WHITE PAPER

Digital Intelligence - The Key to Policing's Future

As criminals become more technologically adept, agencies must be ready to leverage the digital data fingerprints they leave behind to solve more crimes faster.

Cellebrite Digital intelligence for a safer world

Executive Summary

Our lives are more closely connected through digital technology than ever before. From mobile phones and computers to wearables and smart homes, technology influences us in ways that only a few years ago we might never have dreamed possible. While the benefits are amazing, the mountains of information produced leaves many drowning in data.

Law enforcement agencies worldwide are reeling from the effects of data overload. Crimes impacting both our personal and business lives are becoming increasingly complex due to technology. And while higher incidences of certain crime types vary slightly by region (kidnapping and drug trafficking versus terrorism and human trafficking), agencies everywhere are struggling to keep up with the staggering amount of data that must be reviewed to solve a typical case.

Data overload is the primary reason many in agency management and command staff positions are rethinking how their organizations deal with data, but it isn't the only reason. Budget constraints have everyone in law enforcement trying do more with less, while the public demands that more officers be put on the street.

This is why many agencies are beginning to see the value in implementing a Digital Intelligence (DI) strategy to manage and leverage digital evidence to solve more cases faster, reduce case backlogs, and build community trust.

The challenge now is to convince the public and legislative bodies that DI, used lawfully, is the most effective way to protect their communities while ensuring individual rights to privacy are preserved.

This paper will look at this and other challenges law enforcement is facing today, but more importantly, how technology can overcome those challenges with new solutions that can:

- Handle the growing amount of data coming from a wider variety of sources
- Access data from sources that are siloed in different systems
- Take data from the most important sources and break it down into easy-to-understand categories to show trends that can lead to actionable intelligence
- Ensure governance/compliance standards are adhered to and personal privacy is protected

We will then take a look at new ways agencies can leverage existing infrastructures to better manage data in the future.

Contents

What Is Digital Intelligence?

In simple terms, digital intelligence (DI) has two components:

1. The data that is extracted from data sources, including smartphones, drones, computers, CCTV, apps, the 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 it is the method by which information is gathered, stored, and then used to build personal profiles that drive predictive profiling and policing over time.

Digital intelligence does not promote profiling in any way. It is simply the process of gathering and securing data (digital evidence) in a lawful manner and ensuring it can be accessed 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 legislative bodies clearly understand how this information is used to keep communities safe.

The Reality—The Landscape Has Changed

Cellebrite's 2020 Digital Intelligence Benchmark Report revealed that smartphones are showing up in investigations 92% of the time. Today, there are over 5 billion mobile devices in use compared to only 1.5 billion computers being used across the globe.

More sophisticated devices using advanced forms of encryption make it easier for criminals to hide their communications and actions. And data that was once kept on devices is now being stored in the Cloud, creating yet another hurdle for investigators to cross.

To meet the demands of this changing landscape, law enforcement needs a new way to conduct digital investigations and a sound strategy that addresses how digital evidence is shared and used at each stage of the investigation.

There is a clear path to harnessing the power of digital intelligence to solve crimes, but the way forward is not without challenges.

Challenges to DI

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 and command staff must tackle head-on before they can begin to develop a DI strategy.

This perception is incorrect because while laws and threat levels clearly vary from country to country, individual rights as citizens are generally protected by some form of national constitution or legal instrument.

Objections to privacy and unlawful search-and-seizure issues involving digital devices can be overcome if the public understands that digital evidence is collected the same way that physical evidence is gathered—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

legally bound by the rules of search and seizure to protect privacy.

Having the proper procedures and policies in place will ensure that the integrity of evidence is preserved, and individual rights are protected. However, agency management must be ready to explain the process by which digital evidence is collected, handled, and stored to maintain trust through transparency. This declaration needs to be made loud and clear to both the legislative bodies, who provide funding for agencies to meet new challenges, and the public that law enforcement serves. And it needs to be repeated regularly.

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 made by civil liberties advocates in the United States regarding the use of facial recognition technology and also in broader agreements among groups of countries such as the General Data Protection Regulation (GDPR) for EU members.

Data Collection: Frontline investigators tasked with gathering more (and better) evidence from victims in the field face serious push-back from witnesses and victims who are afraid to share their data for fear of reprisals. Gaining trust must be done proactively to overcome those fears, especially when current practices require custodians to relinquish their phones for long or unspecified periods of time.

Cost Savings: Budgets are becoming a huge challenge across Europe as investigative teams are asked to do more with less. This is where the efficiencies of new-generation DI solutions can help, but training is vital to success.

