The Next Evolution of Digital Evidence

Digital forensics can uncover crucial evidence to accelerate case closure. But you need the right technology to quickly access and analyze digital evidence in a defensible way.

Cellebrite
Justice Accelerated.

> *We need to be constantly on the front foot with technology. The pace, the speed and the capability of the criminals and the networks that we're trying to dismantle and prosecute pose the greatest challenge and threat to us."*

Lee Gosling, Detective Superintendent with the North East Regional Organised Crime Unit (NEROCU) in England

Executive Summary

"You can't ignore emerging tech. It has become more prolific, so law enforcement's understanding and utilization of it must evolve. Criminals are already doing that."

Neal Jetton, Director of Cybercrime with INTERPOL.

Technology has also emboldened criminals. They're finding new ways to commit crime and new types of crime to commit. Who could have imagined online sexploitation 20 years ago?

But with new technology law enforcement has a powerful new tool for uncovering and convicting perpetrators: digital forensics. In the same way that DNA unlocks the identifications of victims and perpetrators, digital forensics can unlock the voice of a victim and connect perpetrators to crimes.

Our interactions with digital devices leave a trail of data that can become crucial evidence in criminal investigations. But often, these "Digital Witnesses" are left sitting in evidence storage or waiting in a queue, inaccessible for use in bringing closure to victims and their families. In a Cellebrite survey, 80% of investigators said they lack the proper tools to easily review the digital data.

You'd never take a key witness and wait weeks to interview them or ignore them entirely—so why would you do that with a device found at a crime scene or on a suspect?

"The problem is the volume of data and devices—and I'd say there's been a humongous growth in devices that are being seized by law enforcement," says Dr. Madan Oberoi, Executive Director of Technology and Innovation at INTERPOL. "Most agencies are not set up for that volume, so they're incapable of meeting the demand."

With complex data and tight budgets, this is a problem that agencies need to address through digital transformation and advancing digital capabilities that meet evolving public and operational demands.

Drawing on the expertise of senior leaders in law enforcement, this eBook explores the prevalence of digital technology in crimes and at crime scenes and how law enforcement agencies can use that technology to catch perpetrators. It also explores how your agency can deploy the best solutions and systems to take advantage of these technologies before the perpetrator acts again, thereby preventing future crimes, ensuring public safety, and protecting your agency's reputation.

What your investigators can get from digital evidence

Digital devices such as smartphones, surveillance cameras, GPS and more record real-time events and data that can connect the dots in investigations. These “Digital Witnesses” are unbiased and have perfect recall, providing invaluable information in an investigation. But like any other witness, the longer you wait to interview these Digital Witnesses, the more the information is at risk.

Key Evidence

Last known locations, real-time pings and social media activity can help locate victims faster, increasing the chance of a safe recovery.

Faster case resolution

Encrypted chats, hidden files and online activity expose predators, leading to faster identification and arrests.

Stronger Prosecution

Call logs, location history and deleted messages can place a suspect at the scene and reveal premeditation.

“All is going to be shaped by AI and cloud computing, and there will be an increase in sophisticated cyber threats. All law enforcement agencies must remain adaptable, invest in technology and collaborate with private sector partners.”

Khoo Boon Hui, former Senior Deputy Secretary with the Singapore Ministry of Home Affairs, former Commissioner of the Singapore Police Force and former INTERPOL President

What’s in this guide?

The prevalence of digital witnesses

"I would say 90% of investigations—and that's probably a low number—involve some type of digital evidence, whether it's text messages, Facebook messages, photos, geotags or things like that," Chief Darin Perrotte of the Saranac Lake Police Department. "There's so much information in people's hands on these smart devices. You think about everything we do in life now with our cell phones and our iPads; I mean, our vehicles are equipped with essentially smart screens and have so much data. So there's a tremendous amount of data out there that can help with investigations."

Digital witnesses can help investigators make a case in the following ways

Missing person

Last known locations, real-time pings and social media activity can help locate victims faster, increasing the chance of a safe recovery.

Crimes against children

Encrypted chats, hidden files and online activity expose predators, leading to faster identification and arrests.

Homicide

Call logs, location history and deleted messages can place a suspect at the scene and reveal premeditation.

