2017

The BJA Executive Session on Police Leadership **is a multi-year endeavor started in 2010 with the goal of developing innovative thinking that would help create police leaders uniquely qualified to meet the challenges of a changing public safety landscape.**

In support of an integrated approach to creating safe and viable communities across America, the project directors recruited 20+ principals from a range of disciplines. The principals, in turn, led national field teams of practitioners focused on the work of policing and the organization of the future.

To gain new insights on leadership, the *BJA Executive Session on Police Leadership* engaged police chiefs in documenting their own paths and invited leaders to participate in various audio and video forums to tell their stories and discuss the future of policing and police leadership.

Please visit our website, http://bjaleader.org, to learn more about this project and to access a broad array of interactive, multimedia resources.

The principals are supported in their work by a team that includes project co-directors Darrel W. Stephens and Nancy McKeon, and BJA Senior Policy Advisor Steve Edwards.

The Future is Here and We are Already Late: Leadership Challenges with Emerging Police Technology

by
Nola Joyce, Phil Lyons, Michael S. Scott and Peter Sloly

Contents

Abstract

This paper explores the leadership challenges for police executives of emerging police technology. Such challenges range from deciding to explore the use of new technology to the deployment of these technologies. Basic questions of cost and benefit are still present but today the questions of privacy and the ethical use of

technologies are of growing importance. We explore the current and possible future scenarios for police technology. To manage these scenarios, we offer a broad ethical framework and some general principles. This guidance is general because the specific questions concerning the use of new technology will emerge along with the technologies. However, we believe that these principles and the ethical framework supporting them can be used to start a discussion about whether a new technology should be deployed and if so, how it should be used. We believe that the next step for policing is to develop a specific digital ethical framework that police leaders and their stakeholders can use when considering the use of technology; collection of data; analysis of data to create information; and the consequences of using that information for deployment, tactical, and strategic use.

Introduction

There is no doubt that technology plays, and will continue to play, a critical role in policing. It is also true that police technology and its use is moving faster than the laws, regulations, and ethical guidelines governing it. Often, the use of new technology can have unintended consequences for major policing objectives other than the ones the technology was intended to help police achieve.

> *Thus, despite (and because of) the centrality of technology in policing, law enforcement agencies face major challenges including determining the effects of implementing various technologies; identifying costs and benefits; examining unintended consequences; and exploring the best practices by which technology can be evaluated, acquired, maintained, and managed (President's Task Force on 21st Century Policing, 2015).*

These are the leadership challenges facing police executives today and into the future. In fact, we suggest that these challenges will only grow in number, gravity, complexity, and urgency as we move into the mid-21st Century.

Leading a police department today is a risky business. Policing has always been fraught with difficult challenges. However, technology has increased both the opportunities and challenges. New risks can come from addressing alternative narratives about a police shooting on social media, releasing policies governing the use of body-worn cameras, or using a software algorithm for predictive policing. Wrapped around these challenges are complex policy dilemmas, such as:

- balancing crime fighting with building public trust,
- responding to the demand for public security while safeguarding individual privacy,
- reconciling the relative costs and benefits of technology and human service delivery,
- weighing community demands against professional opinions,
- increasing investments in *catching* cyber-threat actors versus increasing investments in *defending* your agency from them,
- creating a central specialized cyber unit versus creating a more decentralized model where all members are able to acquire greater levels of cyber competency, and
- developing internal cyber competency versus out-sourcing this function to the private sector.

These are wicked policy issues because there is no clear right answer and yet police executives are expected to address them on behalf of their departments and communities.

It is our hope that the digital ethical framework and guiding principles contained in this paper will help police executives lead their departments and communities through these difficult policy issues when considering a new technology. We begin by offering a short review of today's police technology followed by a future scenario of how technology may change policing. Then we offer a digital ethic framework developed for the private sector[1] and suggest that it can be a model for a similar framework for policing. Finally, we offer five principles we believe police leaders can use now to better navigate today's turbulent times and make decisions about technology.

