White Paper

Policing 2025: Envisioning a New Framework for Investigations

Sponsored by: Cellebrite

Alison Brooks, Ph.D.
November 2020

IDC OPINION

Law enforcement agencies today find themselves at a critical juncture as they wrestle with three profound challenges:

- The complexity of digitally mediated crime in the 21st century is extremely challenging. Law enforcement's central goals — to protect the communities they serve, maintain public order and safety, solve crimes, and bring criminals to justice in the courts — are becoming harder to deliver on as agencies struggle to manage the growth and variety of digital assets involved in investigations.
- With data privacy and data manipulation scandals on the rise, agencies around the world are having to address a "techlash" against surveillance. Agencies are thus increasingly having to tightly scope "acceptable use" policies to leverage next-generation technological capabilities.
- Pressures to fundamentally rethink the role of law enforcement, and to reestablish trust, have gained momentum globally.

Combined, these challenges strike at the core of policing. But they also present an opportunity to reenvision a new digital policing framework. More now than ever, law enforcement agencies need solutions that can address the complexities of digital investigations, help manage the volumes of data, and solve crimes in a timely and legal fashion.

Agencies must begin by asking a series of difficult questions:

- What must policing look like in 2025?
- How can law enforcement vastly better demonstrate its value to the community?
- How can law enforcement professionals underscore the value that technology investment delivers to communities?
- What is needed *now* to start delivering on that vision?

At a minimum, policing 2025 must be trusted, ethical, digital, and intelligent. Core operational technologies — increasingly embedded with artificial intelligence (AI) and machine learning (ML), and rendered in real time using data visualization tools — must be predicated on digital trust. To meet the ever-evolving tech-mediated criminal landscape, policing 2025 will need to be evidence based, data driven, usable, and intelligence led. By 2025, the future of policing intelligence will reside in digital intelligence platforms. This white paper examines how digital intelligence platforms can provide the strategic vectors through which agencies deliver on a reenvisioned policing framework for 2025 and beyond.

WHERE IS POLICING TODAY?

