The top trends redefining Law Enforcement
Table of contents

03 Executive Summary
08 In the Field
11 In the Lab
19 In Investigations
24 Management and Compliance
27 Conclusion
Executive Summary

In 2019 Cellebrite published the first Digital Intelligence Benchmark Report for law enforcement. The purpose of this benchmark report was to shed light on the role technology plays in solving crimes today and how it can enhance digital intelligence practices.

This year we’ve focused our 2020 Annual Digital Intelligence Benchmark Report on where agency managers are with driving agency transformation for digital policing. In addition, we examine the trends affecting investigators and examiners in the lab, in the field, and throughout the digital investigative process.

The benchmark report reveals some fascinating statistics, but more importantly, it begins to create a road map to the future of policing by highlighting the technologies that will decrease data overload and the solutions that will expedite time to evidence in the future so that investigative teams can solve crimes faster and keep communities safer.

KEY FINDINGS

Agencies Recognize The Growing Role Of Digital Data But Are Slow To Adapt

Digital data is proving to be more informative and crucial when solving law enforcement cases than physical evidence. Cellebrite’s benchmark report reveals that 64 percent of agency managers see digital investigations playing “a very high role” in keeping communities safe. Thus, with more than 82 percent growth in the role of digital data from devices compared to three years ago, the need for a highly-trained staff to be able to navigate and leverage vast amounts of data has risen considerably. Yet, as much as 43 percent of agencies report either a poor or mediocre strategy or no digital intelligence strategy at all.

Lack of Comfort Highlights Need for Faster Extraction in the Field

Digital evidence captured at the scene of a crime from witnesses and victims with consent-based authorization often contains valuable insights. However, the current means of capturing this digital evidence presents a problem to investigative teams. The survey revealed that over 70 percent of officers are still asking witnesses and victims to surrender their devices so evidence can be extracted at the station or in a lab. However, most people do not want to have their primary communication device taken away for an indefinite period. To combat this issue, 67 percent of agency managers believe that mobility technology is “important” or “very important” to the agency’s long-term digital evidence strategy and 72 percent of investigators believe it is important to conduct in-the-field extractions of this data.
Agency Managers Are Looking At Modernization Initiatives Such As ‘Digital Hubs’ And ‘Mobile First’ To Help Attract A New Generation Of Digital-Savvy Officers.

Eighty-four percent of agency management rate mobility technology (i.e. Mobile First) as being important to their long-term digital intelligence strategy. As the next generation of tech-savvy frontline officers begins to leverage technology at crime scenes, a new level of investigative effectiveness is becoming possible. Most agency managers believe police forces that embrace mobile technology to collect digital evidence in the field will help reduce turnover and be significantly more prepared to meet the digital evidence challenges of 2020.

Budget And Overtime Constraints Limit Digital Investigation Efficiency

With the deluge of digital devices, examiners face an average three-month backlog and an average backlog of 89 devices per station. In order to address these backlogs, examiners increasingly prioritize and only examine time-sensitive data or data from certain cases.

Budget constraints mean working overtime is no longer an option, as seen in the nearly 20-percent decrease in overtime hour allowances in the last year. For this reason, the need to prioritize digital intelligence analysis and management has risen to 40 percent this year, in comparison to 25 percent last year. As reported, the biggest challenge labs face continues to be locked devices and encrypted apps, as 6 out of 10 devices that reach the lab are locked.

Lab Examiners Are Drowning In Data And Device Overload

Cellebrite research shows the number of data sources is continuing to grow for examiners. On average, each case has 2-4 mobile devices that need to be examined, while 45 percent of cases will also involve a computer examination. This means examiners typically conduct 26 mobile-device examinations monthly, translating to more than 300 annually.

Smartphones continue to top the list as the most frequent evidence sources examiners review, but the variety of digital sources used in investigations is increasing. Sources such as CCTV, wearables, smart home & IoT devices, drones, cars, and even gaming systems, are being used by criminals more frequently to mask illegal activity. This is why leveraging technologies that can access the most data sources, and technologies such as artificial intelligence to shorten the amount of time it takes to generate actionable insights, are so important.
High Demand For Digital Data Analytics For Investigations

Investigators and examiners are facing severe challenges in managing the exploding abundance of digital data against the backdrop of budget cuts and a shortage of overtime allowances. This has led to an increasingly large backlog and a need to prioritize casework. Yet despite these glaring challenges, only 25 percent have adopted digital analytics tools.

