Advocating for the Use of Digital Intelligence

How to Leverage Data Effectively and Efficiently During Your Agency's Investigations

Cellebrite

Digital intelligence for a safer world

Executive Summary

Digital evidence has become a driving force organizations use in criminal investigations and is the primary reason many in Agency Management/Command Staff are rethinking the way their organizations use digital data. Agencies are seeing the value in implementing a digital intelligence strategy to manage and leverage digital evidence to solve more cases faster and to build trust within their communities. This paper will describe what digital intelligence (DI) is (and is not) and how an effective digital intelligence ecosystem can harness data to drive actionable intelligence for investigations and overcome many of the challenges agencies are facing today.

Our deep understanding of these challenges comes directly from the feedback we receive from agency personnel every day and from responses to our annual worldwide survey of law enforcement personnel.[1] Many of the statistics referenced in this paper come directly from the survey. This paper will also give examples of real case studies to highlight ways in which various agencies have used DI in the field, in the lab, and throughout the investigative process to solve crimes more efficiently.

The "Partnership to Realize the Benefits of DI" section presents a roadmap to digital policing that is secure, compliant, forensically sound, and one that builds community trust. The conclusion makes four specific recommendations that Agency Management/Command Staff can utilize to advocate for adopting a DI strategy while describing how using DI lawfully and effectively will better protect their communities.

[1] "2019 Industry Trend Survey: Law Enforcement - Cellebrite."

Contents

Foreword

We live in a world where our lives are more closely connected through digital technology than ever before. From phones, computers, and video to wearables and smart homes, technology impacts our lives in ways that only a few short years ago we might never have dreamed possible. The information available at our fingertips is amazing, but many feel inundated with data and unable to make sense of it all.

Law enforcement agencies feel the same effects of data overload. Crimes are becoming more complex and increasingly influenced by technology. From opioids and narcotics to homicides, human trafficking, terrorist threats, and border security, criminals have been quick to adopt digital technology for illicit purposes—and the mountains of data being generated are staggering.

A recent survey of 2,700 law enforcement personnel conducted by Cellebrite showed the value of digital data to investigations.[2] As device and data sources like applications (apps) become more prolific and more data is stored in the Cloud, it becomes increasingly more complicated to follow the data trail and drive actionable insights. And as devices and apps become more sophisticated, criminals are taking advantage of new ways to hide their communications and transactions.

Agency Management must realize that data is now at the forefront of their investigative process, creating actionable intelligence that drives investigations by making clear associations between people, places, and events to solve crimes. The challenge is convincing the public and legislators that digital intelligence, used lawfully, is the most effective way to protect their communities, clear case backlogs, and deal with resource constraints while increasing the effectiveness and efficiency of their force.

Once that support is gained, it then becomes a question of setting up a digital intelligence strategy, getting the right people trained, and establishing best practices to maximize the many benefits that DI can bring, to help keep communities safe. None of this is achievable, however, without a clear understanding of what digital intelligence is and, more importantly, what it is not.

[2] "2019 Industry Trend Survey: Law Enforcement - Cellebrite."

What Is Digital Intelligence?

Defining DI: In simple terms, digital intelligence has two components:

1. **The data** that is extracted from data sources, including smartphones, drones, computers CCTV, apps, cloud, and many other sources. Law enforcement defines this data as "evidence," which, when gathered in a manner that follows the law and is forensically sound, can be used in a court of law.
2. **The process** by which agencies access, manage, and leverage data to more efficiently run their agency..

One of the common misconceptions about DI is that information gathered is then stored and used to build profiles or to drive predictive profiling or policing over time.

Digital intelligence does not promote profiling in any way. It is simply the process of gathering and preserving data (digital evidence) in a lawful manner and ensuring it can be accessed securely by the right stakeholders at the right time during an investigation, just as physical evidence is gathered and stored in the course of a conventional investigation.

