INTRODUCTION OF DIGITAL INVESTIGATION METHODS

Transforming Law Enforcement through Digital Technologies

By John Wright

A Digital Government Series by Unisys Corporation
The digital revolution is disrupting the traditional way of conducting business across public sector and private enterprises. While the early adopters in digital transformation have been industries such as financial services where large data volumes already exist in digitized form, its most powerful impact could very well be in the public sector.

Digital policing and digitization of law enforcement are two such examples. The overall objective of policing remains the same; safeguarding citizens, so imagine the impact if new and disruptive technologies could be harnessed by law enforcement agencies to fight crime and protect the people.

Digital technologies not only stand to transform existing law enforcement processes but open completely new and previously unavailable avenues to fight crime. Examples include increased citizen engagement, predictive policing using data analytics, enhanced use of mobile and social media intelligence, and leveraging of cloud technologies for collaboration, information storage and investigation.

**DIGITAL INVESTIGATION**

Law enforcement agencies are investing in technology to capture, store, and access data, including incident and crime report, images, and video from citizens both for speedier and more effective investigations but also to build better relationships and thereby generate a willingness to provide vital intelligence. Digital investigation is the process of collection, preservation, analysis and presentation of evidence from various digital devices. According to one of the leading research firms, the global digital investigation market is expected to grow at a compounded annual growth rate of 11.3% and will reach $3.2 B by 2020 from $1.8 B in 2015.

Understanding the investigation process and modeling it to meet the requirements of and exploit the opportunities generated by digitalization is key. Digital investigation includes complete evidence management and security processes, analysis frameworks, inter/intra/cross agency communications and modes to effectively and efficiently interact with the public. In addition, a digital investigation solution should be scalable and flexible to allow alignment with ever changing requirements and easy integration with current or future police systems.

There are number of analytical techniques which can be used to improve the effectiveness of digital investigations. For example, US law enforcement officers use complex algorithms to analyze social media feeds together with historical crime data to generate predictive maps. Identifying and interpreting specific events across large data sets and building those events in a visual timeline helps investigators understand the event sequence. Visualization tools help convey output and progress to police leaders, resource managers, partners and the public in a format that meets their particular audience needs. Other techniques such as link analysis help in evaluating the connections between people and evidence sources. This helps in automatically tracking and displaying connections between people and entities such as credit card numbers or phone numbers. Link analysis has proven effective in finding relationships between unrelated people and events.

Traditional methods of detecting, preventing and solving crimes are in need of more advanced approaches. The investigation process is complex starting with collection of evidence and culminating in a case presentation in a court of law which involves multiple agencies and individuals. The complexity is a result of old technologies that require customization to get around limited capabilities for preservation and analysis of evidence, and communication of investigation progress securely and effectively with multiple parties including citizens.

Given technological advancements, it is imperative that police departments move with the times to transform their capabilities. The police must be digitally and dynamically connected to the public, practice predictive policing, and fully harness the power of information technology to assist them in their investigations. Leveraging technology can help police by providing ‘real-time’ access to evidence, enabling them to spend more time in the field and at the crime scene to coordinate their investigation efforts more effectively.

More recently, law enforcement agencies worldwide are beginning to invest in digital investigation techniques and technologies. Social media monitoring tools are widely used by investigation agencies to identify suspects and witnesses, to gather and keep track of a suspect’s location and to learn of their social activity and relationships. One of the surveys conducted by the International Association of Chiefs of Police (IACP) listed almost 82% of law enforcement agencies use social media for criminal investigations. This demonstrates that investigation of digital evidence and the trail it creates have become just as important as investigation of physical evidence.
Advanced analytics is increasingly being leveraged in digital investigations. Using big data tools, law enforcement agencies are able to analyze large volumes of unstructured data to understand criminal patterns and behavior and proactively prevent crimes. Cognitive computing, the use of machine learning and artificial intelligence, enables agencies to reach higher levels of analytical maturity. Utilizing data for insights and presenting those insights for strategic decision making for operational readiness is the goal. The outcome is reduced crime and criminality.

In addition, analytical tools iteratively allow officers to understand how to overlay crime science and criminological practice and interpret the results. Such analytical tools help provide a feedback loop whereby the control, impact, and lessons learned from the data can be interpreted, analyzed and fed into assessments and requirement setting.