At the Nexus of Confluent Crises

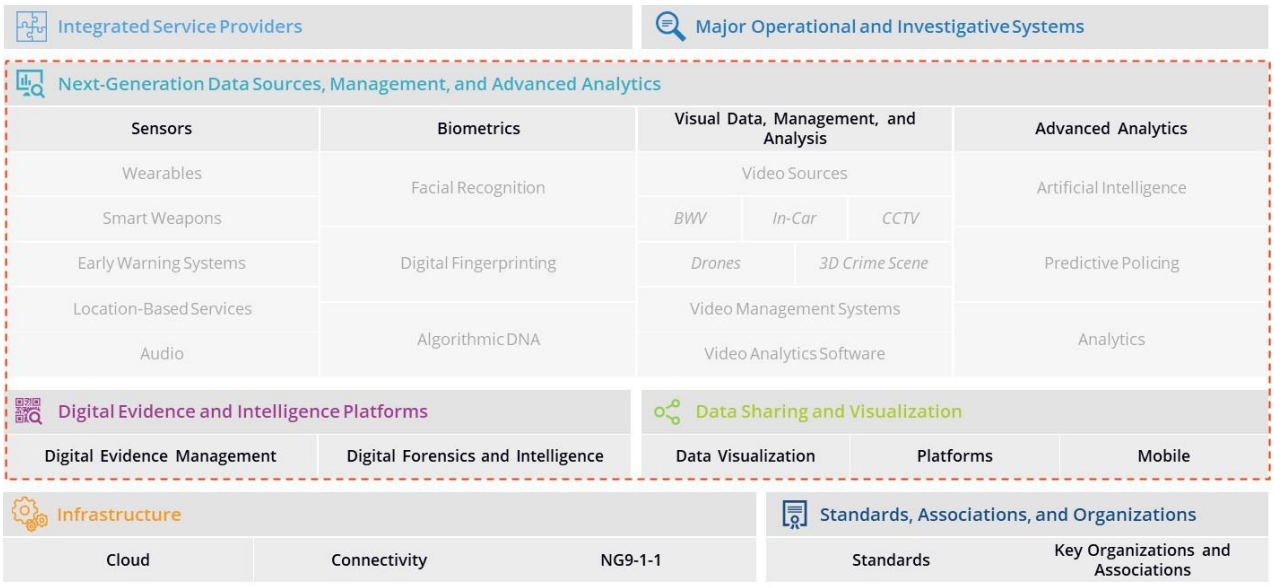
Coping with the Digital Deluge

Criminal investigations are increasingly becoming unmanageable given not only the volume and variety of digital assets coming into agencies but also the velocity at which those digital assets arrive. This includes net-new data sources such as large, heterogenous data sets generated by communications service providers, cloud service providers, laptops, and smartphones, as well as the skyrocketing volume of video and photographic evidence.

Figure 1 illustrates IDC's understanding of the data-driven policing market landscape. Consider the middle layer: "next-generation data sources, management, and advanced analytics." Within this slice of the market, we see a plethora of video sources, sensors, and biometrics, all of which need to be managed within a digital evidence platform leveraging complex analytical tools like AI to rein in the digital deluge. Many of these digital assets, and the solutions to make sense of them, did not exist even five years ago.

FIGURE 1

Data-Driven Policing Market Landscape



Source: IDC, 2020

Amid this technology explosion, it is also clear that crime today, and the resulting investigations, is far more complex, mobile, digital, and global in nature. Furthermore, many of the same solutions – mobile technology, advanced analytics, and cryptocurrency, for example – are both the conduits of crime and the tools used to investigate those crimes. Using the internet to engage in cybercrime and fraud, for instance, is a growing problem for law enforcement, exacerbated by the pandemic. Both INTERPOL and the United Nations have cited increases in cybercrime ranging from 30% to 600% during COVID-19, depending on the particular type of cybercrime.

Stymied by Siloed/Unusable/Underutilized Data

Underutilized data is commonly cited as one of the biggest challenges in policing. Many agencies are:

- Unable to see recurring patterns because of poor institutional knowledge retention and dissemination
- Unable to synthesize diverse internal and external data sources into information, often across jurisdictional boundaries, resulting in substandard decision making and situational awareness
- Taking too long to move from data to information to knowledge to wisdom, resulting in high latency in decision making and an inability to act within needed time windows
- Lacking enough granular visibility into end-to-end workflow to be able to automate
- Lacking the big picture (Data usage is low, and data exists in pockets or resides in the hands of a select few.)

In addition, there are insidious cultural challenges such as:

- Data aversion, or what some have termed *the ostrich effect,* whereby valuable information is ignored in lieu of gut feel
- Lack of data literacy and the resultant inability to have a common language around data
- Lack of data intelligence and the resultant mistrust of data, information, and insight

Complicating the situation further, agencies struggle with a mix of core legacy technology (CAD and RMS) that can be 20 years old and next-generation technology like body-worn videocameras. Not only do these thwart operations, but the default tends to skew to manual workflow. For many agencies, day-to-day operations and workflow remain largely manual, disconnected, and archaic. Contrary to popular public opinion, most police agencies do not currently operate like *CSI*-type televised crime dramas.

Propelled to Digital by COVID-19

Like much of the broader business community, the COVID-19 pandemic forced police agencies to digitally transform at breakneck pace. In the first stage of the pandemic, we saw agency IT scrambling to leverage underutilized but now crucial technology such as mobile solutions, remote working solutions, and virtual tools and to procure technology such as enhanced networking capabilities and software-defined security solutions that would allow the workforce to function virtually. The pandemic highlighted the need to digitally transform to share information and data assets internationally and to work smarter across multiple jurisdictions and nation states. Last, it fundamentally challenged the traditional, in-person, face-to-face police culture.

For many police agencies, COVID-19 pointedly highlighted gaps in digital maturity. Even agencies with very advanced digital workflows found themselves unable to provide core services because of fundamental gaps in core infrastructure — that is, missing elements of the tech-stack foundations — that would allow them to work remotely and securely. Police agencies find themselves on different points of the digital transformation (DX) maturity continuum. They also struggle to find a clear path to reinvention and transformation.