Narcotics

Dealer networks, transaction records and dark web activity can help dismantle entire operations.

Theft

Call logs, texts and location data from multiple phones can reveal stolen goods' movement, link suspects and expose organized theft rings.

Scams

Messaging apps, crypto wallets and transaction histories from scammers' devices can uncover fraud networks and track stolen funds.

Prison contraband

Uncovering money moved via cash pay apps can help investigators tackle organized crime operating inside the prisons.

Human exploitation

Call logs, location data and encrypted chats from traffickers' devices can expose migrant smuggling routes, border crossings and forced labor networks.

Drug Trafficking

"When we talk about dealing in death cases, the only way for that victim to truly be heard is by what their phone says,"

Sgt. Kyle Shiparski of the Michigan City Police Department

Shiparkski was part of a LaPorte County Drug Task Force that responded to multiple drug overdose deaths in a five-day span.

Digital evidence played a critical role in closing that case as investigators recovered vital information from cell phones and computers. They uncovered who victims were selling to, who they bought from, how much they sell and how often. The evidence showed the narcotics that had taken the lives of multiple people were all linked to one person. As a result, several people are now serving time in federal prison.

Digital witnesses

VEHICLES

GPS & Navigation

Infotainment Logs

Bluetooth Connections

PHONE

Contacts

Messages

Photos & Videos

App Data

Deleted Data

SECURITY CAMS

Video Footage

Timestamps

Locations

WEARABLES

Health Data

Location

COMPUTER

Documents

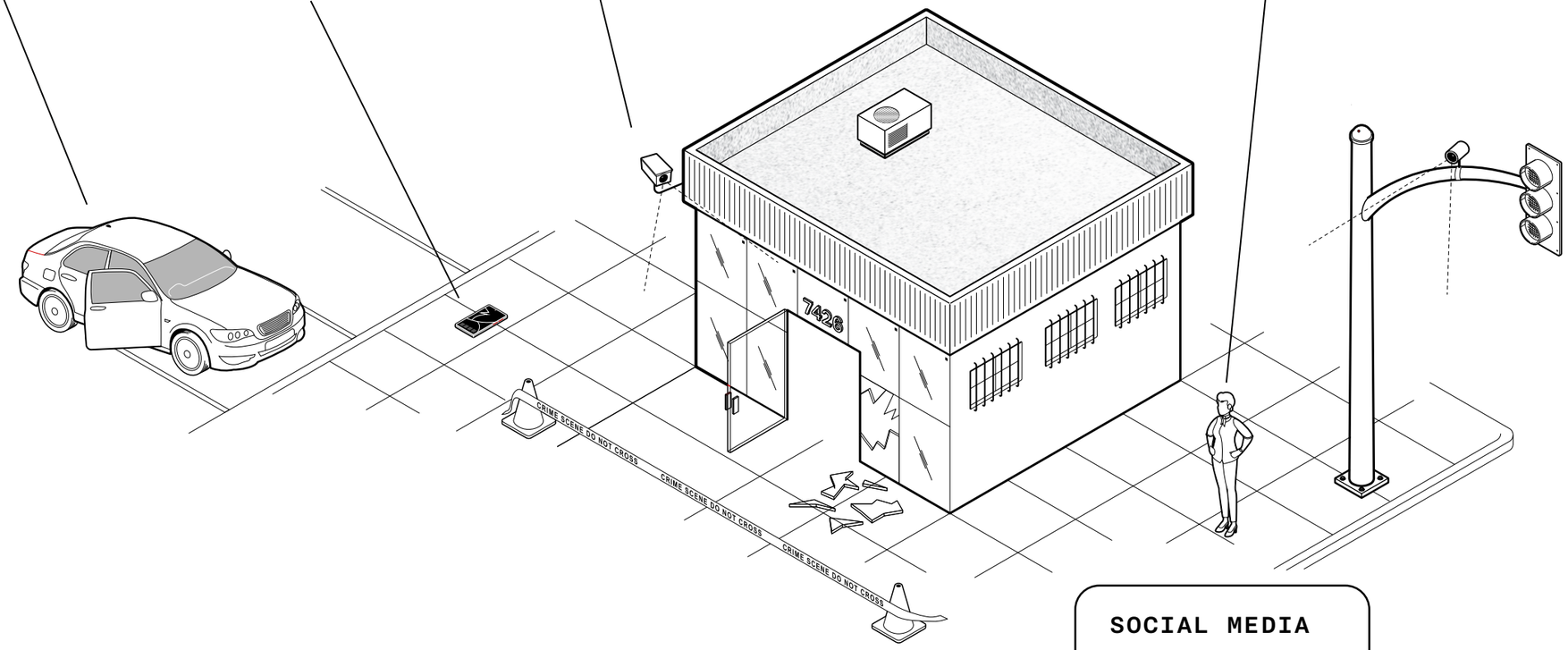
Browsing History

System Logs

CELL DATA

Tower Pings

Call Phone Records



SOCIAL MEDIA

Posts & Comments

Location Data

Connections

The challenges of “interviewing” digital witnesses

On average, two to five digital devices are involved in a crime. That’s a lot of data to wade through—not just a mountain of data, but a mountain range of data. “Once you get into these multiple devices, the volume and complexity of data is amazing,” says Khoo Boon Hui, former Senior Deputy Secretary with the Singapore Ministry of Home Affairs, former Commissioner of the Singapore Police Force and former INTERPOL President.

If investigators are unable to interview these Digital Witness fast enough—and make sense of the data—they risk missing critical facts and connections that can build a case. “I think the big thing now, especially for small agencies, is trying to manage all that data and trying to figure out how do we extrapolate the incredibly valuable information that’s in there with somewhat limited resources,” Chief Perrotte says.