ADDRESSING THE CHALLENGES TO TRANSFORMING THROUGH DATA AND TOOLS

While digital technologies have the potential to transform the investigation process, challenges related to scaling operations, data analysis and security need to be adequately addressed.

Data mining is arguably the biggest challenge which law enforcement agencies face. Leading social media platforms Facebook and WhatsApp have more than 1.5 billion and 1.0 billion monthly active users respectively. The number of devices (PCs, tablets, ultra-mobiles and mobile phones) used to access these platforms is expected to reach 2.4 billion units in 2016. With so much data available from different open sources, law enforcement agencies are grappling with how best to collect, collate and analyze all the different pieces of digital evidence ensuring they add value to, and not confuse, case investigation. Additionally, in order to improve admissibility, law enforcement authorities always need to be sure that the veracity and non-repudiation of digital evidence is maintained.

Outdated technology and workflow tools are limiting law enforcement agencies from leveraging the full value of data that is already available. Today, data are separated across various multiple isolated systems, jurisdictional boundaries, law agencies and state and local citizen service agencies. Currently, advanced data analytics techniques are not fully utilized, constraining the investigation process as well as proactive crime prevention.

When data sets are integrated, predictive analytics can help the police identify patterns followed by criminals and prevent crime, improve investigation, leading to better detection of incidents.

From a technical standpoint, encrypted data and access to data in mobile devices is another huge challenge for digital investigation teams. Based on how recent legal battles are playing out, there is a possibility that data contained in a digital device may never become available for law enforcement. As an example, in October 2015, Apple stated in a US court that it would be impossible for it to access data on a locked iPhone running iOS 8 or later, although this was resolved through third party intervention. The gravity of the situation is so high that bipartisan US congressional legislation could be introduced in the near future to create a national commission on security and technology to address the growing concern over steganography – another variation of the encryption challenge wherein a secret message is hidden between ordinary messages and is extracted at its destination.

Recognizing the benefits of information-sharing securing sensitive data held in police databases and preventing breaches cannot be overlooked regarding digital investigative procedures. While it is important that data be accessible and available for investigations, it is imperative that intelligence and evidence collected is stored and secured with utmost secrecy and confidentiality. Recently there have been several instances of breaches at even the most reputed police departments, causing data protection regulations to become more stringent. In similar commercial market developments in December 2015, the European Union agreed to a new set of legislation that could impose a fine of as much as 4% of an organization’s global turnover for breaching its new set of data protection laws. This regulation is expected to be adopted in 2016 with its enforcement expected to begin in 2018.

Another challenge faced by digital investigation teams is access to data stored in a cloud environment. In a June 2014 report, the US National Institute of Standards and Technology categorized these challenges into nine broad areas including architecture, data collection, analysis, anti-investigation, incident first responders, role management, legal, standards and training. Additionally, different sets of state and national legal systems, country or state specific privacy laws and data protection regulations impact the digital investigation process.
CONCLUSION
Digital investigation is emerging as one of the key areas in policing that stands to gain from the digital revolution. Digital policing is about how information is captured, used, and made available across boundaries, whether they are local, business, or geographic and how the deployment of technology can be used to deliver those requirements efficiently and effectively. With the speed of technological change, it is critical that law enforcement agencies be equipped with new digital tools to counter and prevent crime and safeguard their citizens.

Digital investigation is a new disruptive way to provide a scientific edge not only to decipher complex crimes but also aid in their prevention. In parallel, it also provides law enforcement agencies with a robust medium to make sure that there is strong inter, intra and cross agency collaboration in place to take investigations to their logical conclusions.

ABOUT UNISYS
Unisys is a global information technology company that specializes in providing industry-focused solutions integrated with leading-edge security protocols to clients in the government, financial services and commercial markets. Unisys offerings include security solutions, advanced data analytics, cloud and infrastructure services, application services and application and server software. For more information, visit: www.unisys.com

ABOUT THE AUTHOR
John Wright is the senior director, Justice and Law Enforcement for Unisys Global Public Sector. He has more than 30 years of experience in law enforcement and is an internationally recognized authority in the prevention of terrorism and violent extremism. His insight, leadership and opinion is regularly sought by government and commercial organizations. He has spoken at more than 50 conferences nationally and internationally on counter terrorism matters.

For more information on Unisys’ Digital Government solutions and impact, visit: WWW.UNISYS.COM/DIGITAL-GOVERNMENT