This is why it is essential that agencies establish best practices relating to data storage. It's then imperative that the public and legislators clearly understand how this information is used to keep communities safe.

The Reality—The Landscape Has Changed

Cellebrite's 2019 survey revealed that smartphones alone are showing up in investigations 92% of the time.[3] Today, there are over 5 billion mobile devices compared to only 1.5 billon computers being used across the globe. To meet the demands of this changing landscape, law enforcement needs to rethink the way investigations are conducted as well as how digital evidence is shared and used at each stage of the investigation.

As technology continues to evolve, agencies not embracing a DI strategy will see a decline in their ability to keep their communities safe. Law enforcement agencies today have access to the solutions, training, and advisory services to not only keep abreast of technological changes that criminals are capitalizing on, but also to use it to their advantage in the investigative process. However, doing so is not without its challenges.

Challenges to DI

1. **The DI Misconception:** The perception that digital intelligence is some kind of high-tech bloodhound that is being unleashed by the authorities to track our every move is a monumental misconception that Agency Management/Command Staff must tackle head-on before they can begin to develop a DI strategy. This perception is untrue because our rights as citizens are protected by the Fourth Amendment to the United States Constitution. Agency Management and Command Staff need to explain that:

[3] Ibid

a. Objections to privacy and unlawful search-and-seizure issues revolving around digital devices are dealt with in the same manner as any evidence—by getting a warrant or by having witnesses sign a consent form. Once a judge issues a warrant or a subject signs a consent form, police are protected, but they are also bound by the rules of search and seizure.

   - Agency Management and Command Staff need to explain the process by which digital evidence is collected, handled, and stored. Again, this is about preserving the integrity of evidence while building community trust. Having the proper procedures and policies in place will ensure that both goals are achieved.

b. Evidence collected from any kind of electronic device seized under warrant is subject to the standard operating procedures (SOPs) agencies already have in place:

   - Digital evidence is extracted in a forensically sound manner.
   - Evidence is stored safely and securely; just as physical evidence is safeguarded.
   - DI is used to make associations between different data types and sources to find connections between people, places and things.

c. Analytics is utilized to sort data and find hidden evidence and is done after a warrant has been issued to access the digital data on the mobile device. A judge has already determined that this is lawful by virtue of the warrant issued, so nothing is being done outside of the law.

This message needs to be explained to both the legislative bodies, who provide funding for agencies to meet new challenges, and the public. By dispelling misconceptions about DI from the outset, agencies increase their odds of securing the funding, tools, training, and support necessary for law enforcement to perform in the digital world.

2. **New Regulations:** New laws limiting the scope of searches are placing increased demands on investigative teams to do their jobs within the confines of stricter access limits. We've seen this most recently in the challenges by certain states and cities regarding the use of facial recognition technology
3. **Dynamic Growth in Data Sources:** The variety of digital information sources is also expanding rapidly. While mobile phones and computers remain the major sources of information, digital data sources now include:

- CCTV
- Apps
- Wearable Devices
- Smart Home Technology
- Drones/UAVs
- Electronic Games
- Video and Digital Cameras
- Cryptocurrency/Blockchain Ledgers
- Vehicle Forensics
- Identity Resolution
- Internet of Things
- Biometrics
- License Plate Recognition
- Call Detail Records
- Cloud/Social Media Data