For many agencies, the answer is a shared lab, but digital evidence often waits in a queue for days, weeks or even months. For others, internal labs do the work, but the volume and complexity of data means that the lab moves slower than the investigator. One police chief regularly saw his analytics team taking extended breaks and thought they didn’t have enough to do. But in reality, they were stuck waiting on their systems to download and decrypt information, a process that can take hours for a single device.

An average phone contains

60K+
messages

32K+
images

1K+
videos

Robbery and Murder

“I still recall her reaction saying, ‘This is the whole case, he’ll have to plead guilty at this point!’”

Detective Ryan Salmon said.

After a family had been held hostage and the father murdered during an in-home robbery, the Pierce County Sheriff’s Office in Tacoma, Washington, had a suspect but nothing that connected that person to the case—until investigators checked his cell phone records. Those records allowed investigators to trace the suspect’s location to a cell tower near the scene of the crime. The evidence was presented to the deputy prosecuting attorney and was deemed sub-stantial enough to land a guilty verdict.

The time and effort required to access, process and share digital evidence has grown exponentially.

Challenges with digital forensics workflows

The time and effort required to access, process and share digital evidence has grown exponentially, and while demands continue to increase, investigations are often hindered by limited resources, outdated tools or manual processes.

Evidence in Limbo

You're collecting evidence but doing nothing with it; it's just sitting in storage, not processed and not helping to close cases.

Major Crimes Only

Because of limited resources, you collect and process evidence for major crimes only.

Overwhelmed and Underpowered

You process digital evidence but face significant backlogs and resources shortages, including relying on laptops that aren't designed for the workload of downloading and analyzing content from devices.

Slow, Manual Sharing

Sharing information from digital devices is a slow, manual process that hinders collaboration.

Technology is the cause of these issues—and the solution. Modern technology can streamline digital collection and analysis workflows so that Digital Witnesses can be accessed, searched and examined just as fast as a physical witness can be interviewed, resulting in hard facts that can be used to close cases faster.

60%

of investigators feel that the review of digital data is too complex.[1]

Chapter 3

The need for digital transformation

Criminals are always adopting new technology to stay a step ahead of law enforcement. Agencies need to keep up, or they risk being outmaneuvered by perpetrators.