Coping with the Techlash Against Surveillance

While residents are keen to take advantage of "intelligence everywhere" in a consumer capacity, they are not keen on state intelligence/surveillance everywhere. As technology development continues to outpace the regulatory environment – artificial intelligence and facial recognition are good examples of this phenomenon – there are urgent calls from technology providers, privacy advocates, and police agencies alike to frame the appropriate legal, policy, and ethical environments to proactively and thoughtfully guide technology deployment.

Artificial intelligence, critical to forward-thinking digital policing, is often perceived as a black box technology, with a lingering fear of unintended negative consequences, including the ones not yet known or experienced. Using algorithms to automate important decisions based on machine learning of data that is biased risks biasing the decisions and raises important questions about AI ethics.

REENVISIONED POLICING 2025: ETHICAL, DIGITAL, AND INTELLIGENT

The key question for police agencies today is how to turn a convergent thundercloud of operational and societal challenges into a reenvisioned policing architecture that is ethical, digital, and intelligent. While policing agencies may have unique challenges, they seek to capitalize on the same opportunities as businesses to deploy technology to reenvision operations. And like businesses, policing agencies must be able to demonstrate organizational effectiveness, efficiency, and technology ROI.

Ethical, Transparent, Privacy-Protecting Technology

Policing 2025 leverages acceptable use frameworks to proactively guide technology deployments, and policy frequently precedes technology procurement. It is important to underscore, however, that digital intelligence and digital intelligence platforms are not surveillance vehicles – they are intelligence aggregators.

Policing solutions and workflow in 2025 must be:

- Fair: Algorithmically fair using unbiased data
- Explainable: To many stakeholders
- Robust: Safe, secure, and private, with a human in the loop
- Traceable: Understand the provenance of training data sets and metadata
- Transparent: Reporting in action, communication of results, and auditable

Impact to Operations

In 2025, in the context of increasingly augmented AI- and ML-enhanced workflows, ethical digital investigation ensures that:

- Agency leadership has established policy on responsible and ethical AI usage, initiated training for relevant departments or business functions, and fostered an organizational culture of responsible, data-driven decision making
- IT's governance processes are in place so that the data forensics practitioners are ingesting, analyzing, and sharing data that has been scrutinized for bias. The veracity of data lineage is verified prior to training AI models.

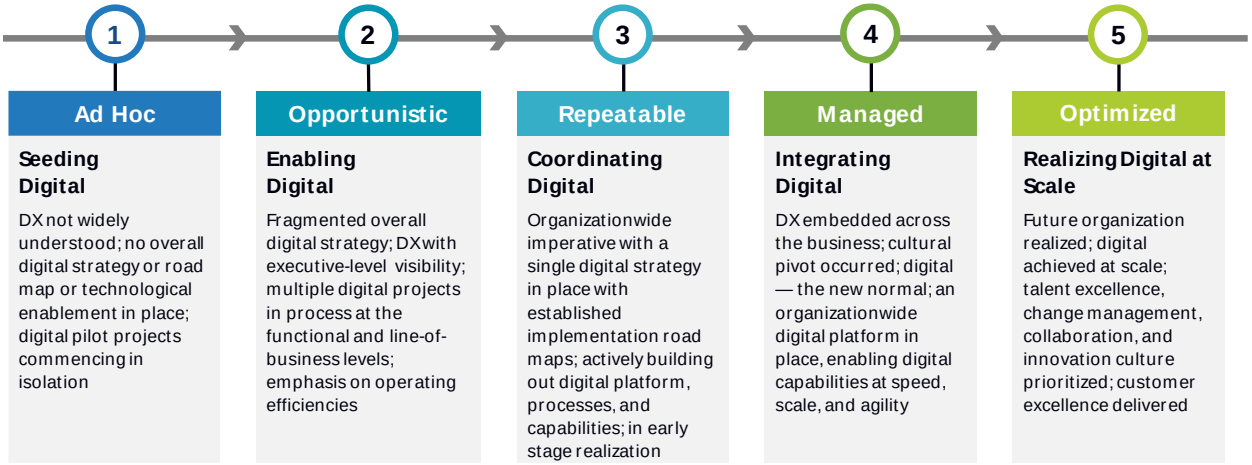
- IT determines appropriate data sources and uses training data that is as comprehensive and unbiased as possible. IT tests for bias and monitors performance. Prototype analytic solutions align with operational needs, providing insights from the data and actionable information, and collaboratively predict and advise agency leadership.
- Patrol and investigative personnel work with agency leadership to vet existing workflows and processes for bias. Transparency, auditability, and traceability are part of day-to-day operations.
- Citizens understand how the application of technology is following acceptable use guidelines and have faith that these deployments are optimizing public safety without creating a surveillance society.