Data Deluge: Cellebrite's 2020 survey revealed that the number of phones the average lab practitioner must examine has jumped 20 percent in the last year to over 300 phones per year. Data extracted from those phones is also growing exponentially, which is causing serious problems. Labs practitioners report that examinations are backlogged three months on average and the number of devices is increasing.

Dynamic Growth in Data Sources: The number of data sources also continues to grow. While smartphones continue to be the largest evidence source, there is a growing list of other devices (CCTV, cars, drones, tablets, skimmers, GPS devices, and more) that also need to be examined for critical evidence.

Data doesn't merely exist on devices, either. Today, one in two cases involves accessing data from the Cloud.

Image and video content are also growing exponentially with typical cases requiring hundreds of hours to review, underscoring the fact that old methods of manually reviewing data sources simply don't work anymore.

In Cellebrite's survey, 62% of respondents said they spend one to 10 hours per week reviewing photos while 70% claim they spend between one and 10 hours per week reviewing videos.

The bottom line is that investigators are spending more time reviewing data and creating reports (43 hours per week on average, compared to an average of 37 hours per week in 2019). This process can now take up to 96% of their hours during an average workweek.

Even well-equipped staffs are hard pressed to keep up with such vast amounts of incoming data. This is why the demand for solutions that can quickly parse mountains of data quickly while managing it in a forensically sound manner is so high.

Lack of Funding: Having the financial means to invest in new technologies, increase staff sizes, and support staffs with adequate training, is a universal challenge. This is why taking a step back to evaluate all facets of policing operations is so important. Reallocating personnel based on threat assessments is key here. While an agency might not be able to increase their headcount, they can at least restructure to use their existing human resources to their best advantage.

Small Staff Sizes: While agencies in large cities may be well staffed, those in smaller counties or jurisdictions often lack manpower. Individual officers must be able to handle multiple tasks during investigations. This is why DI solutions need to be designed in a way that is easy to understand and implement. They also need to be supported by expert training that makes multi-tasking easy.

Fear Of Technology: As the role of digital intelligence in criminal cases grows, the role of the investigator is also changing. The need for law enforcement to mine these sources is clear, but the pressure on investigators to learn the technical skills necessary to do so is causing major stress problems, particularly among older officers, many of whom genuinely fear technology.

Training can solve this issue long-term, but in the interim, if these officers are not logging sufficient time on their computers, the job of ferreting out evidence falls squarely on the shoulders of analysts, many of whom are already stressed by having to output more with less help.

Not Having a DI Strategy: Not establishing a DI strategy is the biggest mistake any agency can make. Managers need to ask themselves where they want their departments to be in the future, then build a timeline backwards from there to become DI ready. In Cellebrite's recent survey, 34% of agency managers reported having poor to mediocre DI strategies while a shocking 9% of respondents said they have no strategy at all.

Budgets and Image: Justifying expenditures of taxpayer money is a continuing challenge as is maintaining a positive public image.

Public Expectations: While the good news is that most agencies are more skilled and technologically adept at using DI than they once were, the bad news is that public expectations for quick outcomes are exceedingly high. This puts increased pressure on teams to "solve crimes quickly," (the Charlie Hebdo case was a prime example) despite budget and staffing constraints. Solid strategies must be adopted that don't just solve the data deluge problem but harness the power of digital data to solve crimes faster.

Law enforcement needs a DI solution that allows every step of the investigation process to be proactively managed in a lawful, forensically-sound way.

Creating a Digital Intelligence Strategy

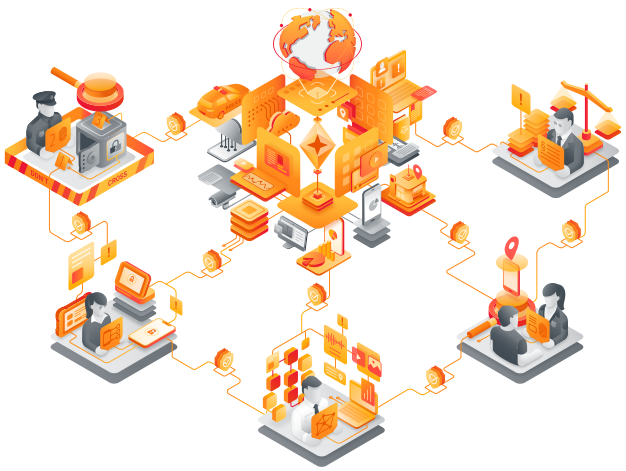
A well-constructed DI strategy doesn't need to be complicated. It does, however, need to provide law enforcement teams with the technology, training, and support to do their jobs more effectively by:

- 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 their ability to access relevant information as soon as it is available.
- Empowering investigative teams to leverage digital evidence at the right time to maintain the confidence of their communities.
- Breaking down investigative siloes to enable secure collaboration across teams and departments.