4. **Significant Increases in Image and Video Content:** Typical cases can require hundreds of hours to review. In our survey, 62% of respondents said they spend one to 10 hours per week reviewing photos. 70% of respondents claim they spend between one and 10 hours per week reviewing videos.[4] Long hours spent reviewing graphic content can also take a psychological toll on investigators.
5. **Data Overload:** The use of mobile phones worldwide is exploding.
    - **Rapid growth in subscriptions:** 8.8 billion mobile subscribers are anticipated by 2024.[5]
    - **Forensic capabilities can't keep up:** The overwhelming amount of data that needs to be examined significantly exceeds the staffing know-how and technology capabilities of agencies.
    - **Growing device capacities:** Devices capable of storing 256 GB to 2 TB (and more) are resulting in 20,000- to 100,000-page extraction reports.[6]
    - **More digital sources:** Most investigations now involve between two and 10 devices.[7]
6. **Advanced Encryption:** Technological advances to protect privacy are resulting in devices and applications that have a much higher level of encryption than ever before, which takes more time and higher skill levels to access
7. **Data Is Underutilized:** Getting the right data to the right people at the right time is critical for moving investigations forward faster. Yet, many agency investigators are still using manual review methods to find evidence. This manual process slows down the investigation and increases the risk of a critical insight being overlooked.
8. **Conventional Methods No Longer Work:** When applied to investigations in the digital world, conventional investigation methods:
    - Are far too slow; data can't be uncovered quickly enough.
    - Don't utilize digital data effectively. Cellebrite's survey shows that the vast majority of investigators are still reviewing data manually; 22% read extraction reports and mark them up with a highlighter, 69% read extraction reports using a reader tool.[8]
9. **Staffing Shortages and Training Demands:** Staffs are leaner than ever and are often forced to forward anything related to finding digital evidence to tech specialists who may also be backlogged.
    - This creates siloed environments that are slow, inefficient, and not collaborative.
    - Not "owning" the data and simply moving it onto someone else's plate also breeds indifference.
10. **Case Backlogs Are Enormous:** In our recent survey, 67% of respondents said their case backlogs are running three or more months behind.[9]
    - Staff can't keep up; they become demoralized.
    - Many case workers are forced to do a less thorough job of investigating data by simply move cases along.
    - Our survey also shows that 50% of backlogs are addressed by working overtime, increasing costs.

[4] "2019 Industry Trend Survey: Law Enforcement - Cellebrite."
[5] "Ericsson Mobility Report June 2019."
[6] https://www.sdsdiscovery.com/resources/data-conversions/
[7] "2019 Industry Trend Survey: Law Enforcement - Cellebrite."
[8] "2019 Industry Trend Survey: Law Enforcement - Cellebrite."
[9] Ibid

11. **Preserving the Chain of Evidence:** Challenges relating to compliance, privacy, civil rights, and civil liberties all raise concerns when DI is discussed.
12. **Perceived Expense:** Agency Management and Command Staff naturally have their eyes on their budgets. The software and training needed to utilize digital intelligence to its full potential can be viewed as expensive when compared to other resources.

Once Agency Management and Command Staff understand that the objections to utilizing DI can be overcome, the real question then becomes: *How, as a leader, can I create a DI strategy to solve more cases faster, reduce the burden on my staff, and realize cost-savings?*

The Solution—Create a Digital Intelligence Strategy

A well-constructed DI strategy provides law enforcement teams with the technology, training, and support to close more cases faster by:

- **Defining** each team member's role and responsibilities regarding accessing, managing, and leveraging data to enhance collaboration and communication across departments.
- **Enabling** people in the field to make the correct command decisions based on accessing relevant information as soon as it is available.
- **Empowering** the investigative team to leverage digital evidence at the right time to maintain the confidence of their communities.
- **Breaking** down investigative siloes to enable forensically sound, secure collaboration across teams and departments.

Law enforcement anticipates events that may impact the community and sets up processes to deal with those challenges. They run drills to ensure they are able to respond quickly, accurately, and efficiently, no matter what the threat is. A DI strategy works the same way. It is the process and procedure by which digital evidence is gathered and utilized to solve more crimes faster, and it needs to be a critical component of every policing strategy.

Ultimately, the right DI strategy empowers agencies to use digital evidence efficiently and proactively to make a more positive impact on their communities and build trust.

How a DI Strategy Works

Building a strong DI strategy involves more than simply gaining timely access to digital data. It's about sharing those insights across the full spectrum of stakeholders to harness the collective intelligence of your entire team.