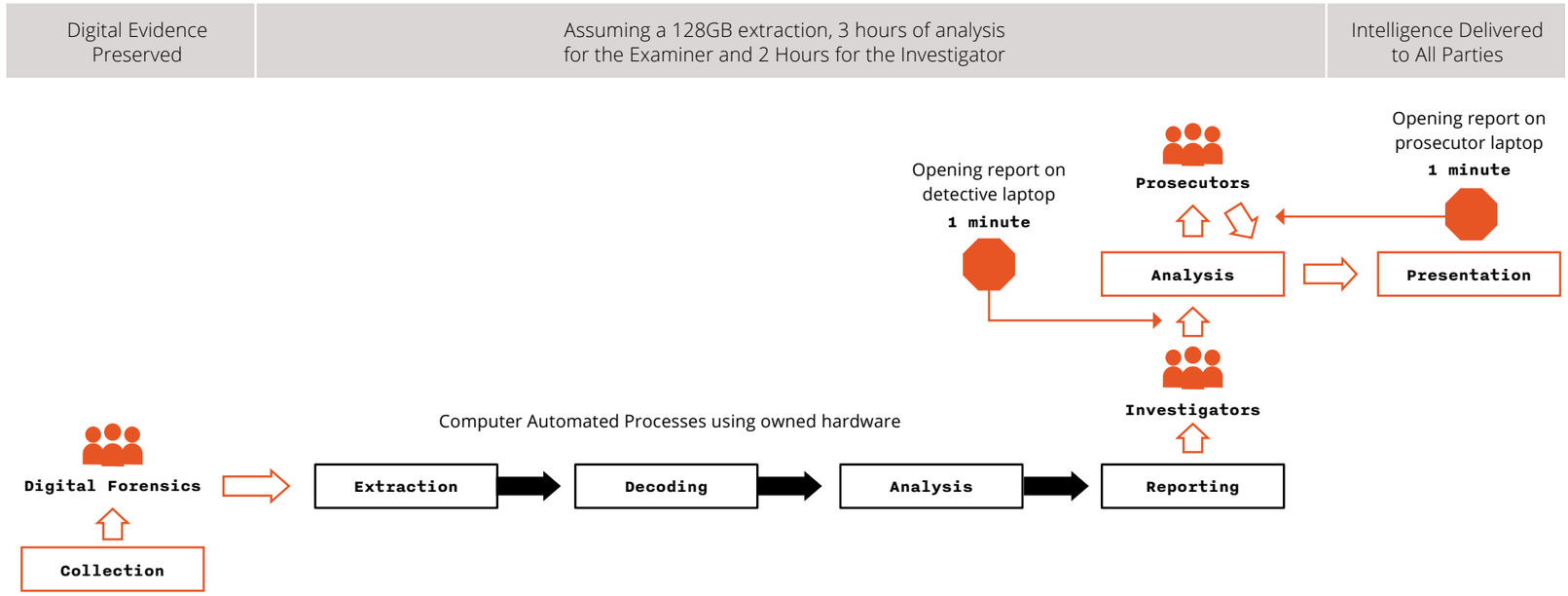
Cellebrite data shows that the right technology can cut the time for processing a single device down from 14 hours to eight hours—and those hours can be spent boots-on-the-ground moving the investigation forward.

That's how you accelerate justice.

"Mobile phones have made cases more involved. They've made them more time-consuming. And after you've gotten the data off of a cell phone, it still takes a detective to sit there and go through all of it. It's awfully time-consuming. That's why I started broaching the subject of how AI can aid our detectives in sorting through digital investigations in a more efficient manner."

Joe Gramaglia,
former Buffalo Police Commissioner

The Cellebrite workflow reduces total time spent by ~6 hours per device



Evidence Review

It's not an unusual occurrence: Investigators with an agency in northern England spent three weeks watching CCTV recordings of a doorway. They used pen and paper to note who was coming through the doorway, trying to make connections between those people.

As a test, the agency later put artificial intelligence (AI) to the same task; the AI tagged key suspects within three hours.

Only 11% of investigators are using an investigative analytics solution to find links between multiple devices; 37% are manually comparing using Excel, while 9% manually compare using a highlighter![1]

"Of cases that settle in plea deals, an average of 66% of cases did so due to digital evidence presented." [1]

How technology can enhance investigations

Innovative agencies invest in training and technology to empower their investigators to stay ahead of digital trends. They employ artificial intelligence (AI), cloud computing and storage and efficient digital forensics workflows.

