BUILD SAFER CITIES AND THRIVING COMMUNITIES

WITH TECHNOLOGY THAT TURNS INFORMATION INTO INTELLIGENCE, AND INTELLIGENCE INTO SAFETY

TURN NOISE INTO INFORMATION, INFORMATION INTO INTELLIGENCE, AND INTELLIGENCE INTO SAFETY

Information is everywhere in our cities. Environmental sensors mounted on public transit vehicles measure air quality while wireless control sensors keep traffic lights from conspiring against drivers. City bike-share systems connect directly to the Web while city apps inform us when our bus is running late. Citizens use social media to engage directly with public service departments while city cameras send real-time streams to keep first responders a step ahead. Within the information flowing between citizens, responders and agencies is the intelligence that builds safer cities and thriving communities.

$1 ▸ $5

EVERY DOLLAR OF PUBLIC SAFETY INVESTMENT HAS BEEN SHOWN TO RETURN 5 DOLLARS OF ECONOMIC DEVELOPMENT RESULTS[1]

70

TOTAL POPULATION DECLINE FOR EVERY HOMICIDE THAT OCCURS IN A MAJOR CITY[2]

Vitalizing our cities and making them more attractive is the one clear focus of all government agencies. Every dollar of public safety investment has been shown to return 5 dollars of economic development results. At the same time, for every homicide that occurs in a city, the total population declines by 70 people. Government leaders understand the need to continually get better at public safety performance because we want our cities to thrive.

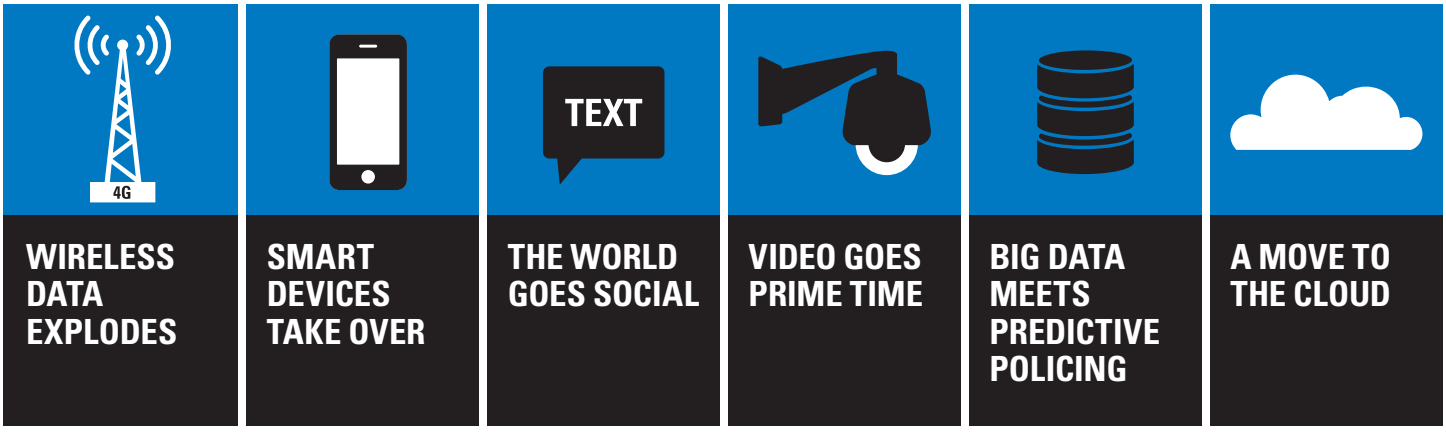
However, tight budgets in all levels of government and taxpayers wanting to pay less seem to contradict expectations for greater protection, safety and service – unless government can find ways to do more with less. And scrutiny of public safety performance data is growing as that data becomes increasing more transparent and publicly available; knowing that citizens are paying attention further increases the pressure to move those performance numbers in the right direction.

Government leaders see technology investments that will help them better collect, filter and share information with mobile professionals in the field as a critical imperative toward advancing their goals for providing exceptional service delivery with force multiplier benefits that lower taxpayer cost. More than 60 percent of them will prioritize investments in mobile broadband technologies to support advanced data communications in the next two years.