[10] Ibid

Step 1: Your DI Strategy Starts with Access

Agencies must be able to access data and devices anywhere and anytime, instantly. Modern digital solutions that empower all team members with the ability to access and collect digital evidence.

Step 2: Manage and Control Data

You can't begin to leverage data until it is in the right place for the right people to see. Modern DI solutions organize data for you in a secure way that protects the integrity of evidence every step of the way.

The right DI solution extends far beyond data security, however, to help teams overcome the many challenges agencies face worldwide. These include:

- **Storing data:** Presently, data management is very inefficient across many agencies. Most agencies have no centralized data storage site that can be easily accessed by different stakeholders. Physical evidence is protected by a chain of custody. There needs to be a similar process in place for digital data as well to ensure that data can only be accessed by approved personnel.
- **Preserving data:** Retention is critical. Data must be held for the appropriate amount of time to avoid generating statute-of-limitations risks.
- **Managing permissions around data:** This involves more than what someone with permission can actually see. It's about granting permissions around what people can do with the data.
- **Meeting compliance:** Always being in a position to meet criminal justice compliance is also critical, especially when dealing with data destruction orders.
- **Preserving integrity:** Having a DI strategy in place ensures that evidence is handled correctly.

Step 3: Leverage Insights

Once all the data has been secured, you can begin to generate and leverage insights. Creating new ways to visualize and leverage critical insights is how you can focus an investigation on only the most important data.

Part of the challenge today is leveraging insights that may come from the wide variety of sources mentioned earlier. This is where automated solutions like analytics that include technology like artificial intelligence (AI) are critical.

AI makes this process of breaking down all the data sources—images, videos, text messages, and other data sources—into simple categories easier. From there the review of data is automated, minimizing the need for manual review of large amounts of digital data. The result is actionable insights that reduce the time needed to make the right decisions. .

It's important to remember that AI alone is not the solution. Rather, AI is the source that powers the tools to gather the right information. In turn, advanced algorithms are what power AI and break down information into categories that are easily understood..

Analytics solutions to process digital evidence enables investigators to:

- Secure precise historical location data.
- Reconstruct event timelines from calendars and messages with time and date stamps.
- Understand motives through social media posts and conversations.
- Show previously hidden connections among suspects, co-conspirators, and victims.
- Illuminate trafficking networks.
- Show images of victims or accomplices.
- Confront suspects and witnesses with definitive information during interrogations.

The right analytics solution makes data accessible and easy to visualize and understand. It can also enable intelligence gathering beyond the investigation. Management must understand what's going on inside their agencies.

- Where can they realize greater operational efficiencies?
- How are they leveraging the information for resource allocation?

The Benefits of a Comprehensive DI Strategy

Formulating a comprehensive DI strategy is a process that takes time, but it does deliver a number of critical benefits. Time savings is the most important benefit because it impacts everything that follows, from the moment a case is opened to the moment the file is closed.

As agencies develop their DI strategies more fully and journey toward becoming more "DI Ready," they will begin to see the progressive nature of benefits building one on top of another to lift the entire team. Here's how it works:

- We know that when team members are provided with the right tools and training, the number of evidence sources grows. Using Analytics, manual review of evidence can be eliminated, reducing time to evidence from months to days. And because Analytics narrows the information choices far better than manual review methods, the quality of evidence improves.
- Human resources using DI in the field and in the lab can be much more productive. Cases can be resolved faster while saving investigative costs. Fewer backlogs are created, and existing backlogs can be diminished over time.
- As cases are resolved faster with more actionable evidence, case backlogs (and the overtime costs needed to resolve them) begin to decrease. As backlogs decrease, employees feel less stressed.

Less crime leads to safer communities, which in turn leads to the continued support of those officials—police chiefs, mayors, and local representatives—who made those positive changes possible.