AI can sift through thousands of files in hours, finding a particular clue among the terabits of data. It can detect trends and connections to strengthen and expand cases and offer tips for creating a more efficient investigation.

With the amount of data being handled, storage is a problem. Cloud storage offers unlimited capacity and makes collaboration easy because investigators can immediately and securely share data.

Technology can also accelerate investigations through more efficient workflows that enhance collaboration, analysis, and data retention. It can allow investigators to prioritize cases using a triage system similar what is used in healthcare settings.

These technologies will change the investigative process, but they will never replace humans. Rather, they will free up investigators to focus on the examinations and interrogations that they are uniquely skilled at.

In other words, technology is a superpower that investigators can use as a force multiplier in their investigations.

But this requires a digital transformation for agencies that lack tools and workflows to access and analyze devices quickly, store those devices and data, and share the information.

Outcomes from leveraging the latest digital forensics workflows

For agencies

Accelerated case resolution

Faster access to crucial digital data

Reduced wait times for evidence processing

Stronger case building

Comprehensive evidence collection

Increased likelihood of plea deals, reducing court strain

Enhanced reliability

Less dependence on eyewitness testimony

Ability to verify or disprove alibis with impartial data

For communities

Improved public safety

Quicker crime resolution

Potential prevention of further incidents

Increased trust in law enforcement

Greater transparency in investigations

Reduced concerns about wrongful convictions

Trauma reduction for victims and families

Less need for courtroom testimony when evidence is clear

Witnesses don't have to relive traumatic experiences

Trust, transparency and privacy

The public expects law enforcement to have access to all witnesses during an investigation—including the many Digital Witnesses that are part of our everyday life. And because Digital Witnesses are impartial and provide only facts, the public trusts evidence gained from devices.

But detaining a Digital Witness has its own privacy risks that agencies must navigate. Because this digital landscape is relatively new, so are the laws governing it, and they vary based on the jurisdiction and crime type.

Technology can help here, too. It can limit data review to just what is relevant, protecting privacy and unrelated sensitive data. Using secure cloud computing, investigators can ensure the chain of custody remains unbroken, eliminating concerns around transporting, mishandling, and misusing data and devices.

Whatever regulations your agency is held to during the interview of a Digital Witness, it must maintain the transparency that builds trust with the community. This means strict adherence to a device-handling policy through proper supervision and holding investigators accountable.

Evolving guidelines require agile, defensible digital solutions

Digital Evidence Guidelines recommend physical and digital tracking of all devices, use of cryptographic hashes (e.g., MD5, SHA256) to validate data integrity and routine audits.

NIJ (National Institute of Justice)

Protocols require formal logs for both device intake and digital image acquisition.

FBI Regional Computer Forensics Laboratory (RCFL)

Details how personal data is collected, stored and transferred—applies even to law enforcement in cross-border investigations.

General Data Protection Regulation (GDPR)

Innocent of Murder

Investigators hear it all the time: After a Columbus, Ohio, father was charged with a homicide, the man insisted that he'd just been in the wrong place at the wrong time. He said he was picking up his kid from school in the area where the homicide occurred. When law enforcement stopped him, he jumped out of the car and started running away with a gun in his hand—which is why investigators thought he was tied to the case.

The case against him was based on records that had been generated using a program that had a three-mile sector for tower orientation, meaning they didn't provide a pin-point location. Detective James Howe of the Columbus Division of Police (CPD) Digital Forensics Unit uncovered proper mapping data that showed the suspect's cellphone pinged a tower near the school—corroborating his story and leading to the dismissal of charges against him.

Chapter 5

The maturity journey

As you can see, digital data is now integral to all investigations, regardless of crime type. Incorporating new investigative workflows for collecting and accessing data can help your investigators solve cases faster.

After collecting the digital device, a five-step digital workflow journey should take place

For most agencies, this type of efficiency and crime-fighting will require a digital transformation—and a trusted, expert partner to help you get there.

Investigators said they spent an average of 69 hours per case reviewing photos, videos, CCTV, text messages and creating reports—time that takes away from investigating other leads and closing cases faster.[1]

Digital forensics workflows can speed up investigations and build stronger cases

1

Quickly access the device and transport it for analysis.

A tool that allows investigators to access a device in the moment preserves the relevant evidence for examination.