Digital Transformation: People, Process, and Platforms

Police agencies globally recognize the inherent value of digitizing core policing workflows and processes. Digital policing modernizes case management, optimizes digital evidence management, and uses mobile-first solutions for community safety. As agencies harness a continually evolving landscape of digital assets, people, process, and platform technologies digitally transform in lockstep. Figure 2 illustrates the stages of digital transformation, from the simplest, unstructured ad hoc stage to the advanced, systemized, and optimized stage. Digital transformation must occur across people, culture, process, workflow, and technology.

FIGURE 2

Digital Transformation



Source: IDC, 2020

People — Skilled for the Future

In 2025, police agencies are capitalizing on the revamped skill sets of personnel. Leveraging skilling, upskilling, and reskilling, law enforcement operates more efficiently while retaining organizational knowledge. Broadly speaking, "skilling" involves identifying skill gaps in the workforce and then developing the necessary programs to address these gaps. "Upskilling" is teaching employees to perform current jobs in new ways using technology. "Reskilling" is teaching employees new skills to transition into different jobs and career paths. Each of these programs addresses different types of personnel (field, station, and specialized workforces) that need different skills and technology solutions. As the line between traditionally siloed workflow of "response" and "investigation" further blurs, responding and investigative agents are skilled, reskilled, and/or upskilled.

Broadly speaking, "skilling" involves identifying skill gaps in the workforce and then developing the necessary programs to address these gaps. "Upskilling" is teaching employees to perform current jobs in new ways using technology. "Reskilling" is teaching employees new skills to transition into different jobs and career paths.

Process — Radically Reformed for Efficiencies

In 2025, public safety agencies have fundamentally and radically rethought public safety workflow, integrating workflow process chains that were historically sequential and leveraging next-generation technology. Leadership and staff are committed to deploying an integrated policing platform. Digital intelligence platforms transform the collection and investigation workflow from the field to the lab and on to prosecution. For example, a detective from Victoria Police Department (Victoria, British Columbia) was recently able to leverage digital intelligence tools to link disparate mobile data sets to illustrate that a suspect was geographically nearby a victim and using a cellphone to harass the victim. All this was captured on video. Using digital intelligence tools to collapse previously sequential workflows, agencies compress the time it takes to make connections, follow leads, and corroborate evidence. Economies of scale, time, and effort efficiencies are gained by integrating workflow from the field to the lab and through to prosecution.

Platform Technologies — Delivering Agility, Scale, and Performance

Core police workflows and processes are digital and platform based. Neither a short-term nor a simple task, this is a necessary and critical step to modernization. Widespread adoption of "innovation accelerators" such as AI/ML, bots, drones, AR/VR, and wearables help agencies integrate their systems to manage these assets proactively. Agencies also leverage next-generation core infrastructure: cloud-enabled, agile, responsive, scalable solutions that rely increasingly on edge processing to minimize the storage burden while also preserving privacy.

Cloud

Resilient digital infrastructure helps meet greatly increased processing demand in sustainable and cost-efficient ways. Cloud infrastructure, advanced analytics, and a focus on digital intelligence allow agencies to securely share information across jurisdictional boundaries. Agency personnel are more competent in digital technology, and modernized solutions are built and updated quickly while running at internet speed. Cloud-native applications are developed to facilitate the data-driven user experience, allowing agencies to take advantage of the cloud's elasticity and scalability while also providing access to the newest functionality, the latest security provisioning, and the fast-paced innovation delivered through cloud services.