Police Technology

Today's Landscape

The 2013 Law Enforcement Management and Administrative Statistics (LEMAS) survey of a representative sample of state and local law enforcement agencies found the following (Reaves 2015):

- The percentage of local police departments that authorized their officers to use conducted energy weapons such as Tasers increased from 60% in 2007 to 81% in 2013.
- About a third (32%) of local police departments used body-worn cameras in 2013.
- About 1 in 6 local police departments used automated vehicle license plate readers in 2013, including a majority of those serving a population of 25,000 or more.
- About two-thirds of departments had patrol officers transmit incident reports electronically from the field to a central information system.
- Among departments serving 10,000 or more residents, more than 90% had their own website and more than 80% used social media.

There is reason to believe that these numbers have increased over the past four years. Technology, as these statistics suggest, is important to policing.

One of the incongruities highlighted by the above facts is that 90% of the departments serving a population of 10,000 or more have a web site and 80% are using social media but only 66% have automated field reporting. The Federal Bureau of Investigation and the Bureau of Justice Statistics are actively supporting police departments in converting to the National Incident-Based Reporting System (NIBRS) by 2021, a "new" technology introduced in the mid-1980s. Policing is so far behind in some areas of technology and at the same time, their use of newer technology has raised concerns in the public discourse. In some instances, police adoption of technology lags well behind its original development and need, as in the case of the national crime-reporting system. In other instances, full consideration of the fiscal and ethical implications of new technology lags behind its widespread adoption, as in the case of body-worn cameras. It seems as though policing has one foot still firmly planted in the late 20th Century with the other leaping into the 21st Century. This dichotomy complicates the

[1] The business-consulting firm Accenture (2016) developed the digital ethic framework we reference.

decision-making environment. The knowledge and practices developed in the 1990s may not be sufficient for dealing with 21st Century technology.

Visiting a Real-Time Crime Center or Fusion Center in a major jurisdiction, you would likely find:

- hundreds to thousands of surveillance cameras monitoring the public streets and public transportation,
- a gunshot detection system that alerts on the sound of a gunshot,
- feeds from automated license plate readers that read and alert on plates of interest and computers that store millions of plate numbers with the location and time they were detected,
- facial recognition software for identifying persons of interest,
- a unit that monitors and analyzes public social media feeds, and
- access to numerous databases, many automatically cross-referencing one another in search of leads to criminal activity.

We can add to the above list the technology used in the field, such as hand-held devices like tablets, body cameras, and fingerprint and retina readers. In considering today's policing technology, many of the policy issues are in bold relief; others are less readily apparent.

Each of these technologies operates, for the most part, within its own system and their associated data are stored separately. The linking of multiple technologies is rare, but is beginning to occur. For example, gunshot detection systems and cameras are increasingly being linked. In some jurisdictions, a camera will turn automatically toward the sound of the gunshot, allowing a real-time view of the scene. As cloud computing becomes more competitive and cheaper, and big-data analytics begins to trickle into the public sector, multiple technologies can be linked and the data from those technologies can be analyzed in ways that will lead to new insights and investigative leads. Some people will find this possibility exciting; others will find it scary and an overreach of government.

Police technology is not just about hardware but also software and the integration of data to create information. Predictive policing is based on the premise that data already collected by the police can be fed into an algorithm that can predict when and where crime is likely to occur or one that can predict who is likely to offend and who is likely to be a crime victim. However, civil libertarians and civil-rights champions have expressed concern that predictive policing will intrude unnecessarily into people's private lives and exacerbate biased policing (Wilson, 2015). The challenge is compounded when the algorithms themselves are kept secret, and thus inaccessible for assessing the validity of their assumptions, but the predictions they generate are not (Perry et al., 2013; Miller, 2017).

The Future Scape

We can imagine policing in eight to ten years to see how technology could shape policing. Picture a police officer who just downloaded her daily brief[2] and is entering her driverless

[2] The Metropolitan Police Service in the U.K. is developing One Met Digital Policing Strategy which will deliver applications only available in the police station to mobile devices (Parker and Andrews, 2017).

patrol car[3]. The car is equipped with external cameras[4], environmental sensors[5], and a companion drone[6]. The car's route is programmed along with maximum speeds. The officer can take over the controls. When doing so, she must notify the command center and justify taking control. There is a heads-up screen embedded in the windshield[7]. The car's computer will respond to the officer's verbal requests and can record notes and reports dictated by the officer accompanied with any associated information the officer references.