2

Examine the device for relevant information.

Inspecting the data on devices can give investigators insights, clues and connections to accelerate their cases. As mentioned, when done manually, this step in the journey could take a lot of time; AI can help significantly shorten that time.

3

Safeguard the chain of custody.

Defensible lab technology eliminates fear of the case being dropped or appealed because of a lab mishap.

4

Fast collaboration across teams to strengthen cases.

Drawing on information from a device, investigators can find connections to other cases or crimes.

5

Expand the case.

With new information gained during collaboration, a single investigation can expand into a network of connected crimes.

Child Sex Predators

Operation Overwatch was an undercover operation among multiple agencies that was more than a year in the making. Its mission: catch suspected online child predators. Law enforcement agents set up fake profiles of underage girls and chatted with men who solicited them for sex.

When the suspects showed up at a designated house, law enforcement was there to arrest them. Cellebrite was also there to support law enforcement as they immediately collected and analyzed data on devices used by suspects. As a result of the operation, eight suspects were arrested. “Our smoking gun is the digital evidence. We don’t have a case quite often without that digital evidence,” a member of the team said.

Chapter 6

Cellebrite as your strategic partner

Since 1999, Cellebrite has been working with law enforcement agencies around the world to help protect the public and safeguard assets with efficiency and transparency. Our technology has been bought by about 7,000 public safety agencies and enterprises, including 72 of the Fortune 100 companies, in more than 100 countries. In 2024 alone, it was used to solve more than 1.5 million serious crimes through legally sanctioned investigations. Because we're bonded, we bring privacy to everything we do.

Cellebrite's case-to-closure software platform helps you

Face public scrutiny with confidence.

Law enforcement agencies face growing pressure from high-profile incidents, community safety concerns, and demands for transparency and quick investigations. Cellebrite provides secure, defensible chain of custody management, data security and privacy controls and data that demonstrates your positive impact in the community.

Overcome resource constraints.

Law enforcement executives must tackle rising demands with limited resources. Cellebrite's scalable, cost-effective technology allows agencies to justify and optimize expenses with demonstrable efficiencies.

Turn back evolving and rising crimes.

Agencies need help to keep pace with technology-enabled crimes that traditional methods fail to effectively address. Cellebrite brings the technology that accelerates case resolution through digital evidence. The court-ready reports enhance the likelihood of a successful prosecution or plea deal.

Increase officer well-being.

Advanced filtering and categorization algorithms minimize officers' exposure to potentially disturbing material, preserving their mental well-being without impacting investigative thoroughness.