Anticipating events that may impact their communities is a core competency agencies everywhere share. They run drills to ensure their teams 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 leveraged to provide actionable intelligence, and it needs to be a critical component of every policing strategy.

How a DI Strategy Works

Building the right 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.



Step 1: Access

Agencies must be able to access data and devices anywhere and anytime, instantly. Modern digital solutions 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 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 actionable intelligence is how you can focus an investigation on only the most important data.

Part of the challenge today is leveraging insights that come from a growing number of sources. This is where automated solutions like Analytics, that include artificial intelligence (AI) technology, are critical.

AI makes the process of breaking down all the data sources—images, videos, text messages, and others—into simple categories easier. From there the review of data is automated, minimizing the need for team members to parse mountains of data. The result is actionable insights that reduce the time needed to make the right decisions.

It's important, however, to remember that AI alone is not the solution. Rather, AI is the source that powers the tools that can gather the right information. With advanced algorithms, AI organizes information into categories that are easily understood.

In effect, Analytics processes digital evidence, which 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.
- Surface previously hidden connections among suspects, co-conspirators, and victims.
- Illuminate trafficking networks.
- Isolate 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 to answer these questions:

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

The Benefits of a Comprehensive DI Strategy

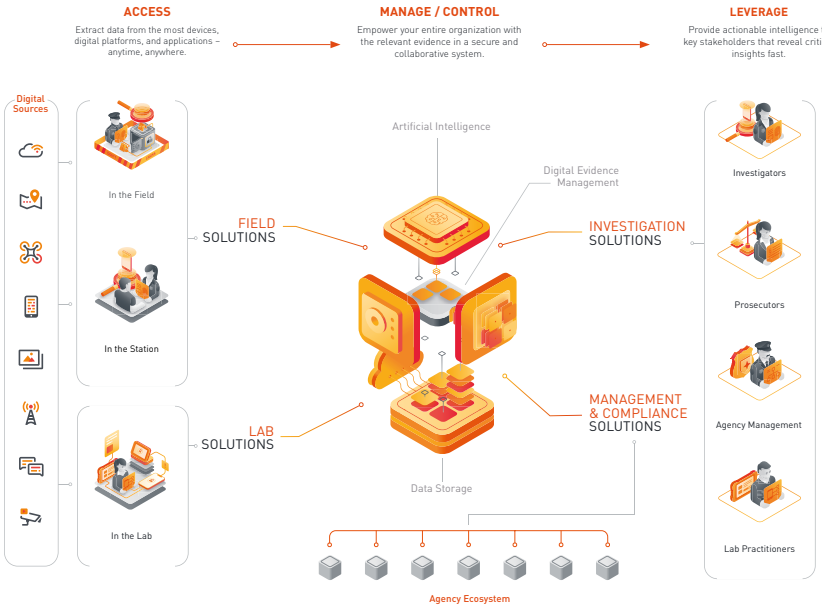
Formulating a comprehensive DI strategy is a process that takes time, but it delivers a number of critical benefits. Time savings is the biggest because it impacts everything that follows, from the moment a case is opened to the moment the file is closed.

As agencies develop their DI strategies to become "DI Ready," they will begin to see the progressive nature of benefits that can 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 digital evidence sources they can access will grow. 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.
- Frontline officers using DI in the field can be much more productive. Cases can be resolved faster while saving investigative costs. Fewer backlogs in the lab are created, which provides examiners more time to concentrate on the most difficult cases.
- 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 DI changes possible.

A New Paradigm

Cellebrite's DI platform revolves around a robust central core, but the vision is much greater. Picture a world in which trained frontline officers can perform simple extractions in the field in real time. Now imagine them being able to upload that data from the field or a kiosk to a central core where it can be properly stored, cataloged for quick reference, legally secured to meet all privacy laws, and managed so that the right people get the right information at the right time.



Imagine a platform that can provide a full view of the entire scope of the investigation, and one that pulls all of the disparate pieces of data together to provide intelligence that is of the highest quality and actionable—right away!

Now envision your team being able to share that intelligence—not just between the lab and examiners but across departments or other agencies around the world—all in a digestible, easy-to-understand format that provides critical insights to be acted on quickly.

That's the future we see and it's the future we're building with our partners right now.

Key Benefits

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

1. Timely access to digital data anytime, anywhere, no matter what size your organization is.
2. AI-powered analytics to surface hidden connections that can resolve cases quickly.
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 and seamless 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 available to assist you with your most challenging investigations.
6. The ability to break down data siloes, enabling secure collaboration while creating efficiencies within your agency.
7. Turning basic information into timely, reliable, and actionable intelligence, allowing law enforcement to more proactively protect their communities, which builds trust.
8. The power to feed real-time, actionable intelligence direct from the field to decision makers, which allows 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. Gaining agency-level insights into data to better understand trends and statistics impacting operational efficiency.

