com)

[www.boyarmiller.com](http://www.boyarmiller.com)

## Panelist

### John Myers

An eDiscovery and Digital Forensics professional with over 25 years of experience assisting clients with solutions in various industries including IT, electronic discovery, consumer goods and hospitality.

He holds a B.A. in Business, has held leadership positions in several large consulting firms and worked with over 100 law firms and corporations. He holds several industry certificates of training and is a licensed Private Investigator/Qualified Manager in the State of Texas.

[john.myers@chorusconsulting.net](mailto:john.myers@chorusconsulting.net)

[www.chorusconsulting.net](http://www.chorusconsulting.net)

## Panelist

### Richard Clark

Mr. Richard "Rick" Clark began his career in Orlando serving the legal community in a full spectrum of discovery and data related services. As the industry evolved to adopt technology with the growing needs in including data as a part of the discovery process, He expanded his technology skill set to include information governance, litigation readiness, and analytics applications spanning platforms and workflows that encompass the full spectrum of the EDRM.

[rick.clark@esianalyst.com](mailto:rick.clark@esianalyst.com)

[www.esianalyst.com](http://www.esianalyst.com)

# Question / Answers

- **Why isn't this tested on bar exam or MPRE?**
  - Bar tests vary from state to state, and it's been about nine years since I took mine! I would not be surprised if ESI-related testing material shows up, if it has not already.
  - {Can be viewed in our recorded Questions & Answer session}
- **How do you deal with preservation issues if you don't start with a subpoena and the employer disclaims possession, custody and control?**
  - Preservation duties and duties to avoid spoliating potentially-relevant evidence inhere to parties regardless of subpoenas, and emerge as soon as litigation is reasonably anticipated. There are, however, a lot of tactical considerations to keep in mind before deciding how to proceed.
  - {Can be viewed in our recorded Questions & Answer session}
- **What do you advise clients for BYOD policies and/or what are you seeing in terms of the spectrum of employers' approaches to BYOD?**
  - BYOD policies are inherently client specific—how aggressive they are depends on a client's jurisdiction, business, strategic outlook, and specific concerns. There is no one size fits all. Feel free to pop me an email—lblack@boyarmiller.com--to discuss your specific needs further!
  - {Can be viewed in our recorded Questions & Answer session}
- **Do they claim the right to do a factory reset?**
  - This is an aggressive approach with BYOD devices, given the amount of personal information that will likely be on the device.
- **Do they install software to isolate work apps and only deal with that work data on the device?**
  - While not yet widespread, I can see this practice becoming more pervasive with devices used for both work and personal functions.
- **Is there any pressure being placed on device manufacturers to have functionality allowing multiple profiles on mobile devices (such as iPhones and iPads) so that work data can easily be partitioned from personal data for BYOD devices?**
  - I am not aware of such efforts, but they would not surprise me.

# Question / Answers

- **Are cell phone communications (texts, emails, files) considered Records that would be subject to an InfoGov policy of Records Management? If so, then regular disposition of data according to an entity policy would not be spoliation?**
  - Given the prevalence of portable digital devices, it is no surprise that many employees are using their own personal devices to perform work for their employer. This practice is often referred to as Bring Your Own Device or BYOD. BYOD raises many issues and concerns for records management practices (e.g., security and privacy).
  - ISO 15489, the international standard on records management, defines records as: "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business". Texts, emails and files stored on a mobile device could be considered "records" but likely duplicates of files that are also stored within the organization's enterprise.
  - "Spoliation" of evidence is the destruction, disposal, or erasure of evidence such that it becomes irretrievable and unable to be produced when needed in the course of litigation. To avoid "spoliation," counsel should send spoliation letters (also called "preservation" letters) to defendants and even non-party witnesses to inform them of their duty to preserve potentially relevant evidence that may be stored on mobile devices.
  - {Can be viewed in our recorded Questions & Answer session}
- **Were you saying that a personal phone could be accessed by the employer for certain types of investigations either during employment or upon termination?**
- **Can you elaborate on the legal basis to collect and inspect a person's personal phone. Do you rely upon the consent of the individual? If they object, what recourse do you have?**
- **Do you find that this guidance won't work in the EU or other jurisdictions with different privacy requirements and perspectives?**

