Public Safety, Justice, and the Internet of Everything

How connecting the unconnected can transform public safety and justice agencies, and make communities safer
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>3</td>
</tr>
<tr>
<td>What Is the Internet of Everything?</td>
<td>3</td>
</tr>
<tr>
<td>Public Safety Trends and Challenges</td>
<td>4</td>
</tr>
<tr>
<td>IoE for Public Safety</td>
<td>5</td>
</tr>
<tr>
<td>Key Technologies and Applications in Public Safety and Justice</td>
<td>6</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td>6</td>
</tr>
<tr>
<td>Emergency Response</td>
<td>7</td>
</tr>
<tr>
<td>Corrections</td>
<td>8</td>
</tr>
<tr>
<td>Courts</td>
<td>9</td>
</tr>
<tr>
<td>National Security</td>
<td>10</td>
</tr>
<tr>
<td>Key Factors Related to IoE in Public Safety</td>
<td>11</td>
</tr>
<tr>
<td>Getting Started</td>
<td>11</td>
</tr>
<tr>
<td>Conclusion</td>
<td>12</td>
</tr>
</tbody>
</table>
Abstract

This paper examines how the increasingly ubiquitous connectedness of our IoE world can help provide public safety and justice agencies with new opportunities to meet and overcome the challenges they face. It specifically examines this topic through applications in law enforcement, emergency response, corrections, courts, and national security, and shows how IoE can help transform agencies to better protect citizens and make communities safer. Finally, this paper will provide recommendations on strategy implementation to enable agencies to take the next steps.

What Is the Internet of Everything?

The Internet of Everything (IoE) is a continuous interaction among people, processes, data, and things. Sensors, networks, and smart devices are ubiquitous, providing a torrent of streaming data, or “data in motion.” Cisco is helping customers and strategic partners take advantage of the entire potential of IoE to achieve radical results across all sectors and industries. Indeed, IoE is capable of helping public safety and justice agencies increase cost efficiency, improve safety and security, provide better response times, and increase productivity.

As shown in Figure 1, the right combination of technology, process, and culture is required to unlock the full value of IoE.

People

Today, most people connect to the Internet through their devices, such as PCs, tablets, televisions, and smartphones, as well as through social networks, such as Facebook. According to the technical research firm Gartner, in the future people will become connections on the Internet and support two-way data transmissions. Police, corrections, and other public safety personnel may be tracked with sensors placed on the skin or sewn in to clothing to transmit vital signs and other information and thus becoming nodes on the Internet to both transmit and receive information.

Process

Process plays an important role in how each of these entities (people, data, and things) works with the others to deliver value in the connected world of IoE. With the correct process, connections become relevant and add value because the right information is delivered to the right person at the right time in the appropriate way. Imagine a commander being able to seamlessly route information, even across disparate agencies, in real time as an incident unfolds. Processes are what enable information sharing and interoperability for better situational awareness.

Figure 1. Equal Parts Required for Success
Data

With the Internet of Things (IoT), devices typically gather data and stream it over the Internet to a centralized source, where it is analyzed and processed. With IoE, instead of just reporting raw data, connected things will send high-level information back to machines, computers, and people for further evaluation and decision making. This transformation from data to information in IoE is important because it enables public safety and justice personnel to make faster, more intelligent decisions.

Things

This group is made up of physical items such as sensors, consumer devices, and enterprise assets that are connected to the Internet and each other, radio-frequency identification (RFID), and actuators. An actuator is an object that makes an action. For example, an actuator can turn off an engine or a light, or start a process to control a more complex system. In IoE, these things will sense more data, become context-aware, and provide more experiential information to help people and machines make more relevant and valuable decisions.

Public Safety Trends and Challenges

Public safety and justice agencies are under pressure to modernize and to cut government costs by streamlining operations while making data more accessible to law enforcement, corrections departments, emergency responders, courts, and national security agencies.