This is an incredibly transformative period for government. There is such an acceleration of technology today, and it is bringing capabilities and use cases along with it that are wholly unprecedented. When citizen-generated inputs marry with public safety inputs and voice, data and video merge into a single unified stream, multiple perspectives become a single point of view and we move from reacting at a moment's notice to whatever comes our way to intelligent prediction, communication centers can anticipate, forecast and predict. Actions in the field become more informed and collaborative. "Ready for anything" becomes "ready for what's next."

KEY TECHNOLOGY TRENDS SHAPING NEXT GENERATION GOVERNMENT

This paper considers the technology inflections taking place in the industry today that are most dramatically poised to transform government operations and help achieve the key performance metrics of city officials. Our leaders are determined to use technology to evolve government into a platform for interaction, moving away from a vending machine model where citizens put in money and receive a service (and perhaps kick it if it doesn't work). City leaders are looking to these technology inflections to elevate their service delivery at lower cost to taxpayers while enabling high standards for more open, participatory government. Leaders have high expectations for how these technologies will help government collect more information from across their cities, synthesize to find patterns and make smarter decisions, and distribute it to the people who need it, when they need it.



KEY TRENDS

WIRELESS DATA EXPLODES

Less than a decade ago, a worker in the field would require 2 to 3 minutes to receive an image the size of a postage stamp. Today with 4G wireless, multi-megabit mobile Internet is a reality, delivering the promise of empowering first responders and mobile government workers like never before. Governments have been adapting; mobile government workers and public safety professionals today are recording and streaming video, accessing remote databases, monitoring social media and more. 70% of public safety agencies have installed digital video recorders in their vehicles and 46% of them are streaming wireless video. In fact, 89% of public safety decision makers now recognize data as being just as critical to supporting their missions as the instant, two-way voice communications they depend upon.

70%
PUBLIC SAFETY AGENCIES INSTALLED DIGITAL VIDEO RECORDERS IN THEIR VEHICLES[3]

46%
OF PUBLIC SAFETY AGENCIES STREAM WIRELESS VIDEO TO THEIR PATROL VEHICLES[3]

SMART DEVICES TAKE OVER

The smartphone has rapidly emerged as an indispensable tool. Smartphone penetration in the US surpassed the 50% mark at the end of 2011 and outpaced personal computer sales by 30%. With the benefits of open sourced software and digital advancements doubling every two years, we are seeing rapidly increasing processing speeds, storage density, sensors and camera pixels being packed into a surprisingly small technology footprint. The first people at any incident scene are the witnesses and victims; with their mobile devices locked and loaded they are capturing, documenting and publishing content with an expectation that city leaders will be able to use that information. 72% of public safety agencies have expressed strong interest in harnessing citizen-generated text messages and video content to inform their investigations; 60% of them can connect the use of citizen generated data in helping support a recent response.

72%
WANT THE ABILITY TO USE VIDEO AND TEXT MESSAGES PROVIDED BY CITIZENS[4]

60%
SAY CITIZEN GENERATED DATA HAS HELPED SUPPORT A RECENT RESPONSE[4]

STAYING AHEAD OF WHAT'S NEXT WITH MISSION-CRITICAL INTELLIGENCE.

New, more sophisticated threats and criminals emerge every day while agencies try to manage increasing workloads at the same time with fewer workers. Public safety agencies are turning to mobile broadband to provide responders with applications that increase situational awareness, enhance tactical collaboration and enable greater in-field productivity to address these challenges.

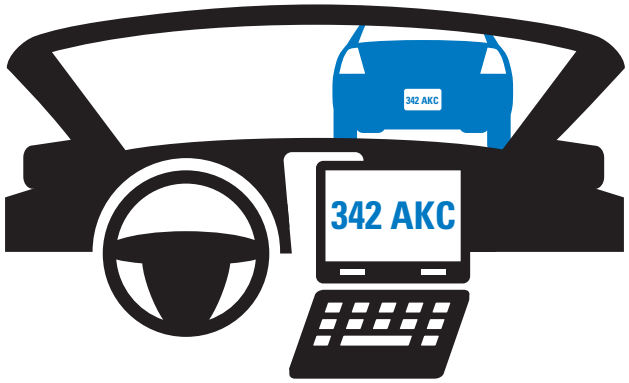
A SAFER WAY TO PROTECT

50%
REDUCTION IN TIME REQUIRED FOR A TRAFFIC STOP WITH ELECTRONIC CITATION[5]