Cloud platforms function as an essential data management and integration tool in an increasingly crowded digital ecosystem. The lower costs of storing data and the higher compute power needed to analyze large data sets, in addition to the functionality built into cloud platforms, make the cloud preferable for data storage, integration, analysis, and sharing. Cloud functions synergistically with AI and ML to advance DX and reinvention.

Impact to Operations

By becoming digital, agencies are:

- Delivering insights in real time
- Benefiting from time and cost savings from reduced data collection and entry burdens and rationalized workflows
- Scaling across jurisdictions and agencies quickly when needed
- Using edge processing to minimize data management constraints while protecting privacy
- Easily and speedily incorporating innovations built on the cloud
- Gaining economies of intelligence, by synthesizing information, fostering the capacity for employees to adapt, and leveraging force multiplying technology to deliver insights at scale
- Hiring and cultivating staff with appropriate skills to complement the inevitable increase in automation of data processing

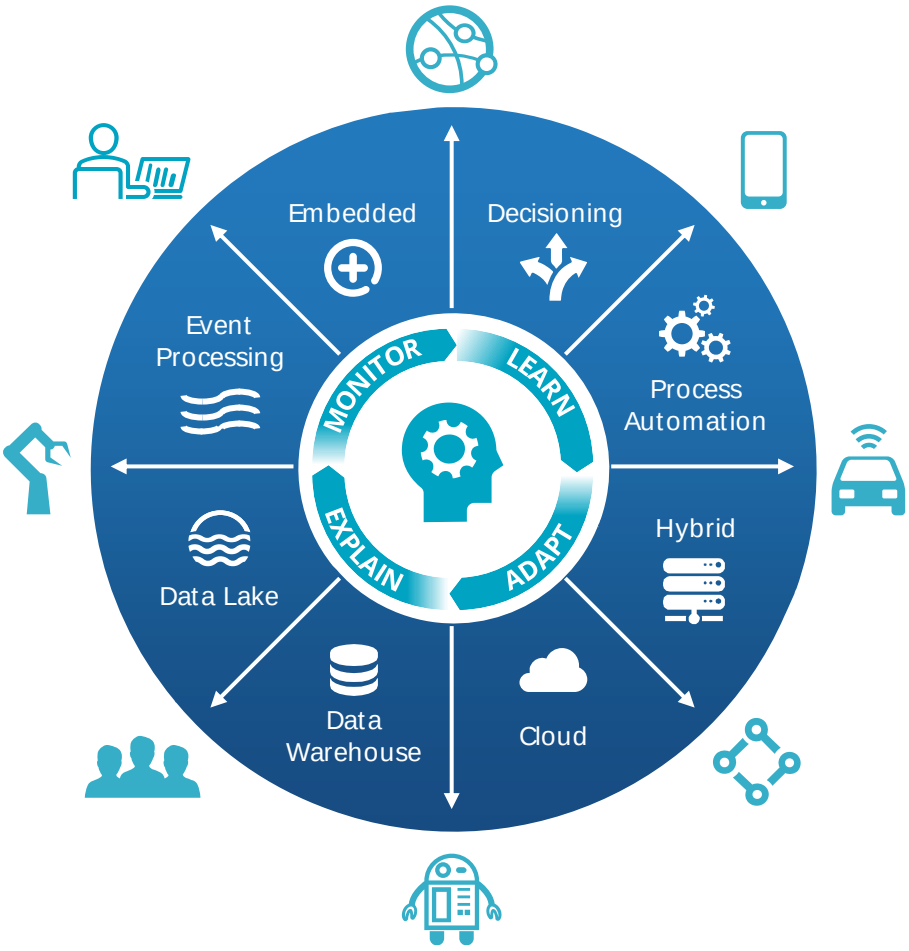
Intelligent — Digital Intelligence and Policing 2025

Data-driven policing and digital intelligence platforms recognize the crucial role that data plays in generating insights and catalyzing operational efficiencies. Digital intelligence platforms consist of investigative solutions and collected artifacts related to information as well as the analysis, management, sharing, and delivery of data. The platform ingests digital assets, many of which become digital evidence via digital forensics. The ability to derive insights from these disparate data sources is rendered by digital analytics, and increasingly, the ability to render these insights quickly is facilitated by artificial intelligence and machine learning embedded into the platform. Digital intelligence is much more than mobile forensics — it is integrated, scalable, and searchable and focuses on producing highly automated results.