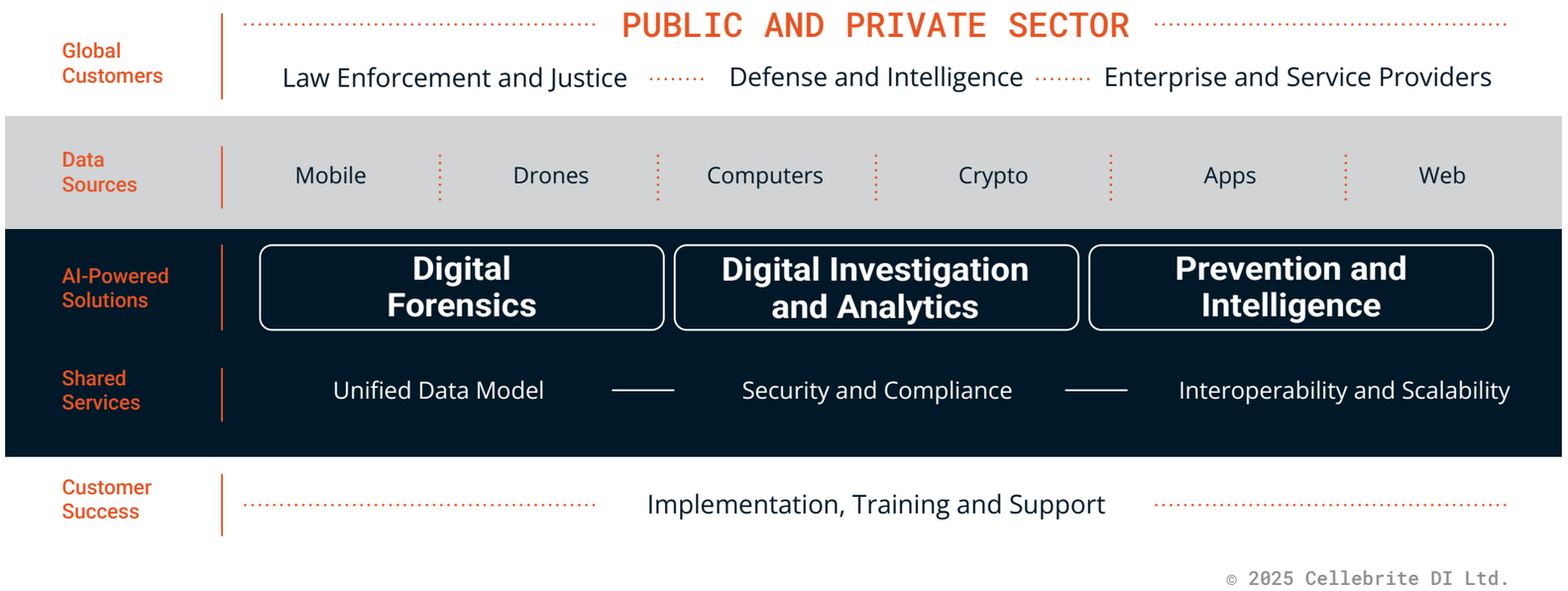
Officer Retention

Saranac Lake Police Chief Darin Perrotte's teenage son and daughter grew up in an era where their lives revolve around technology. So have the young officers joining his department. "This generation of young officers that are coming on staff expect high-tech stuff. They grew up watching TV and seeing these shows where everything is about law enforcement technology. They kind of expect that," he says.

So, when an agency keeps up with the latest technology, that agency is more attractive for recruits and current staff. "One thing that we've really done is build the department's technology, and that's helped us with the recruitment and retention of officers," Chief Perrotte says.

Protecting Communities, Nations and Businesses

Turn digital data into actionable insights to accelerate investigations, operations and threat detection.



Today's public safety teams face growing volumes of digital evidence, tighter timelines and increasing expectations for accuracy and transparency.

Whether you're building new workflows or strengthening existing ones, success depends on solutions that support fast, secure access to critical data—and are built to leverage technologies like AI and cloud to handle modern demands.

Cellebrite helps:

- Accelerate case resolution
- Simplify evidence handling and collaboration
- Protect chain of custody and data privacy
- Adapt to your agency's structure, resources and mission

Designed to meet agencies where they are and move forward with them—every step of the way.

What if the key piece of evidence in a high-profile case is locked in a phone?

If you have a lab, ask your analysts

Does it take less than five hours to access a phone?

Are you certain you're getting all the evidence you need to get from devices—especially when the messages are encrypted or deleted?

Do you have an automated chain of custody?

If you don't have a lab, ask your investigators

Does it take less than a day to get evidence back from the lab?

Does it take under a minute to load a digital evidence file onto your computer?

Are you certain you're getting everything of evidentiary value from digital devices to build the strongest case?

If you answered "no" to any of these questions, we need to talk.

Contact us today to empower your team to solve cases faster and more confidently. Visit cellebrite.com/contact.

About Cellebrite

Cellebrite's (Nasdaq: CLBT) mission is to enable its global customers to protect and save lives by enhancing digital investigations and intelligence gathering to accelerate justice in communities around the world. Cellebrite's AI-powered Digital Investigation Platform enables customers to lawfully access, collect, analyze and share digital evidence in legally sanctioned investigations while preserving data privacy. Thousands of public safety organizations, intelligence agencies and businesses rely on the Company's cloud-ready digital forensic and investigative solutions to close cases faster and safeguard communities.

To learn more, visit us at www.cellebrite.com, https://investors.cellebrite.com and find us on social media @Cellebrite.

[1]"2025 Industry Trends Survey," September 2024. https://cellebrite.com/en/industry-trends-survey-2025/

[2]"Digital Evidence: Enhancing public safety using digital investigative technologies," Major Cities Chiefs Association Digital Evidence Working Group. October 2024.