10,800
FEWER HOURS, OFFICERS HAVE TO STAND AT THE SIDE OF THE ROAD DURING 162,000 TRAFFIC STOPS[5]

There's no such thing as a routine traffic stop. Unknown risks, distractions are inherent and incidents can escalate. With in-field, electronic citations, police departments can reduce the time required in a traffic stop by 50%. This keeps officers safely off the side of the road for an additional 10,800 hours during 162,000 traffic stops.

STAYING IN FRONT OF RIGHT NOW



50-100
NUMBER OF PLATES AN OFFICER CAN MANUALLY CHECK IN AN 8 HOUR SHIFT[6]

8,000
NUMBER OF PLATES AN ALPR SYSTEM CAN SCAN DURING AN 8 HOUR SHIFT DRAWING ATTENTION ONLY WHEN THERE IS A HIT[6]

To stay one step ahead, responders and those who watch over them, need the right technology to have better visibility to what's happening around them at all times. With Automatic License Plate Recognition (ALPR) solutions, smart vehicle cameras automatically read and process thousands of license plates, drawing the attention of responders only when a "hit" occurs.

COVERING MORE GROUND

TIME TO PROCESS MISDEMEANOR

8 HOURS
AT STATION, MANUALY[7]

30 MINUTES
ON SCENE, WITH MOBILE IDENTITY MANAGEMENT[7]

Mobile solutions empower officers and personnel in the field to do more at the point of work, allowing them to remain available and visible to the community they serve. With biometric identity management solutions, officers can quickly check for outstanding warrants and complete a report at the scene. A misdemeanor which could otherwise occupy 4 hours, pulling an officer out of the field for a half shift and cost an agency $6000 to process can now be completed in minutes.

KEY TRENDS

THE WORLD GOES SOCIAL

We are approaching the billion mark for active Facebook users and witness more than half using the mobile app; it's clear that social media is changing everything. Government officials are working hard to harness the power of social media to create a more open, participatory and transparent engagement with their citizens. Major cities are opening access to city data to drive social media innovations; they're exploring mobile apps that help residents submit, poll, vote and share ideas for maintaining the vibrancy of their communities. 83% of public safety agencies use social media to share information with the public and 70% use social media to receive information from the public. 89% are actively using social media to monitor for investigative leads; listening to chatter, seeing if known criminals may be bragging about committed crimes. Police departments are increasingly establishing Police Advisory Committees to drive their social media initiatives and manage the popularity of these programs.

83% SHARE
USE SOCIAL MEDIA TO SHARE INFORMATION WITH THE PUBLIC[2]

70% RECEIVE
USE SOCIAL MEDIA TO RECEIVE INFORMATION FROM THE PUBLIC[3]

VIDEO GOES PRIME TIME

Intelligent video surveillance solutions are improving decision making by adding the power of real-time sight and predictive analytics to government operations. Cities that have been long exploring video projects focused on critical infrastructure or highly localized public spaces managed across multiple agencies. These same cities are now evolving the disparate, smaller video projects into well-connected and highly intelligent city-wide surveillance systems. Emergency operations centers can see across public safety cameras to public service systems supporting the city transit authority, department of water and aviation as well as schools, banks and retailers. The measured returns on these video surveillance investments have been extraordinary. Factoring the savings from criminal justice costs and victims' financial and emotional costs, a $4.30 savings has been calculated for every dollar spent on the surveillance system in high crime areas. Even taking the victims' costs out of the calculation, the cameras have been shown to provide a $2.81 in savings for every dollar spent.

