Durham Police Department & Peregrine Technologies

Town Hall – Background and Q&A

Thank you for the opportunity to share how Peregrine supports organizations like the Durham Police Department in unifying data, strengthening coordination, and improving decision-making across public safety operations.

Public safety agencies nationwide face a similar challenge: an abundance of data — spread across disconnected systems — without the tools to connect it, interpret it, and turn it into coordinated action to drive better outcomes. Critical information often lives in separate silos or on paper, creating blind spots, compliance risks, and barriers to coordination. Peregrine was built to close that gap.

Whether helping agencies enhance operational efficiency, improve and accelerate response, streamline investigations, resolve cases more quickly, and deepen community trust through clarity and accountability, our platform replaces the fragmented landscape of siloed information with one unified, secure, and fully auditable environment aligned with Criminal Justice Information Services (CJIS) standards — where every action is logged, every access is controlled, and every data point can be traced with confidence.

Peregrine is committed to helping public safety agencies protect and leverage the information they already own to make their communities stronger and safer. It is a privilege to support the people who dedicate their lives to public safety, and we are honored to do so in service of the communities they protect.

About Peregrine

Peregrine was founded to help public safety agencies make better, faster, and more accountable decisions by unlocking the data they already have.

Our platform takes siloed and disconnected data and instantly surfaces mission-critical information to empower more informed decisions that improve outcomes.

Peregrine currently serves more than 90 million people through its support of hundreds of public safety agencies across 23 states and two countries — spanning from police departments and sheriff's offices to emergency management agencies and local governments.

Peregrine's Technology Solution

Peregrine is a secure, cloud-based platform built specifically for public safety agencies. It brings together data from systems agencies rely on — Computer Aided Dispatch, Record Management System, video, sensors, license plate readers, and more — into one unified view. The platform is fully interoperable and vendor-agnostic, able to integrate structured and unstructured data from virtually any system.

Because Peregrine is fully hosted in AWS GovCloud, it meets the strict security and compliance requirements of government customers. AWS GovCloud is designed specifically to host sensitive data. This ensures that agency data stays protected, accessible only to authorized users.

Peregrine meets CJIS standards with security built in at every level, including encryption in transit and at rest, permission-based access controls, single sign-on, and full audit logging.

Peregrine's intuitive interface gives users powerful analytics and visualizations, all designed to support faster, smarter decision-making. With a deployment engineer embedded with every customer, the platform is tailored to serve the diverse needs of every organization — allowing civilian and sworn users across department functions to utilize the entirety of the agency's data to keep communities safe.

Questions & Answers

What exactly does Peregrine do?

Peregrine is a data integration and analysis platform that helps public safety agencies connect information they already own. It brings together siloed systems so teams can see the full picture, make faster, more informed decisions, and improve coordination and transparency — all while keeping data under the agency's full control.

Who owns the data in Peregrine?

The customer exclusively owns and controls access to their data. Every user action is logged and auditable, so agencies have complete visibility into how information is accessed.

How does Peregrine protect sensitive data?

Peregrine protects data from unauthorized access and misuse through multi-level security, encryption, and granular permission controls. Every user action is tracked in an audit trail that shows who accessed what, when, and why. Peregrine complies with CJIS and HIPAA standards and enables agencies to continuously enforce their own data-use policies.

What specific data does Peregrine have? What data will Peregrine have access to?

Peregrine does not collect or own any data. The platform connects and organizes information that the agency already controls — such as case reports, calls for service, or other lawfully held records — to help teams see the full picture faster. Peregrine itself does not expand that data; the agency determines what sources are connected and who can access them.

Agencies choose what systems they connect to Peregrine and control all permissions. Any Peregrine personnel assigned to a customer's account will only be able to access data for purposes of supporting the account upon completion of a background check (and fingerprinting) in compliance with CJIS requirements.

Has Peregrine ever had a data breach?

No. Peregrine has never experienced a data breach. The company maintains a robust security posture with continuous monitoring, regular third-party audits, and compliance with CJIS and

HIPAA security frameworks. Protecting sensitive data is a core part of the company's identity and track record.

How is the data/information protected?

Peregrine protects sensitive data from unauthorized access and use through multiple layers of security. Every deployment includes encryption in transit and at rest, role-based access controls, and continuous logging of user activity. The platform maintains detailed, permissioned audit trails, allowing administrators to see exactly who accessed what, when, and why. Peregrine complies with CJIS and HIPAA standards, and its privacy-first design ensures data is only accessed or used by those with authorization.

How long is data stored?

Peregrine does not determine data retention periods — those rules are set by each customer in line with their internal policies, records-management laws, or local ordinances. The platform simply enforces those policies automatically, helping agencies ensure compliance through configurable retention settings and auditable logs.

If data is ever destroyed, how does Peregrine actually get rid of the data and how would the City of Durham receive confirmation that it is destroyed/gone?

When a customer requests data to be deleted, Peregrine follows secure deletion procedures that meet federal and state standards. Once deletion is complete, customers receive written confirmation and digital evidence verifying that all customer data and backups have been securely removed. Because the data remains under the customer's control, any deletion process is initiated and approved by the customer itself.

What happens to the data if a contract with Peregrine is not renewed?

If a customer chooses not to renew, the agency retains ownership and custody of all data. Peregrine does not take possession of any information; it resides within the agency's controlled environment or designated cloud. Upon contract expiration, Peregrine's access credentials are disabled, and any supporting materials or temporary caches are securely deleted in accordance with the agency's direction.

How does Peregrine use AI?

Peregrine utilizes recent developments in artificial intelligence (AI) to allow our customers to more efficiently and effectively leverage their data to improve public safety and broader government operations. Peregrine's use of AI reflects four principles:

1. **We implement AI where it can have a practical, real-life impact on customer operations.** We do not attempt to utilize AI in a "just because" manner, running data through models simply to see what happens or to sell AI as a feature. In the public safety space, Peregrine's primary applications of AI currently are to deduplicate person records, summarize reports, and generate safety flags for officers. Other applications include optical image recognition (OCR) and audio transcription.
2. **We believe a human must be in the loop.** In the AI applications described above, Peregrine makes it easy for users to see the sourcing and details of information that led to a model's output(s) and correct for any errors.

3. **We let customers decide whether and when AI gets used.** We do not automatically deploy these features at the start of an engagement; customers get to decide whether they are implemented based on their communities' and agencies' specific goals and concerns.
4. **We do not train on customer data.** Customer data is not used to train any AI model. In addition, customer data never leaves the CJIS and HIPAA compliant environment where Peregrine securely stores customer data.

Does Peregrine release its data for any other reason, like training AI?

No. Peregrine never uses customer data for AI training or any other secondary purpose in which customer data is shared or exposed to parties outside a customer's organization. Unless explicitly authorized by the customer, data never leaves the CJIS- and HIPAA-compliant environment where it is securely stored. Peregrine's AI tools are designed only to help users summarize, deduplicate, or extract insight from their own authorized data — not to build external models or datasets.

How does Peregrine benefit the community?

Peregrine helps agencies respond faster, allocate resources more effectively and efficiently, and make decisions based on its data. It supports transparency by making data easier to understand and share publicly. The result is safer, more accountable, and better-informed communities.