Police now are turning to technology for force multipliers to compensate for recent reductions in staff as department budgets have been drastically reduced by budget cuts in the past 10 years. Results from an International Association of Chiefs of Police and Major Cities Chiefs Association survey estimated 53 percent of U.S. counties are working with fewer staff today compared to a decade ago.

At the same time, public safety is trying to determine how video and other multimedia can be shared across public-safety agencies. Disparate communications systems and network technologies that are currently in place create roadblocks to interoperability.

Emergency responders at an incident scene are looking for new ways to access data before they enter a disaster area, while incident commanders seek to track emergency responders and their vehicle locations and conditions.

National-security agents also are looking at technology to act as a force multiplier and move data to and from field agents’ mobile devices. Currently, many investigators in the field must determine in person a specific threat when a device, such as an unmanned ground sensor, is activated. Agents seek a network of technologies that can access data and video, and transmit that information quickly to decision makers.

The top priority for agencies is secure data transfer. Given the current initiatives around network security and other threats facing public safety networks, it becomes even more important to secure networks from nefarious Internet attacks.
IOE for Public Safety

The IoE brings together people, process, data, and things to make networked connections more relevant and valuable. This combination can enable public safety personnel to move critical video data from incident commanders to field officers, giving public safety agencies and their personnel access to real-time, multimedia data in the field.

The IoT component is a network of physical objects that can sense and communicate data, and is accessed through the Internet. The technology enables users to take action based on intelligent data. The advent of the IoT has expanded dramatically the scope and capabilities of connected cameras, which now can be used as intelligent platforms to deliver gains in operational efficiency, situational and acoustic awareness, and forensic investigations. The evolution of video analytics, such as facial and license plate recognition, as well as audio analytics, has enhanced the ability of IoT-enabled cameras to deliver superior insights into all application areas, from safety and security to operational intelligence.

With IoE, in conjunction with the IoT platform, public safety officials can move sensitive information with mobile devices over a secure network environment because IoE’s intelligent, secure, next-generation networking and collaboration capabilities connect public safety and justice agencies to their data through a single and secure solution. An IoE-based network can take advantage of a multilayer architecture that integrates the best-of-breed capabilities to deliver a secure mobile architecture and a comprehensive solution to protect against most security risks.

IoE also provides enhanced interoperability, situational awareness, mobility, and overall security through next-generation computer, network, collaboration, and storage applications. With the IoE’s secure cross-architecture approach, public safety and justice leaders can rethink how they deliver and safeguard critical services and assets during unprecedented budgetary challenges, all while increasing workforce productivity, enhancing operational efficiencies, and driving down costs.

Public safety and justice agencies, just like all other agencies and private businesses, are potentially at risk of being hacked, no matter whether in an urban or rural area. IoE can help ensure data is available, yet confidential, when needed, with the owner of the information deciding which people, groups or agencies may have access to it. However, it is critical to remember that agencies should make sure they have a strong security policy in place and take proper precautions.

As seen in Figure 2, IoE has the potential to increase the effectiveness of public safety agencies while promoting efficiency, lowering costs, enabling rich video, and helping to protect responders from harm.

Figure 2.
Key Technologies and Applications in Public Safety and Justice

IoE has myriad applications for public safety and justice agencies, including law enforcement, emergency response, corrections, courts, and national security. Because IoE is a flexible network, innumerable applications are available for public safety agencies seeking access to data to streamline operations and better safeguard personnel.

Law Enforcement

IoE can be used as a force multiplier to help supplement labor cuts in many law-enforcement budgets. Technologies used as force multipliers can safeguard public-safety personnel by creating better situational awareness and by supporting interoperability.

Video and other situational data helps dispatchers and officers make decisions based on information instead of going into a situation blind, while also having access to video data for investigations and training. In addition, IoE officers in the field can become mobile offices, using tablets to submit incident reports that connect them to judges from their vehicles. IoE also supports video arraignment to reduce costs and enhance safety during detainee transport, remote court appearance to eliminate travel and delays, and remote interpretation to conduct interviews immediately in the field, no matter the language required.