$4.30
SAVED FOR EVERY DOLLAR SPENT ON CAMERAS IN HIGH CRIME AREAS[8]

40%
REDUCTION IN CRIME IN THE FIRST YEAR OF DEPLOYING A VIDEO SURVEILLANCE SYSTEM[9]

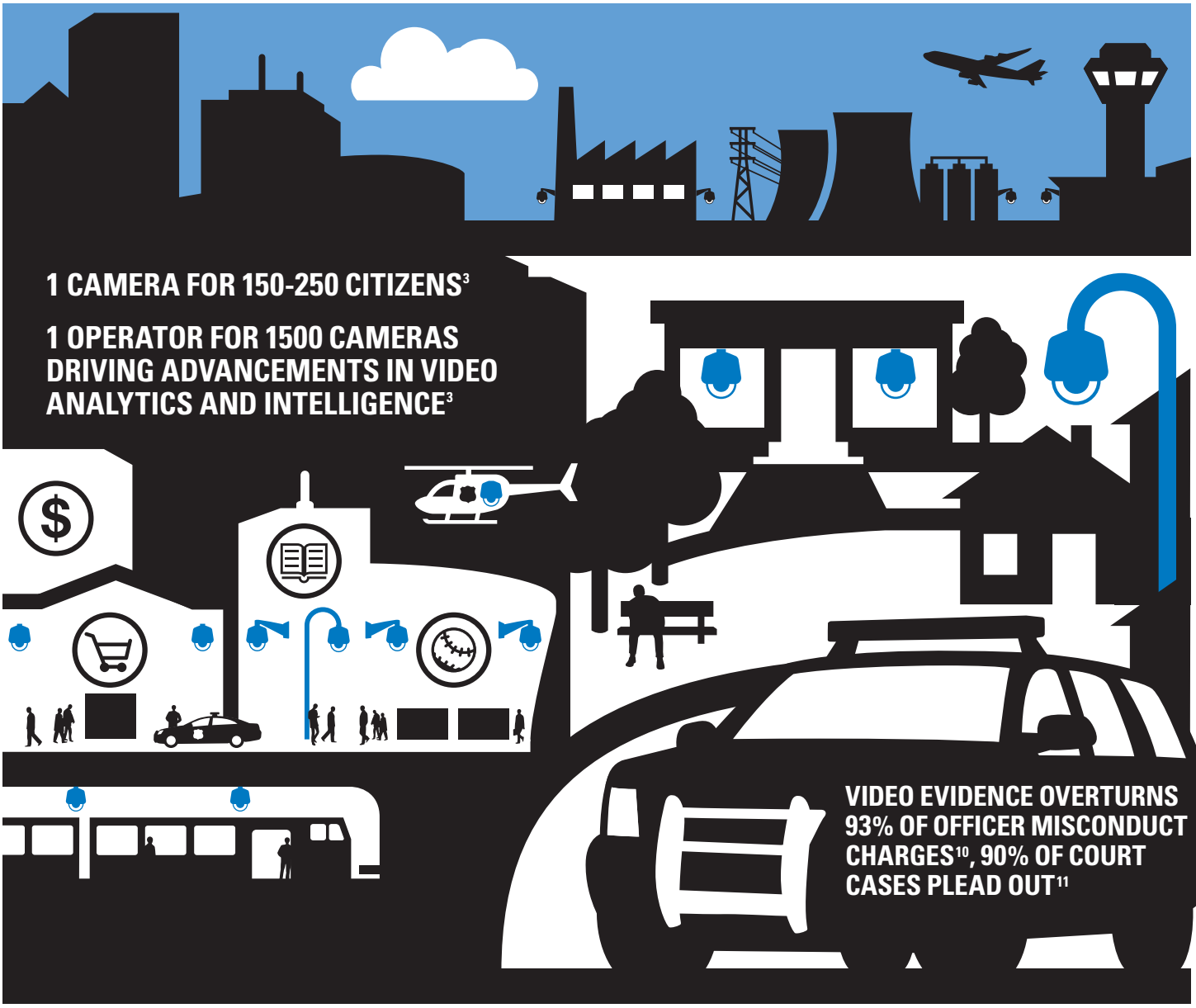
SECURITY: THE EYES HAVE IT

As the world becomes increasingly security conscious, municipalities of all sizes are discovering that there's safety in sight. Real-time video surveillance systems are proving to be one of the most effective methods of addressing a wide range of security challenges in both the public and the private sectors. In the January 2012 "Critical Issues in Policing Series", the Police Executive Research Forum (PERF) shared information from police chiefs about how they are using video and the impact that it is having on their communities.