In 2025, digitally intelligent police agencies combine an organization's *capacity to learn and adapt* with its *ability to synthesize* the information it needs to *apply the resulting insights at scale* to investigate and solve crimes. Delivering insights at scale, agencies have decision support and decision automation requirements for everyone in the organization, from senior leadership and analysts to first responders and investigators (and machines). As depicted in Figure 3, the delivery of insights at scale surfaces actionable information to all users (human or machines) in the flow of work. Users leverage scalability through cloud-native architecture to not only process large volumes of data but also support the requirements of many concurrent users.

FIGURE 3

Insights at Scale



Source: IDC, 2020

Impact to Operations

By becoming intelligence driven, agencies are:

- Synthesizing information and providing insights at scale – adding value, not volume (Agencies deliver trusted and actionable information in the context of its recipient.)
- Evidence based, both culturally and architecturally, accommodating purpose-built components and services for different workloads
- Disciplined in their approach to value measurement, setting a baseline and tracking progress by project and program over time

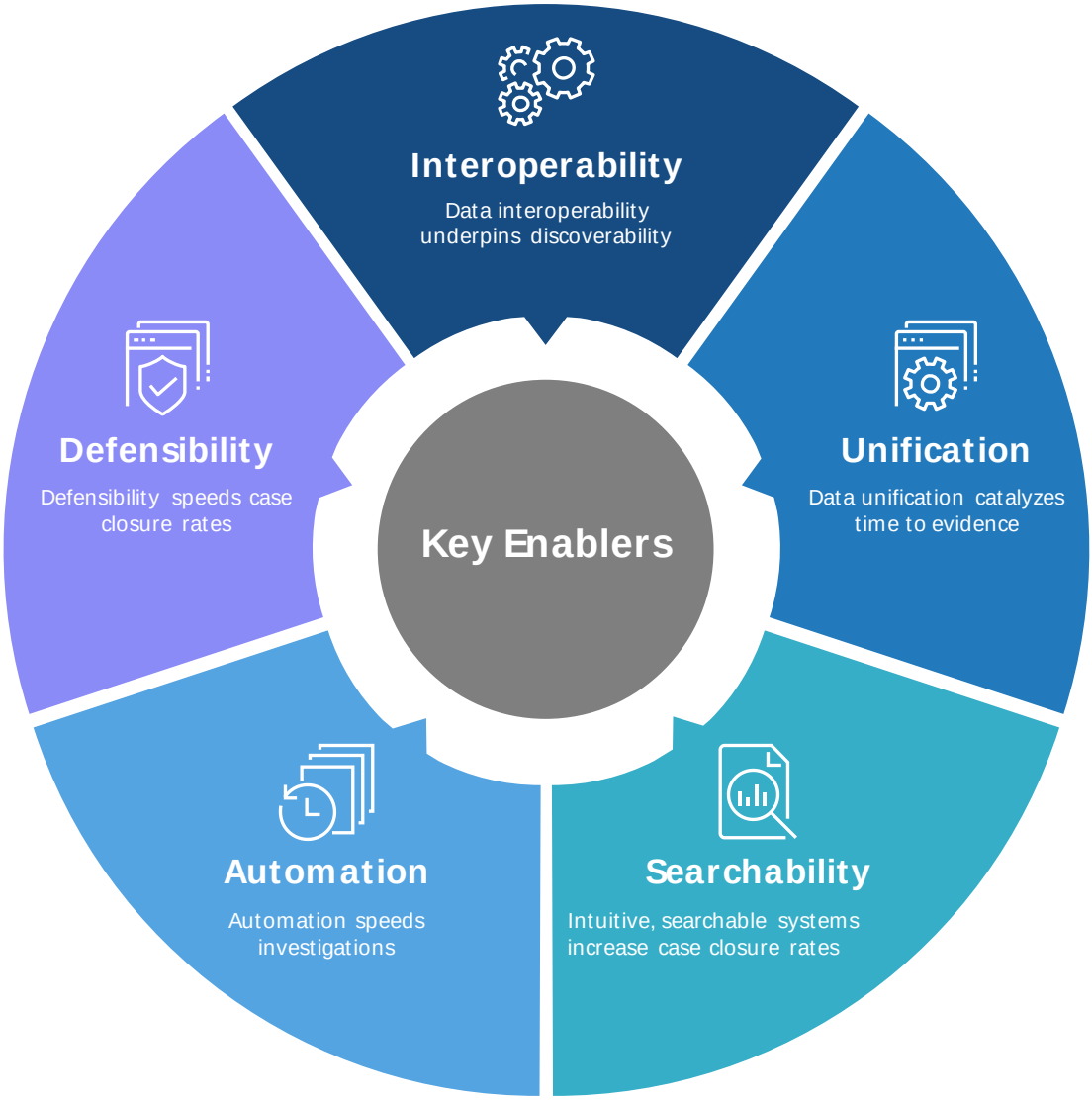
HOW DO WE GET THERE?