By using the IoE, law enforcement agencies can have quick access to information at any time from virtually any place, wired and wireless, enabling real-time collaboration, incident response, investigation, and resolution. Integrating remote video and real-time collaboration at all levels of law enforcement allows agencies to:

- Control costs
- Manage evidence
- Reduce response time
- Decrease crime

“IoE lets police officers send and receive real-time video data from the field, greatly improving situational awareness.”

Chief Bob Stanberry (retired)
Business Development Manager for Connected Justice and Public Safety

Case Study: Florida DHSMV In-Car Video Deployment

The Florida Department of Highway Safety and Motor Vehicles (DHSMV) uses IoE to deploy in-car video on police car dashboards. These video systems enable officers to collect video footage for evidence in trials involving DUI charges and resisting arrest, as well as other situations. Should a citizen file a complaint about an officer’s conduct during an arrest, the video footage can be used defensively by the trooper to prove that the arrest was conducted properly.

Before installing the Wi-Fi antennas in designated areas, the upload time for video footage was about 3 hours. By deploying Cisco-engineered access points and antennas throughout the state, upload times were reduced to only 20 minutes. This saved the department $1.1 million for the year in overtime due to slow upload times.
Effective management of emergency response vehicles, whether ambulances, fire trucks, or police cars, is critical to the safety and well-being of citizens. If emergency vehicles are out of service or unable to respond quickly, it can be a matter of life or death. For emergency responders, IoE’s ubiquitous connectivity can be used to develop applications to track emergency response assets through connected vehicle technologies. In addition, ruggedized routers, switches, and surveillance cameras can be leveraged to help emergency response and public safety vehicles:

- Comply with safety mandates and regulations
- Maintain constant contact with dispatchers and fleet managers
- Transmit live telematics data for proactive maintenance of vehicles
- Use a GPS device to guide them to the scene by way of the fastest and most direct route
- Use vehicle-to-infrastructure (V2I) communication so vehicles can communicate with traffic lights, rail crossings, traffic cameras, and roads

Also, high-resolution monitors can be loaded on emergency response vehicles to provide comprehensive intelligence and emergency management capabilities through multiple perspectives using video and sensor information. Images captured by first responders, and even drone-based video cameras, can provide real-time situational awareness back to commanders and headquarters, which can help incident commanders manage resources.

In addition, users can monitor and show live GPS tracking of each vehicle responding to an incident and visually track their location on a color-coded interactive map using geofencing to map safety areas. First-responder vehicle fleet managers also can be notified immediately when accidents occur or when speed thresholds are exceeded.

Use Case: Intelligent Networking of Emergency Vehicles and Their Surroundings

An alarm sounds in Engine House 23, alerting firefighters to a factory fire in an industrial park with a potential hazardous materials (hazmat) alarm. As they race towards the fire, a rail crossing equipped with a sensor triggers an audio and visual alert in the truck to notify the driver that a train is crossing at an intersection on their route. The fire truck driver quickly diverts the route to maintain response time, saving critical minutes.

As the truck approaches the fire, it receives data from the cloud about the factory, the number of occupants, and the location of nearby fire hydrants. Environmental air sensors in the industrial park can send live updates to firefighters to help them assess the area and identify potential dangers.

With many first responders racing to the scene, sensors in nearby traffic lights are triggered to stop opposing traffic safely, so first responders can respond as quickly as possible without endangering themselves or the public. Data is sent wirelessly over the cloud to fire, police, nearby hospitals, and hazmat dispatchers to prepare other first responders and medical personnel.