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 quickly.

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 was also uncovered.

Unlocked digital evidence proves to be key in murder case

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

Managing For The Future

Agency managers may already have existing ecosystems and infrastructures that have taken years to build and at significant cost. Their big questions are:

- How do you leverage the existing technological framework?
- How do you integrate new technologies into your existing systems to provide an even stronger platform for future investigations?
- What will be needed in three years or five years to solve crimes enabled by more advanced technologies?
- How can you reimagine your existing environment to ensure you're building a sturdy foundation of solutions today that will allow your agency to proactively evolve to solve more complex crimes in the future?

These are tough questions, but Cellebrite's experts are deeply committed to helping our partners solve them. This is why the holistic approach we take to looking at the entire investigation process from end to end is so important.

Many agency managers are dealing with fragmented architectures that support a variety of solutions that have undergone add-ons and updates making it difficult for new solutions to interface. Add to this a range of file formats and government rules that dictate how digital data must be captured and managed to protect privacy, and it's easy to understand why even the most conservative managers are rethinking their plans.

At Cellebrite, our experts can demonstrate how you can take advantage of the power of our solutions to work within your existing infrastructure to maximize your capabilities and deliver better results.

Training

Having access to the latest technology is of little value, however, if team members don't know how to use it to its full potential. Cellebrite's Learning Center offers a variety of training options both onsite and online to ensure your team members are ready to get the most out of each solution within the DI platform.

Taught by the leading experts in the field, these classes build confidence and provide a deep knowledge base that teams can share, so educational investments are optimized.

Agencies can choose between three training-class options to best suit their needs and schedules.

Conclusion

As we look ahead, the amount of data and devices investigative teams are going to need to deal with will continue to grow, driving the demand for secure repositories where data can be safely and lawfully managed, accessed, and analyzed to produce actionable intelligence.

Machine learning and artificial intelligence will be invaluable when parsing large quantities of data, but it will ultimately be up to skilled analysts to connect the dots and expose the complete picture of key areas and individuals to investigate.

Insights gleaned through the DI Platform will greatly reduce time to evidence, shortening case times and providing cost savings by reducing the number of hours investigations require.

To take advantage of everything that advanced DI technology can provide, however, agencies will need to rethink the way they allocate resources. New tools that integrate seamlessly with existing infrastructures will provide the backbone for analyzing digital data, but staffs will need the training and guidance to gather, evaluate, and share data collaboratively to solve more cases faster with less stress.

This is a completely new way of policing, where departments leverage a DI strategy that works in concert with modern communities to build a safer world. Because digital transformation is an ongoing process that advances the expectations of agencies and their communities, it still needs to be explained.

Agency management or command staff must be able to articulate how a DI strategy will allow their organizations to lawfully use digital data to protect their communities without infringing on individual rights and privacy. Here are four recommendations we believe can help nurture community trust.

Recommendation #1: Be Totally Transparent

Law enforcement must reassure both the public and legislative bodies that having a DI strategy will produce positive results in a lawful way. When used by properly trained staff, DI is the leading 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 reassured that law enforcement agencies have set boundaries for DI use and communicated to regarding who has access to this information. Doing so will foster trust and build confidence that police are doing their very best to protect their communities.

Recommendation #3: Publicize Successes

Don't be afraid to share how the use of DI is positively impacting your community and increasing public safety. Our case studies show how DI can be used in the field, in the lab, and during 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

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 proactively make a more positive impact on the safety of their communities.

Agencies need the right solutions, training, and support to use data to their fullest advantage. At Cellebrite, we not only imagine what the solutions are that can solve the crimes of tomorrow; we're delivering those solutions today.

How to Start

Cellebrite's industry-leading experts are available to conduct digital intelligence strategy 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 that can benefit from better operational efficiency to enhance the public-safety capabilities of your entire team.

To learn more about our DI Workshops, click here.

CORPORATE

Cellebrite
94 Derech Shlomo Schmeltzer St.
Kiryat Aryeh, Petah Tikva PO Box 3925, Israel
Tel: +972 3 394 8000
Fax: +972 3 924 7104

USA

Cellebrite Inc.
7 Campus Dr. Suite 210
Parsippany, NJ 07054, USA
Tel: +1 201 848 8552
Fax: +1 201 848 9982

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
Fax: +49 (0) 89 2 15 45 37 99

APAC

Cellebrite Asia Pacific Pte. Ltd.
150 Beach Road
#08-05/08 Gateway West
Singapore 189720
Tel: +65 6438 6240
Fax: +65 6438 6280

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