Key Enablers to Optimizing Digital Intelligence

Digital intelligence solutions are complex entities with multiple moving parts that must function seamlessly for a wide variety of trained personnel including first responders, forensic examiners, investigators, and prosecutors – and all associated workflows. Data interoperability, unification, searchability, automation, and defensibility are key factors propelling real progress in solving cases quickly in exceptionally complex times (see Figure 4).

FIGURE 4

Digital Intelligence Enablers



Source: IDC, 2020

These key enablers are described as follows:

- **Interoperability.** Data interoperability underpins discoverability. In 2025, police agencies rely on standards-based and platform-based solutions that are vendor agnostic. They are founded on data exchange models like the National Information Exchange Model (NIEM), fundamentally transforming data exchange and making it easier to seamlessly connect data sources. Data interoperability facilitates discoverability.
- **Unification**. Data unification catalyzes time to evidence. Managing a wide variety of data types is now the norm, and data complexity is managed seamlessly and in near real time. Digital intelligence solutions fundamentally transform how first responders, forensic examiners, investigators, and prosecutors discover defensible evidence within exceptionally large data sets coming from smartphones and social media as well as internet- and cloud-based service providers. The unification and integration of diverse sources and digital artifacts into a single intelligence platform provide agencies with a rich set of digital evidence that is unearthed quickly.
- **Searchability.** Accessible, intuitive, collaborative, and searchable systems increase case closure rates. Data analysis in the intelligence platform is intuitive and simplified so that agencies can visualize meaningful patterns, connections, and networks in minutes. Searchability is central to the platform, allowing investigators to keyword search for coded data and metadata for call records, social media postings, photos, and so forth.
- **Automation.** Automation speeds investigations. Artificial intelligence, machine learning, data visualization, and advanced and predictive analytics provide decision support capabilities while eliminating endless hours spent on manual exploration of data. Advanced video and image analytics solutions automatically identify and hash mark images related to key investigative areas such as trafficking, weaponry, nudity, faces, patterns, and child exploitation.
- **Defensibility.** Solution defensibility closes cases. Almost all investigations involve digital evidence of some kind, and of varying levels of complexity; digital intelligence from cloud-based assets (public domain and private social media data, transaction-generated information, instant messaging services, etc.) is managed appropriately in a legally defensible manner.

CONSIDERING CELLEBRITE

With more than 60,000 deployments in 150 countries, Cellebrite is a global leader in the digital intelligence platform. Cellebrite supports over 35,000 different smartphone device profiles. Its central lines of business include law enforcement, military, the intelligence community, and enterprise investigation solutions. As such, its customers are among the world's largest and most technologically advanced public safety agencies.