The dispatch center uses a fleet management system to track the location of all vehicles, which are seen as moving dots on an interactive screen. Vehicle sensors monitor oil and tire pressure, and fluid levels for proactive maintenance to keep more emergency vehicles in service while sensors communicate with mass transit buses so they can alter routes to keep on schedule and minimize traffic near the scene, which helps to protect first responders and passengers.
Corrections organizations can use IoE to streamline collaboration tools. These tools can help corrections facilities processes by increasing staff improvement services while decreasing costs, increasing staff and prisoner safety, and reducing transportation costs and risks through controlling contraband, facilitating visitations, addressing overcrowding, and controlling costs. Collaboration technologies can use IoE to reduce the need for inmate transfer and to provide more effective services to inmate populations that help corrections personnel to:

- Address overcrowding
- Control contraband
- Facilitate visitation
- Improve inmate management
- Increase staff and prisoner safety
- Reduce transportation cost
- Save money

Collaboration tools can help corrections facilities improve services while decreasing costs and security risks through:

- Education: Provides distance learning opportunities for staff and inmates at a fraction of costs involved with traditional face-to-face education
- Remote interpretation: Facilitates faster response to medical or legal problems, or inmate management with immediate access to interpreter services
- Remote arraignment and appearance: Provides instant access to court and counsel without transport security concerns
- Remote visitation: Allows counsel and family members face-to-face interaction without physical security and contraband concerns
- Telehealth: Provides remote access to practitioners and specialists, and emergency evaluations to inmates, without requiring inmate transfers

“IoE supports collaboration across jail, court, and police systems all securely via the cloud.”

Commissioner Daniel Stewart (retired)
Senior Justice Advisor

Case Study: California Correctional Health Care Services

The California Correctional Health Care Services (CCHCS) is using the universal connectivity of IoE to improve healthcare services in California prisons and increase patient access to specialty care, mental healthcare, and primary healthcare. IoE connectivity enables CCHCS to operate a telemedicine program, as well as to provide virtual specialty-care services to California inmates. This program has enabled collaboration among more than 7,000 California healthcare workers and prison staff in 33 correctional facilities, as well as CCHCS headquarters.

Cisco installed 81 Cisco TelePresence® Clinical Presence System endpoints to virtually connect staff and patients to specialists through video, audio, and other sensory technologies, such as stethoscopes. The deployment now streamlines delivery of specialty healthcare to 166,000 inmates throughout California.
IoE-based court and justice solutions can streamline court processes by providing face-to-face collaboration without the time and cost of travel, or the need to move inmates or bring in live interpreters. By improving collaboration and increasing safety and security, it is possible for courts to:

- Control costs
- Increase the pace at which cases are decided
- Reach beyond courthouse walls, instantly

Remote adjudication can speed up court services and improve citizen access and satisfaction. Remote testimony can enable courts to scale resources and experts easily and effectively while improving public safety and reducing the need to transfer inmates. In addition, remote interpretation can take advantage of a central pool of interpreters, eliminating travel costs, improving access to specialized languages, and eliminating delays.

“Once you have the infrastructure in place, you can use it for myriad applications, such as arraignment, testimony, or interpretation services.”

Judge Boyd Patterson (retired)
Dallas County Chief Magistrate and Cisco Business Development Manager

Case Study: Dallas County Public Defender Video Deployment

Dallas County operates the largest public defender office in the state of Texas with 94 lawyers who try more than 45,000 cases annually. The county needed to streamline operations for the courts, enhance productivity, and ensure that all activities were aligned with the state’s Fair Defense Act, which requires public defenders to communicate with clients within 24 hours of being appointed.

The county took advantage of IoE’s potential by installing a robust IP network backbone capable of supporting video applications and deploying 200 video endpoints for remote court appearances and other types of video in remote locations. The system is used to arraign prisoners in the jail and communicate with the Justice of the Peace Courts and the Dallas County Community Supervision and Corrections Department.
Federal security agencies can better carry out their missions through IoE. Regions with few resources and personnel in the field can access real-time data for better decision making on how to deploy available personnel resources effectively. IoE applications provide improved situational awareness and act as a force multiplier. In addition, information derived from IoE-connected sources provide a common operating picture to save time and lives.