Case Studies: Digital Intelligence in Action

Digital forensics helped solve a mass murder case

This real-life case of a mass murder investigation in the U.S. illustrates the importance of streamlining all digital evidence into a single centralized location, and how Cellebrite Analytics helped automate and simplify cross-case examination to help solve the case.

Text messages and images lead to arrest of drug dealers

Digital data from a mobile device and cloud accounts helped uncover a drug cartel in Nepal. With this digital evidence, police launched an operation, which led to the arrest of multiple suspects. A larger international network of drug dealers also was uncovered.

Unlocked digital evidence proves to be key in murder case

Digital evidence proved crucial to convict a suspect of premeditated murder.

A Partnership to Realize the Benefits of DI

Cellebrite's DI platform manages each part of the investigative process, from the crucial first hours of an investigation to the final moments of justice. And it does so in a way that provides both compliance and sound governance.

- Cellebrite in the field provides first responders with access to digital data from victims, witnesses, and suspects at the time when it matters most to quickly start and focus an investigation.
- Cellebrite in the lab enables access to the greatest number digital devices, cloud sources, and applications so that every investigation has the digital data it needs to get to actionable evidence faster.
- Cellebrite for the investigation team leverages the data collected to create a complete picture of the investigation. This allows investigators to focus on surfacing critical insights that would remain hidden without DI. Multiple data sources can be layered and filtered to create "eureka" moments that investigators would never be able to see through manual means.
- Cellebrite management and compliance solutions in the Agency Management or Command Staff's toolbox provide a roadmap to more efficiently utilize human resources to solve cases faster and reduce case backlogs. Time saved by investigative teams can add substantial cost-savings to the bottom line over time and allow more time to focus on community building efforts.

Key Components

A partnership with Cellebrite provides access to an integrated, end-to-end solution with the tools, training, and expert support to bridge the technological and resource gaps across all types of investigations. Benefits include::

1. Timely access to digital data anytime, anywhere, no matter what size your organization is.
2. AI-powered analytics to find hidden connections to resolve cases faster.
3. Tools that allow collaboration between departments or task forces to find connections among seemingly unconnected people, places, and events to resolve cases faster.
4. Simple integration into your existing technology ecosystem for better efficiency.
5. Training and support from leading digital forensic experts with decades of digital investigation experience who are there to assist you with your most challenging investigations.
6. The ability to break down data siloes, enabling secure collaboration while creating efficiencies within an agency.
7. Turn basic information into timely, reliable, and actionable intelligence, allowing law enforcement to more proactively protect their communities. This builds trust.
8. The power to feed actionable intelligence in real time direct from the field to decision makers to allow investigators to focus on the most relevant information.
9. The ability to meet all of the challenges relating to privacy, civil rights, and civil liberties by establishing SOPs for collecting data using DI technology.
10. Gain insights into data at an agency level to gain understanding into trends and statistics impacting operational efficiency

Conclusion

Digital intelligence is critical for law enforcement to do its job. Nevertheless, DI is poorly understood by the public, evoking misbeliefs that "Big Brother" will soon be invading private lives and recording every move. To dispel this misconception, Agency Management or Command Staff must be able to articulate how a digital intelligence strategy will allow their organizations to lawfully use digital data to protect their communities without infringing on individual rights and privacy. As a trusted partner, here are four recommendations we believe can make a tremendous difference in how you protect communities and how you can continue to earn the trust of citizens every day.

Recommendation #1: Be Totally Transparent

Law enforcement must reassure both the public and legislative bodies that having a DI strategy will produces positive results in a lawful way. When used by properly trained staff, DI is the only effective means to thwart the ever-growing threat from criminals who are using technology for illicit means.

Recommendation #2: Establish Policies and Procedures

The public must be made aware that law enforcement agencies have set boundaries for DI use and who has access to this information. Doing so will build trust and confidence that police are doing their very best to protect their communities.