While past mobile-device storage was limited to a less than 16GB, the new generation of devices have storage capacities reaching as high as 1TB (1,000GB). Despite the backlogs, variety of digital sources, and the amount of digital data that typically need to be reviewed in an investigation, the vast majority of law enforcement agencies are reviewing this information manually instead of using AI-based analytics solutions. This means, on average, investigators spend 43 hours per week reviewing and reporting on evidence. This accounts for 96% of their average workweek hours, up from 37 hours in the prior year.

Putting A Process Around Storing And Sharing Digital Evidence Is A Key Concern Of Agency Managers

In our benchmark report, 64% of agency managers said that governance and management of data is “very important.” This is particularly important due to the large amounts of data that need to be maintained. If data is mismanaged, it can quickly be misplaced in various storage solutions. A thumb drive can be misplaced. The data may not be stored in the proper place on a server. The data could be stored in a staff member’s individual storage component. A staff member may no longer be employed and it becomes very difficult to determine that person’s storage solution.

This benchmark report, in which more than 2000 law enforcement personnel were surveyed, paints a compelling picture of where the needs of agency leaders and investigative teams stand today. There is a pressing need for a solid digital intelligence strategy to be put in place to balance the digital data reality and needs with available, finite resources. Only when such strategy is put in place will law enforcement agencies be positioned to meet today’s tactical challenges while also preparing for tomorrow.
A Deeper Look Inside

METHODOLOGY
The benchmark report was conducted online and sent to a global audience of known law enforcement members. The first question in the benchmark report asked recipients to identify their roles within their organizations. The four roles they could choose from were:

- Investigator
- Examiner
- Agency Manager
- Prosecutor

RESPONSE
Over 2000 law enforcement personnel completed the benchmark report with the majority of responses coming from examiners and investigators. The responses and the volunteered comments provided valuable insight into the daily professional lives, trends, and challenges of law enforcement, and how Cellebrite should develop solutions to better service the community going forward.

Armed with the information gathered from the benchmark report, Cellebrite can hopefully direct future innovation toward areas that will have the most impact to accelerate time to evidence and expedite the resolution of investigations.

KEY FINDINGS
Some of the more important points gathered from the benchmark report included the following:

- 90% of cases involve smartphones as the main evidence source.
- The variety of digital sources used in investigations is increasing. Sources, such as wearables and smart-home technology, are being used with more frequency during investigations.
- 6 out of 10 devices that reach the lab are locked.
- Extracting data from encrypted apps is the biggest challenge, aside from locked devices.
- Law enforcement agencies are averaging 3-month backlogs on investigations.
- One in every two cases requires access to cloud-based data.

Despite the backlogs, variety of digital sources, and the amount of digital data that typically needs to be reviewed in an investigation, the vast majority of law enforcement agencies are continuing to review this information manually instead of using AI-based analytics solutions.
Access
Extract data from the most devices, digital platforms, and applications - anytime, anywhere.

Manage / Control
Empower your entire organization with the relevant evidence in a secure and collaborative system.

Leverage
Provide actionable intelligence to key stakeholders that reveal critical insights fast.

DIGITAL INTELLIGENCE ECOSYSTEM

Artificial Intelligence
Digital Evidence Management
Data Storage
Management & Compliance
Investigation

Field
In the Field
In the Station
In the Lab

Prosecutors
Agency Management
Lab Practitioners

Investigators
In The Field

Consent-based extractions from witnesses and victims conducted at the station or in the field are critical for investigators. Of those surveyed, 72% of investigators responded by saying it is important to conduct in-field extractions of this data. However, the current means of capturing this digital evidence presents a problem to investigative teams.

Challenges

Currently, the primary way that first responders collect this data is by asking witnesses/victims to surrender their devices for extractions. Most people do not want to have their primary communication device taken away for an indefinite period of time.

Add to this the fact that labs are already operating beyond capacity and running three months behind on average, and it’s clear that sending more and more devices from witnesses and victims will only worsen the bottlenecks.

Solutions

To avoid lab slow-downs, mobile technology should be used to empower first responders to gather consent-based data from these devices at the scene of a crime. In the benchmark report, 67% of agency managers said they believe that mobile technology is “important” or “very important” to the agency’s long-term digital evidence strategy.

Collecting evidence on site will relieve bottlenecks in the lab while also surfacing critical insights much faster. Data will be able to be seen in context with the case at the crime scene, allowing potential suspects and incriminating digital evidence to be factored in much faster. Frontline officers could surface the suspect’s or victim’s journey before and after the crime, and a data-driven investigation could immediately commence.