Cellebrite's Digital Intelligence platform consists of an integrated suite of solutions and offerings that have recently begun to segment workflows into interconnected segments, defined as follows:

- **Collection:** Lawful access to ever-evolving data types and sources
- **Investigative analytics:** Analyze and manage vast amounts of data to create actionable intelligence

Recent product development has separated capabilities for the field, station, and lab solutions. This distinction is important as providing field personnel with more tailored tools democratizes access to data throughout the workforce. The field solutions are also more targeted in the digital assets that they are extracting, in response to privacy concerns, specifically concerns over "overreach." For example, during large-scale incidents, it is common protocol to extract all of the data from smartphones in the

area at the time of the incident; this typically requires that the device is ported back to the lab or, conversely, that the data is extracted on scene, which can take hours. Targeted extractions are faster, are less intrusive, and can also help investigating agents understand whether there is in fact cause to take the phone back to the lab.

Cellebrite is currently developing its next-generation collection and investigative analytics solution, Cellebrite Pathfinder, which is specifically designed to more rapidly find digital evidence and drive investigations, all while ensuring compliance with privacy and chain-of-evidence protocols. Consider, for example, the data generated by drone footage as part of an investigation. Five years ago, this would have been used very infrequently; now it is commonplace in policing. Furthermore, Cellebrite's research lab is focused on innovations to counter advances in encryption on smartphone devices and social media platform information.

Within law enforcement, Cellebrite's offerings are particularly useful in investigating complex and covert crimes including gang violence, drug trafficking, counterterrorism, border security, homicides, and child sexual exploitation. Cellebrite's advanced unlock services can overcome complex locking and encryption technologies, allowing investigators to access data, remove blind spots in the data, and unearth case-relevant evidence. The insights gleaned from the digital intelligence platform are increasingly generating formative leads, which are important in terms of decreasing the time to evidence while augmenting success in that critical 48-hour window.

As agencies cope with a continual state of reinvention, in an increasingly complex world, Cellebrite's digital intelligence solutions, training, and services help agencies digitally transform, quickly automating discoverability across a myriad of digital assets and evidence and providing insights to all manner of personnel across the judicial continuum including investigators, examiners, analysts, prosecutors, and command staff.

Challenges

The data-driven policing solution landscape is crowded, complex, and evolving daily. Cellebrite will need to articulate its message to rise above the crowd; this is no small undertaking. This trend toward congestion is likely to continue as vendors with niche technology offerings outside of policing are recognizing the opportunity that exists in this market. In addition, post COVID-19, there may be considerable shortfalls in tax revenue, and this will likely create budgetary constraints, shifting spending to what is necessary to public safety. Cellebrite will need to communicate the essential nature of its solutions and drive home the ROI that is gained from its technology implementations. Last, momentum in the encryption space, both on the smartphone and within social media-generated content, is likely to cause Cellebrite to work creatively to provide clients with the data and insights to which they are accustomed.

ESSENTIAL GUIDANCE/CALL TO ACTION

Police agencies globally are experiencing a series of rapid, momentous changes, the pace and scale of which are unprecedented. They must reinvent core service delivery while simultaneously reestablishing public trust in policing. COVID-19 has been a catalyst to deploy new technology that can provide a solid foundation to enable future reinvention in response to the inevitable next disruption. The crisis has also highlighted the need for consistent digital maturity across solutions, agencies, and jurisdictions.

Policing agencies looking for digital intelligence platform solutions to make them more efficient and transparent, and to establish credibility while enhancing trust, should heed the following advice:

- With the continuous escalation of digital assets, digital intelligence platforms are more important now than ever. Digital intelligence platforms rein in data chaos and complexity, quickly transforming data into information, then into knowledge, and then into insight. This translates into faster time to establishing evidence.
- It will be increasingly important to automate the collection, analysis, and sharing of heterogenous data sets. Agencies will need to focus efforts on force multipliers such as AI, machine learning, and cloud processing to deliver insights at scale.
- Understand where there are gaps in the agency's digital maturity; the vendor community supporting this market understands how to help surmount critical gaps, no matter how and where you are in the process of digital reinvention. There is no wrong door.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com