Recommendation #3: Publicize Successes

Law enforcement must make a concerted effort to share how the use of DI is positively impacting their communities and increasing public safety. The case studies we've shown are just a few of the ways that DI can be used in the field, in the lab, and in the investigation to expedite cases and bring criminals to justice. Celebrating these victories with your communities will engender more trust and goodwill.

Recommendation #4: Provide Best Practices

Establishing sound policies and regulations up front about how information is gathered, shared, and stored is of paramount importance. Privacy standards, training levels and requirements, anti-bias safeguards, and standards for how investigations are carried out must be made clear. The public must be made aware that any violation of these standards will be met with the severest consequences.

Ultimately, establishing the right DI strategy and seeking public approval through open dialog will enable agencies to efficiently and proactively make a more positive impact on the safety of their communities.

Agencies need the right tools, training, and support from a trusted partner to use data to their fullest advantage. We are that partner. Cellebrite empowers agencies worldwide to harness data through a comprehensive DI strategy that drives investigations to keep communities safe.

How to Start

Cellebrite's leading industry experts are available to conduct digital intelligence workshops, and drive proof of concept projects with your essential personnel. These efforts can assess your agency's DI readiness and identify areas of opportunity within your current technology environment to realize the benefits of operational efficiency and enhance the public safety capabilities of your team.

For more information contact your local Cellebrite office.

References

"Battling the Narcotics Crisis with Analytics." Cellebrite, April 16, 2019.

https://www.cellebrite.com/en/whitepapers/battling-the-narcotics-crisis-with-analytics/

"Ericsson Mobility Report June 2019," 2019.

https://www.ericsson.com/49d1d9/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf

"2019 Industry Trend Survey: Law Enforcement - Cellebrite," 2019.

https://www.cellebrite.com/en/insights/industry-survey/

Thebault, Reis. "California Could Become the Largest State to Ban Facial Recognition in Body Cameras." Washington Post, September 11, 2019, sec. Technology.

https://www.washingtonpost.com/technology/2019/09/12/california-could-become-largest-state-ban-facial-recognition-body-cameras/

CORPORATE

Cellebrite
94 Derech Shlomo Schmeltzer St.
Kiryat Aryeh, Petah Tikva PO Box 3925, Israel
Tel: +972 3 394 8000

USA

Cellebrite Inc.
7 Campus Dr. Suite 210
Parsippany, NJ 07054, USA
Tel: +1 201 848 8552

UK

Cellebrite UK
First Central 200
2 Lakeside Drive
Park Royal
London NW10 7FQ, United Kingdom
Tel: +44 20 3949 9521

GERMANY

Cellebrite GmbH
Herzog-Heinrich-Strasse 20,
80336 München, Germany
Tel: +49 (0) 89 2 15 45 37 18

APAC

Cellebrite Asia Pacific Pte. Ltd.
152 Beach Road
#19-06/08 Gateway East
Singapore 189721
Tel: +65 6438 6240

LATAM

Cellebrite Ltda.
Av. Engenheiro Luiz
Carlos Berrini, 550-12º
Andar Brooklin
04571-000 São Paulo, Brazil
Tel: +55 11 3216 3800

Digital intelligence for a safer world

Digital data plays an increasingly important role in investigations and operations of all kinds. Making data accessible, collaborative and actionable is what Cellebrite does best. As the global leader in digital intelligence, and with more than 60,000 licenses deployed in 150 countries, we provide law enforcement, military and intelligence, and enterprise customers with the most complete, industry-proven range of solutions for digital forensics and digital analytics solutions in the field, in the lab and everywhere in between. By enabling access, sharing and analysis of digital data from mobile devices, social media, cloud, computer and other sources, Cellebrite products, solutions, services and training help customers build the strongest cases quickly, even in the most complex situations. As a result, Cellebrite is the preferred one-stop shop for digital intelligence solutions that make a safer world more possible every day.

To learn more, visit www.cellebrite.com

Cellebrite