Ultimately, modern police forces that embrace mobile technology to collect digital data in the field will be significantly better prepared to meet the digital evidence challenges of 2020.
How important is it to you to be able to have mobile device extractions at the scene of a crime?

2020: Global avg of Investigators

- 0%
- 10%
- 20%
- 30%
- 40%
- 50%
- 60%
- 70%
- 80%
- 90%
- 100%

72%
How do officers currently collect digital evidence from victims/witnesses in the field?

**KEY TAKEAWAYS**

- 75% of investigators said that gathering digital evidence at the scene of the crime is critical for investigations.
- Asking witnesses and victims to give up their devices for indefinite periods of time for examination doesn’t work.
- On average, labs are backlogged 3 months on phone examinations. Adding more devices to their workload will only increase the bottlenecks.
- First responders need to be equipped to gather consent-based data from devices at the scene of a crime quickly and easily.
- **Cellebrite Frontline** empowers first responders to quickly and easily collect this data.
- Data can be seen in the context of the case at the crime scene, and potential suspects and incriminating digital evidence can be factored in much faster to streamline the digital investigation process.
Lab practitioners are being buried by requests for device examinations. On average, examiners conduct 26 mobile device examinations monthly, translating to 300+ annually—up 20% from the prior year.

With the deluge of digital devices, backlogs continue to average three months (unchanged from last year) with departments reporting an average backlog of 89 devices.

Locked phones, encrypted devices, and weeks needed to get answers to warrants for cloud-based data are huge impediments.
Challenges

In order to reduce backlogs, examiners are being forced to prioritize and only examine data from certain cases or swiftly run through examinations to examine only certain data.

Data doesn’t just live on devices, however.

The benchmark report results show that one in every two cases require accessing data stored in the Cloud. Agencies are beginning to realize the importance of accessing this critical data source.

To access this data, 48% of practitioners worldwide [72% in North America] submit warrants to the relevant tech companies.

The problem is that it can take nine weeks on average to receive the data from a warrant return. And when data arrives it may either be scant or in such volumes that time must be spent to sort it all out, which slows investigations down even further. Others are manually accessing public data on cloud sources using a social media account, which can be very time consuming.

Locked devices and encrypted apps remain the greatest challenges faced by lab practitioners, with respondents noting that six out of 10 devices that reach the lab are locked—a ratio unchanged from the prior year.

Solutions

Examiners need first responders to take some of the device extractions off their plate. Cellebrite Frontline and Cellebrite Kiosk are two solutions that are empowering first responders to make simple extractions at the crime scene to reduce backlogs and get cases moving quickly.

Encryption and locked-device problems can be quickly overcome using UFED Premium.

Accessing cloud-based data is no longer a problem thanks to UFED Cloud Analyzer, which allows practitioners to extract, preserve, and analyze public- and private-domain social-media data, instant messaging, file storage, web pages, and other cloud-based content using a forensically sound process. Easily search, filter, and sort data to quickly identify suspects, victims, locations, and more— all within pre-approved legal boundaries.

Finally, only Cellebrite Physical Analyzer supports the most amount of applications, and with tools like Virtual Analyzer, encrypted apps are no longer a challenge.
In the past month, how many mobile device examinations did you conduct?

![Chart showing mobile device examination data]

How backlogged are digital forensic examinations? (in months)

![Chart showing digital forensic examination data]
If you are experiencing backlogs, how do you handle them? (Please select any and all that apply)

KEY TAKEAWAYS

- On average, examiners conduct 26 mobile device examinations monthly, translating to 300+ annually, up ~20% from the prior year’s ~250 average.
- With the deluge of digital devices, examiners still face an average 3-month backlog—unchanged from last year.
- In order to address these backlogs, examiners are increasingly prioritizing and examining data from certain cases or certain data.
In the past year, how frequently did the following evidence sources appear in your investigations?

- Smartphone: 92% (2019), 97% (2020)
- Computer: 65% (2019), 53% (2020)
- CCTV: 40% (2019), 36% (2020)

What percentage of your cases involve/require access to data stored on cloud sources (such as Facebook, Gmail, Dropbox, etc.)?

- 2019: Global Avg 40%
- 2020: Global Avg 50%

**KEY TAKEAWAYS**

- The number of data sources continues to grow. Smartphones continue to top the list for most frequent evidence source. However, there is a growing list of other devices that also need to be examined for critical evidence: Computers, CCTV, Tablets, SD Cards, Wearables, Gaming systems, IoT, Drones, Skimmers, GPS devices, and others.