Agencies have looked to deploy surveillance cameras for finite periods of time to address high-crime hot spots and then move them to a new area in the city. When they try to move a camera, there's an immediate outcry, and it has become increasingly clear that cameras can't be moved due to community objections.

Government leaders say that one of the biggest obstacles in establishing a city-wide video surveillance system isn't the technology itself, but rather the intergovernmental agreements and memoranda of understanding across agencies, with schools and the private sector, that are required.

To ensure proper use of video and protection of privacy, government and public safety officials are also requiring First and Fourth Amendment training as a best practice for all surveillance system users.



KEY TRENDS

BIG DATA MEETS PREDICTIVE POLICING

Government and public safety communications centers are rapidly evolving into highly complex, multimedia command and control theaters. These centers have to manage a deluge of information coming from citizen-generated inputs, city data sources, public safety sensor networks and surveillance feeds, as well as massive volumes of historical records. It is no wonder that government agencies are focusing increasing attention toward bringing automated intelligence and analytics into their command environments to help analyze and interpret the mass amounts of information. 70% of departments are using some form of predictive policing today – using crime mapping software, identifying serial offenders, or using historical data to allocate resources to prevent crimes. Public safety leaders recognize the urgency to manage the flood of data to bring focus toward critical content, alert users to potential threats and emerging situations and – most importantly – present information in a way that enhances the users' performance rather than overwhelming their cognitive loading. 90% of departments plan to increase their use of predictive policing over the next five years.

70%
DEPARTMENTS ARE USING SOME FORM OF PREDICTIVE POLICING[3]

90%
DEPARTMENTS PLAN TO INCREASE THEIR USE OF PREDICTIVE POLICING OVER THE NEXT FIVE YEARS[3]

A MOVE TO THE CLOUD

One of the most aggressive challenges for government and public safety leaders is managing the pace of technology change while pressed with significant budget limitations. There can be tremendous complexity and scale involved with the technology solutions that meet the expectations of citizens, responders and government workers who know that there are tools and information out there that can help them do their jobs better and more safely. There is also a growing appreciation among government leaders that they do not have the resource pool with the necessary skills to support these next generation platforms, and it is increasingly challenging to find and hire the right talent to take on the ongoing management and operations of these systems. Responding to the current economic conditions, government and public safety leaders are increasingly looking to shift from more capital-intense, customer-owned business models to operational expense-focused, managed service models where a predictable, recurring fee takes the place of a large upfront spend. In many instances, agencies have also begun to follow a broader institutional trend toward off-premise computing models such as cloud computing and software-as-a-service. 4 in 10 Government IT leaders report that they plan to invest in cloud technology services in the next two years.

4 IN 10
GOVERNMENT IT LEADERS SAY THEY WILL INVEST IN CLOUD TECHNOLOGY SERVICES IN THE NEXT TWO YEARS[4]

THE NEW THREAT MATRIX

While governments and enterprises continue to ramp up spending on information security compliance and data loss prevention, intrusions are rising. Over the past 6 years, the number of cyber-security incidents reported by government agencies has increased by nearly 680 percent. Some of the biggest data breaches in history occurred in 2011. Today, polymorphic attacks – capable of modifying themselves with every execution – are ubiquitous. While many organizations would like to think their most sensitive data or mission critical information is inoculated, it is becoming increasingly clear to city leaders that they are not immune.

OVER THE PAST 6 YEARS, THE NUMBER OF CYBER-SECURITY INCIDENTS REPORTED BY GOVERNMENT AGENCIES HAS INCREASED BY NEARLY 680 PERCENT[12]

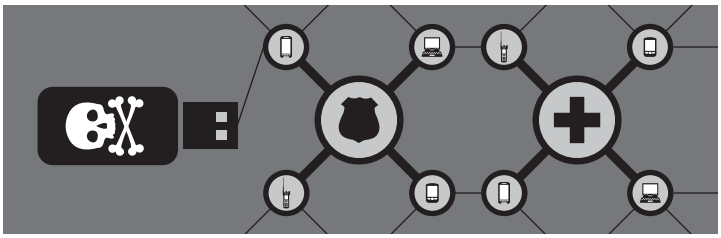
Governments around the world are being increasingly targeted, and The Department of Homeland Security has reported significant increases in the number of cyber incidents and advanced persistent threat activity affecting critical infrastructure.