IoE applications help national security agencies better analyze information from field sensors and other technologies and get that information to a mobile U.S. border control agent, who can then determine whether a sensor is tripped by a person or by animals moving along the border. Unmanned aerial vehicles (UAVs), armed with video and night-vision payloads, can be deployed to capture data before agents are deployed, which provides a common operational picture to better safeguard the lives of border control agents.

Case Study: National Safety Agency’s Connected ESIC Vehicle

The National Safety Agency, an Australian not-for-profit research and development organization and a leader in the development of solutions for emergency management, has worked with Cisco to design a prototype vehicle known as the Emergency Services Integrated Communications (ESIC) vehicle. The goal of the ESIC vehicle is to provide a mobile command and control capability to address all hazards and to link all agencies involved in an emergency situation.

When activated, the self-contained ESIC vehicle meets these demands by combining all the necessary technology for emergent services with the ability to travel in proximity to the incident. After it is at the incident scene, the ESIC vehicle is completely operational in 15 minutes. Trained operators immediately can begin to manage and monitor the incident.
Cybersecurity and Data Integrity

IoE security will become an enormous issue across all markets, particularly in public safety. Information must be available, yet confidential, when needed, with the owner of the information deciding which people, groups, or agencies may have access to it. Embedded devices will help create complex networks of people and things, and such devices likely will create new relationships among people and computers.

Integrity of data must be assured, as well as its accuracy and authenticity. Success will be predicated on an open platform that allows all partners working together to use the same baseline technologies.

A balance must be maintained between understanding the positive impacts discussed in this paper and generating awareness about the risks to privacy and security. Public safety and justice agencies will need to have a better understanding of the risks of IoE, as well as ways to mitigate those risks. Personal and communal data will need to be treated differently, and the individual’s privacy will have to be respected.

Government Policies

Policies that encourage adoption of technology in public safety are crucial. Such policies must include sound change management practices among the agencies to reduce the barriers to technology adoption and increase its scale. Governments will continue to have a policymaking and regulatory role in relation to IoE so there must be a strong partnership, between them, public safety agencies, and technology providers, such as employing Cisco’s IT experts to help build out long-term technology strategies.

Getting Started

If you are a public safety decision maker, take the following steps to begin creating an IoE strategy:

1. Identify the IoE capabilities your organization currently has in place.
2. Seek and incorporate in your strategy the complementary insights of public safety personnel and Cisco IT leaders.
3. Identify major IoE opportunity areas and establish an IoE public safety vision that includes future needs.
4. Reach out to public safety organizations on local, regional, state, and federal levels to share the benefits of IoE platforms across governmental borders.
5. Build an IoE culture by helping public safety personnel determine the possibilities of connecting data to mobile devices used in the field.
6. Develop a 5-year plan to map out future applications, because the IoE is flexible enough to grow with public safety users’ requirements.
Conclusion

As the leader in world-changing technology for more than 20 years, Cisco is uniquely positioned to improve every day experiences for court administrators, judges, other court personnel, law enforcement and public safety officers, correctional facility officers, and many other stakeholders.

Cisco also offers the justice community a secure, resilient network backbone that enables decision makers to be more responsive and agile by removing barriers to communications, facilitating information sharing, promoting collaboration, and supporting innovation.

There is tremendous value in connecting the unconnected with intelligent networks across public safety and justice. This paper demonstrates IoE’s potential impact on protecting citizens and making communities safer.

However, to realize the benefits of connecting people, processes, data, and things, reliable connectivity and continuous access must be guaranteed. Additionally, for IoE to be accepted, both policymakers and public-safety leadership must be well-prepared to work with technologists to improve services to their constituents.

For more information, go to www.cisco.com/go/uspublicsafety.