- Data doesn’t just live on devices, however, and agencies are starting to realize the importance of accessing this critical data. One in every two cases involve access to data stored on cloud sources.
How do you gain access to data stored on cloud sources?

- I utilize a forensic tool that gives access to private and public sold data: 13% Very often, 7% Often, 9% Somewhat often
- I manually access public data from cloud sources by utilizing a social media account: 18% Very often, 8% Often, 11% Somewhat often
- I submit a warrant for data from the relevant tech companies: 31% Very often, 9% Often, 8% Somewhat often

If you submit warrants to relevant tech companies, how long on average does it take to receive the data? (in weeks)

- 2020: Global Avg 9 Weeks

**KEY TAKEAWAYS**

- To access cloud-based data, practitioners most often submit warrants to the relevant tech companies. However, it takes nine weeks on average to receive the data from a warrant return.
- Manually accessing public data on cloud sources using a social media account is also very time-consuming.

Going forward, as the amount of data in the Cloud continues to grow, practitioners will need better tools that can easily and quickly extract public and private cloud data to assist in investigations.
In the past three months, what percentage of devices that reached your lab were locked?

- **2019: Global Avg**: 59%
- **2020: Global Avg**: 58%

In the past three months, of all phones you examined, what percentage were iOS?

- **2020: Global Avg**: NA
- **NA**: 45%
- **EMEA**: 54%
- **APAC**: 39%
- **LATAM**: 41%
- **LATAM**: 26%
Aside from mobile devices being locked, what are the biggest challenges you face when performing digital extractions?

![Bar Chart]

**KEY TAKEAWAYS**

In addition to the increased volume of devices, locked devices and encrypted apps are the biggest challenges facing examiners.

- Six out of 10 devices are locked, and one in every two devices is iOS.
- 77% cite encrypted apps as their second biggest challenge.
To solve cases today, investigators need an easy way to sort, review, and analyze data that comes from many different sources. While text messages, images, and videos are the most widely reviewed sources, contact lists, location data, and other sources must also be investigated.

Previously, manual review of digital evidence may have been possible because device storage was low. Today, however, new-generation devices have storage capacities above 1,000 GB, which makes manual review impossible.
Investigators are spending more time reviewing evidence than ever before (up to 43 hours per week on average, compared to average of 37 hours per week the prior year). This accounts for 96% of their average workweek hours.

While tools to easily review and analyze the data exist, only one in four investigators said they use a digital analytics tool to review digital evidence—similar to the 26% response rate last year.

In 2020 and beyond, investigators need to utilize artificial intelligence to sort through mountains of incoming data, to automatically find and filter specific objects in images, find keywords in text conversations, and create relationship analysis. Over 70% said that these AI-enabled features would be very important.

Furthermore, since evidence sources continue to grow, investigators will need the ability to unify all the data and view it easily and logically. In the benchmark report, 80% of respondents believe data unification is important while 87% believe viewing activities visually on a map is important.

**Challenges**

- Text messages, images, and videos are the main evidence investigators review.
- With the deluge of data, manual review is quickly becoming impossible. However, only 25% use digital analytic tools.
- Time spent reviewing data is increasing and constitutes over 43 hours per week.

**What data types do you most frequently review in a typical investigation?**
Phone Internal Storage (in GB)

KEY TAKEAWAYS

- Investigators most frequently review text messages, images, and videos.
- While manual review of data may have been possible while device storage capacities were low, and the amount of data was limited, newer devices can hold TBs of data making manual review nearly impossible.

Investigators need better tools to sort, review, and analyze the variety of different data that comes from different sources.
What is your review process for digital evidence? In other words, how do you review the data from forensic extraction(s) for a case?

In the past week, how much time did you spend reviewing and reporting on digital evidence?

KEY TAKEAWAYS

- Despite needing to review overwhelming amounts of data, only 25% of investigators are using digital analytics tools.

- Almost 20% still print extraction reports and mark them up with a highlighter, while others continue to use other outdated manual methods like Excel.

- As a result of digital analytics tools being underutilized, investigators must spend even more time (up to 43 hours per week) reviewing evidence. This accounts for 96% of their work-week.
Solutions

Investigators need to utilize artificial intelligence to sort through mountains of incoming data. AI can also identify objects in images to create relationship analyses and easily filter specific persons.