As government employees bring their own devices to work, we expose government enterprise networks to a new world of vulnerabilities. Government mobile workers are more proficient than ever with technology and more dependent on their mobile devices. Unfortunately, most of them do not appreciate their role in securing the devices and data government relies on.

With increased electronic engagement with the public through eGovernment initiatives, introduction of new network access points through smart meters and city appliances, and a growing pervasiveness of Internet connections over public wireline and cellular data networks, the number of incidents are predicted to increase.

The security requirements of the government and public safety community are driving formalized guidelines for comprehensive security practices that establish concentric rings of protection and holistically address all the people, policy, process and technology aspects specific to government communications.

The subject of information security lives in the top ranks of the government CIO agenda as senior leaders work to ensure the establishment of an effective communications security framework that is up to the challenge of our new mobile communications environment and the ever changing threat matrix it invites.



FRENCH GOVERNMENT

SUCCESSFULLY TARGETED BY SOCIALLY ENGINEERED EMAIL CAMPAIGN – DEC 2010 - MAR 2011

RESULT: REMOTELY CONTROLLED MINISTRY COMPUTERS FOR OVER 3 MONTHS

US DEPARTMENT OF DEFENSE

FOREIGN INTELLIGENCE AGENCY PLACED MALICIOUS SOFTWARE ON A USB FLASH DRIVE – EARLY 2008

RESULT: SIGNIFICANT COMPROMISE OF CLASSIFIED MILITARY COMPUTERS

AUSTRALIAN GOVERNMENT

PARLIAMENTARY COMPUTERS ACCESSED OVER A PERIOD OF A MONTH – FEB - MAR 2011

RESULT: ACCESSED PRIME MINISTER, FOREIGN AND DEFENSE MINISTER EMAILS

SOUTH ASIAN GOVERNMENT

CYBER-ESPIONAGE OPERATION INFILTRATED 1295 COMPUTERS IN 103 COUNTRIES – MARCH 2009

RESULT: ACCESSED MAIL SERVERS TO VIEW SENSITIVE INFORMATION

INTERNATIONAL MONETARY FUND

SOPHISTICATED CYBER ATTACK WITH SOFTWARE WRITTEN SPECIFICALLY TARGETING IMF – MAY - JUN 2011

RESULT: VISIBILITY TO SENSITIVE ECONOMIC AND POLITICAL INFORMATION

WHAT'S NEXT

Two significant regulatory outcomes driving the industry pivot that is taking place as a result of these technology trends is the drive toward Next Generation 9-1-1 and Public Safety LTE broadband. One is about collecting more of the data that surrounds us and applying analytics and correlation to operationalize the intelligence; the second is about being able to instantly distribute that intelligence to the field to help mobile workers be safer, smarter and faster.

NEXT GENERATION 9-1-1

ANSWERING THE NEW CALL FOR HELP

We don't use our smartphones just for talking anymore. We text. We tweet. We send photographs. We upload videos. It's only natural that we should be able to call for emergency help and engage with our government service organizations in the same ways we communicate every day. Next Generation 9-1-1 (NG9-1-1) refers to an initiative aimed at updating the 9-1-1 service infrastructure in North America that has been in place since the 1970s. The aim is to improve the public emergency communications services to support the modern, mobile communications revolution.

The National Emergency Number Association (NENA) first identified the need for NG9-1-1 in 2000, and the initiative kicked into high gear in 2006 when the United States Department of Transportation decided to study the existing 9-1-1 infrastructure and determine how it could be adapted to capitalize on today's technology advancements.

NG9-1-1 systems are comprised of Emergency Services IP networks (ESInet), hardware, software, data, operational policies and procedures that will enable the public to transmit text, images and video to a 9-1-1 emergency call center, which is also called a PSAP (Public Safety Answering Point). The PSAP of the future will also be able to receive data from personal safety devices such as advanced automatic collision notification systems, medical alert systems, and environmental sensors.

NG9-1-1 provides a secure environment for emergency communications ensuring the delivery of calls, messages and data to the appropriate PSAP and any other appropriate emergency entities. The new infrastructure will support "long distance" 9-1-1 services, as well as transfer of emergency calls to other PSAPs – including any accompanying data. In addition, PSAPs will also be able to issue emergency alerts to wireless devices in a particular area via voice or text message, and to highway alert systems.