# Question / Answers

- **When you are expecting your opposing counsel to be collecting cell phone data (and you don't ask for the whole phone), what questions should you be asking opposing counsel about what they are doing to collect and search?**
  - {Can be viewed in our recorded Questions & Answer session}
- **Can hacking tools such as Wireshark steal metadata from one's smartphone while I am sitting at a coffee shop? Wireshark is used to steal data from computers. But what about smartphones?**
  - From Wireshark's website - "Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions."
  - By design, if your smartphone is connected to a network that is being monitored by the Wireshark tool, the data that the tool is monitoring and analyzing could be intercepted.
- **Which hacking tool can steal metadata from a smartphone user that is sitting at a coffee shop?**
  - This is not a question being addressed in this presentation, but John Myers may be able to answer in a direct conversation
- **Can deleted info: texts, photos, chats be recovered/discovered?**
  - Depending upon how the data was stored upon the device, how it was deleted and in some cases the elapsed time - yes deleted data may be able to be recovered.
  - {Can be viewed in our recorded Questions & Answer session}
- **Which security app can I install on my smartphone that will prevent someone else sitting at a coffee shop from stealing the metadata on it?**
  - This is not a question being addressed in this presentation, but John Myers can answer in a personal conversation

# Question / Answers

- **What forensic tools do you recommend as far as collecting mobile phones remotely?**
  - The leading mobile forensic tools, like Cellebrite, Oxygen and XRY, have various options for collecting mobile device data. In some cases it is not the tool, but the process and methodology that the professionals have developed that allows for the capability. Most professionals have several tools to accomplish the task at hand.
  - {Can be viewed in our recorded Questions & Answer session}
- **How can SMS/MMS texts or other data be retrieved from an iPhone after it is factory reset by the custodian?**
  - Our experience has been that once a device has been factory reset, no data can be retrieved from the device.
- **How do you approach production of phone data, for example, chats, where there is effectively one "document" -- the export from the chats. Isn't producing only the relevant chats altering a document?**
  - Much of the data stored in a mobile device is stored in small databases, especially chats, texts, etc. A chat is made up of numerous records and thus not a "document", therefore the exporting of only the relevant chat records is not altering any document.
- **Can you produce all the text messages in a conversation thread together to keep the conversation intact?**
  - Yes, all of the text messages in a conversation thread can be kept together maintaining the conversation.
  - {Can be viewed in our recorded Questions & Answer session}
- **How do you protect personal information when extracting data from someone's personal cell phone? That is, during data extraction, you may also extract unrelated texts, photos, and other personally embarrassing, and wholly unrelated data.**
  - The protection of personal information is a combination of process and technology. We have had numerous conversations with individuals and counsel regarding what is to be extracted and provided.



# Question / Answers

- **Since different tools find different data, do you recommend that clients use more than 1 tool to extract and review data if it is a highly important case?**
  - While the leading mobile forensic tools have similar features and functionality, the use of more than one (1) tool to extract and review data may be advised. In most cases the data is readily extracted however a secondary tool may need to be deployed to perform deeper analysis.
- **Third party app such as WhatsApp have numerous deletion features that a user can utilize to obliterate activity. What best practices do you use to capture all messages?**
  - With applications such as WhatsApp, collecting not only from the device but the apps servers may be necessary. All options should be explored.
- **If someone is using SnapChat (or Wickr, Slingshot, Yovo, ClipChat, CyberDust, etc.) are the chat records really gone? Is there any way to retrieve those conversations?**
  - Depends on the setting that were used when installing the app on the device. Additional analysis of the smartphone or another associated device (i.e. a computer that may have accessed the account)
- **How do you access a phone that is password protected if the owner has died? Like in a wrongful death suit or a car wreck?**
  - There are services that have the ability to unlock devices and provide the credentials to access the data. However this is not a solution for every situation. It greatly depends on whether there is a legal reason to access the data and if a Court has provided the authorization to do so. Otherwise authorization from the next of kin to perform the service may be required.

# Question / Answers

- **Have you ever had anyone intentionally lock their phone out so you can't access the data? What do you do to unlock the phone?**
  - Yes, we had a custodian intentionally lock herself out of her phone (she forgot the password) in an effort to keep from turning over damning evidence. The Court had the Custodian write down all of the passwords she could remember, then her Attorney, opposing Counsel and Forensic Expert attempted the other passwords without success. This was an iPhone that eventually disabled the device after 10 incorrect attempts.
  - The Court then had to prepare an Order so that we could send the device to Cellebrite to be unlocked. This is a \$5,000 service that must be paid upfront, regardless of whether they are successful or not. This is also an activity that can take a day, a month, a year, or a decade. There is no way to determine how long it will take to run the unlocking algorithm and successfully access the device.
  - {Can be viewed in our recorded Questions & Answer session}
- **Can you get access to someone's phone from iCloud?**
  - Cloud collections are becoming a more widely used norm in this day of Social Distancing and virtualization. Utilizing one of our several collection tools combined with some personal interaction with the Custodian, we can virtually collect cell phone data from the Cloud environment
- **Are there resources for expert testimony to explain and introduce the information obtained from a phone in court? Is this something that ESI Analyst does?**
  - These are services that BoyarMiller or Chorus Consulting offer.