Over 70% of investigators said that these AI-enabled features would be very important:

• The ability to automatically merge large quantities of disparate mobile, cloud, computer, and telco data sources so users can simultaneously identify patterns, reveal connections, and uncover leads with greater speed and accuracy.
• Collaboration capabilities to share critical case data across departments.
• Advanced image-recognition capabilities to recognize people, places, and objects in images.
• The ability to visualize a suspect’s journey on a map.

**Cellebrite Analytics** automatically surfaces formative leads to discover key evidence in the critical hours of an investigation. With industry-first, custom-media-categorization capabilities, investigators can harness AI to quickly find specific objects in images to speed up their investigations.
Management and Compliance

In the benchmark report, 64% of agency managers said digital investigations play a very high role in keeping communities safe, but collecting, using, and storing digital data is a huge challenge.

The role that data from digital devices plays in investigations has grown 82% in the past three years. The need for more trained staff to be able to leverage the data is very important.
Having a comprehensive Digital Intelligence strategy is important – 34% of respondents have a mediocre or poor strategy, and 9% have no strategy at all.

With increased privacy laws, data compliance is of paramount importance. The failure to comply with data policies can render evidence inadmissible. That is why 95% of agency managers rated data governance and management as “important” or “very important”, higher than the previous year.

The next evolution in digital intelligence is to unify disparate data into one digital intelligence core solution, ensuring the right people have the right access, at the right times.

Challenges

- The role of digital data in investigations is growing quickly—up 82% in just three years.
- Agencies need to enhance their digital intelligence strategy to cope with the changing environment.
- 34% of respondents have a poor or mediocre strategy, while another 9% have no digital intelligence strategy at all!

Compared to three years ago, by how much has the role of digital data from devices grown?

![Chart showing the increase in the role of digital data from devices]
How would you rate your strategy for managing digital evidence?

- 9% rated their strategy as 1 - No strategy at all.
- 10% rated their strategy as 2.
- 24% rated their strategy as 3.
- 33% rated their strategy as 4.
- 21% rated their strategy as 5.
- 3% rated their strategy as 6 - Excellent strategy.

Key Issues for agency managers relating to digital data included:

- Analyzing the growing amount of data quickly and easily.
- Storing digital data.
- Unifying data from digital investigations in one solution.
- Controlling the data with data governance and management.

**KEY TAKEAWAYS**

- The role of digital data in investigations has grown 82% in three years.
- Agencies need to respond by improving their digital intelligence strategy.
- 64% of agency management see digital investigations playing a very high role in keeping communities safe, but collecting, using, and storing digital data in investigations is a very large challenge.
- Having a comprehensive digital intelligence strategy is important – 34% of respondents have a mediocre or poor strategy, and 9% have no strategy at all.

Key Issues for Agency Management include:

- Dealing with and quickly analyzing the growing amount of data
- Storing digital data
- Unifying data into one solution
- Controlling the data
Conclusion

DIGITAL INTELLIGENCE ECOSYSTEM

Access
Extract data from the most devices, digital platforms, and applications - anytime, anywhere.

Manage / Control
Empower your entire organization with the relevant evidence in a secure and collaborative system.

Leverage
Provide actionable intelligence to key stakeholders that reveal critical insights fast.

Access
Extract data from the most devices, digital platforms, and applications - anytime, anywhere.

Manage / Control
Empower your entire organization with the relevant evidence in a secure and collaborative system.

Leverage
Provide actionable intelligence to key stakeholders that reveal critical insights fast.
Implementing a digital intelligence strategy to access, manage, and leverage digital evidence to solve more cases faster and build trust within communities is critical.

Cellebrite's DI Platform provides a complete end-to-end solution that:

- Empowers first responders in the field to access consent-based evidence from witnesses and victims, and allows frontline teams to quickly perform extractions at police stations and border-control checkpoints.
- Ensures lab technicians are equipped with the most advanced tools to access all the digital data, and, when needed, dive deep to thoroughly examine evidence with powerful analytics to review and surface insights.
- Enables investigative teams to leverage AI and machine learning to quickly sort mountains of data to surface formative leads and discover key evidence.
- Provides the means for teams to collaborate to solve more cases faster.
- Helps management easily manage and control digital data to meet all requirements for security and record keeping.
- Ensures the right people have access to the right data at the right times.

Cellebrite also provides world-class training and certification for maximum results.

To learn more about how Cellebrite’s innovative solution can help your team, click here.