PUBLIC SAFETY LTE

STREET-READY DATA

Video, images, text messages, location data and electronic records are becoming critical sources of information to support public safety operations; in the field and at the point of engagement. Commanders, dispatchers, and front line responders rely on this data to both support critical incident and provide the productivity boost that delivers the force multiplier benefits for agencies tasked to do more with less. Recognizing the need for a highly available and reliable broadband network that will not be adversely impacted by congestion peaks on public carrier networks – which are known to occur during those times public safety requires access the most – governments are turning toward private, dedicated broadband solutions.

Fueled by the open standards environment and the promise of scaled economies from public carrier adoption, government organizations worldwide have selected LTE (Long Term Evolution) as the pre-eminent global standard for public safety mobile broadband.

Government leaders have high expectations for the benefits they believe should be achieved by deploying public safety broadband. These benefits must certainly include protecting first responders and helping them be more efficient, but there is also an expectation that these broadband systems will support the broader community of mobile government workers and bring to life new possibilities for smart sensors and metering applications.

Human services case management, electronic work orders and automated scheduling, inspections and code enforcement, asset management and maintenance – are all government broadband use cases that city leaders believe can help them boost their neighborhood vitality programs.

In February 2012, the United States Congress enacted The Middle Class Tax Relief and Job Creation Act which contained provisions for creating a nationwide interoperable broadband network to serve public safety. The governing entity for the deployment and operation of this network will be a new, independent authority within the NTIA called FirstNet (First Responder Network Authority). FirstNet will hold the spectrum license for the network, and is charged to deploy and operate the network, in consultation with federal, state, tribal and local public safety entities.

The Act provides $7 billion in funding toward deployment of this network, as well as $135 million for a new State and Local Implementation Grant Program administered by NTIA to support state, regional, tribal and local jurisdictions' efforts to plan and work with FirstNet to ensure the network meets their wireless public safety communications needs.

CONCLUSION

We've just scratched the surface of data, and it's already changing everything. Inputs from smartphones, from social media, from cameras, sensors and alarms – from everywhere – offer the promise to help government agencies see, hear and do more with less.

But capturing that data is just the start. The real inflection is when agencies can operationalize the data that surrounds them so they can make more intelligent predictions, offer more targeted counteractions and establish a more enduring safety.

Today, next generation technologies are transforming government and public safety organizations by allowing them to collect the information flowing between citizens, responders and agencies, make it actionable and securely distribute it across mission critical devices and easy-to-manage networks.

It's the technology and expertise that turns noise into information, information into intelligence, and intelligence into safety. And it's how to do the absolute most with less – building safer cities, counties and states, and communities that thrive.

SAFER CITES THRIVING COMMUNITIES WHITE PAPER SOURCES

1. "What Cost-of-Crime Research Can Tell Us About Investing in Police," RAND Center on Quality Policing, 2010
2. "Crime, Urban Flight, and the Consequences for Cities," The Review of Economics and Statistics, Julie Berry Cullen and Steven D. Levitt, May 1999
3. "Critical Issues In Policing Series: How Are Innovations in Technology Transforming Policing?" Police Executive Research Forum, January 2012
4. Motorola Government and Public Safety Data Communication Survey, January- February 2012
5. "Maryland's Pursuit of the Paperless Patrol Car: Using Mobile Technology to Foster Interagency Collaboration and Improve Officer Safety", The Police Chief, June 2009
6. "Automated License Plate Recognition Investment Justification and Purchasing Guide," PIPS Technology, 2008, page 10
7. Motorola Solutions Misdemeanor Processing Time Analysis, 2010
8. "Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention," Urban Institute, September 2011
9. Measuring the Effects of Video Surveillance on Crime, Jordan Downs, Los Angeles, Calif., 2006-2007
10. "The Impact of Video Evidence on Modern Policing", International Association of Chiefs of Police, 2005, page 26
11. New IACP in-car camera spec recommendations and what they mean for your department, governmentvideo,com, 2009
12. "Cybersecurity: Threats Impacting the Nation", United States Government Accountability Office, April 2012

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. **motorolasolutions.com**

MOTOROLA