Her routine day could look like this:

> As the officer is riding in the car, information is flashed on the car's heads-up screen. An alert is flashed that she is traveling through an area with a recent robbery pattern occurring during this time period. Pictures of robbers who are known to frequent the area are displayed. Augmented reality tags the locations of recent robberies on a virtual map[8]. The real-time analysis of social media feeds provides the officer with the level of social sentiment surrounding the robberies and provides possible witnesses and intelligence about the crimes. The officer is asked to stop into high-risk robbery-target businesses to alert proprietors and assess whether robbery-prevention measures are in place.
>
> A notification comes across that Billy, who lives in the house coming up, has missed a lot of school and whose name has appeared in a local crew's social media posts. The predictive analysis suggests Billy is at high risk of dropping out of school and becoming criminally involved. The officer has access to Billy's recent school attendance record and social services contacts with his family. The officer is asked to stop at the house and have a talk with Billy and his parents about his risky behavior, share information about some youth programs, and offer a referral.
>
> Once back in the car and further along the beat, another notification comes up suggesting that Mrs. Smith at 1200 Main Street may be an emerging community leader based on her 311 requests, attendance at recent community meetings and social media postings. The officer is asked to make an effort to introduce herself to Mrs. Smith and determine whether any police-community collaboration is warranted.

[3] The Dubai police announced that by the end of 2017 they will be deploying mini autonomous police cars equipped with thermal imaging, license-plate readers and paired with companion drones with facial-recognition to patrol the streets and to help identify and track suspects. They are already using a police bot to help monitor tourist attractions. Both the mini police cars and police bot can be controlled by a human through a computer dashboard. Dubai plans to have 25 percent of their police force made up of robots by 2030 (Shaban 2017).

[4] The Palo Alto police department equipped cars in their marked fleet with four external cameras that provide a 270-degree view around the car. The cameras record and the video is displayed on the monitor in the car and wirelessly uploads the data (Coppola 2015).

[5] In 2010 the Washington, D.C. police field-tested a mobile radiation detection system (Long 2010).

[6] Dubai is pairing companion drones with their autonomous police cars (Shaban 2017).

[7] Maryland State Police in 2002 tested a 'smart car' that included a heads-up display mounted on the windshield that displayed the results of criminal background checks and license information (Potter 2002).

[8] In 2016, the U.S. Department of Homeland Security funded ten startups for research and development of wearable technology for first responders. Included is a technology consisting of rugged wearable devices that stream video and display data with augmented reality overlays (Leonard 2016).

Problem locations along the beat are tagged through augmented reality[9]. The officer is expected to work with stakeholders on addressing problems at these locations. There is computer-assisted guidance on how to address the specific problems identified for each location[10]. As the patrol continues, information and pictures of wanted persons known to frequent the areas are made available. If a wanted person is located through facial recognition software[11] embedded in the car's external cameras, an alert sounds and the criminal history of the individual is prominently flashed on the head's up screen.

A call-for-service is received and the car routes itself to the address. As the officer arrives, she sees a crowd growing with two men in the middle fighting. The sensors woven into her uniform are picking up her vital signs[12]. As her stress level increases, as measured by her blood pressure and heart rate, her command center and supervisor are sent an alert. Both begin to monitor the officer. The officer gets out of the car and releases her companion drone. The drone flies ahead of the officer as she begins to move toward the crowd. Her body camera automatically turned on when she opened the car door. As she walks toward the crowd, the facial recognition software associated with her body camera is sending information to the command center and will alert the officer if a violent offender is identified. The drone is sending pictures to the officer and the command center. It is obvious, as the officer gets closer, that the fight just involves two men but there are definite sides forming in the surrounding group of about ten people. The officer's heart rate and blood pressure goes up and she touches her weapon. All of her weapons are biometrically identified with the officer and will not discharge except by her[13]. The increase in vitals and the fact she touched her weapon produced two alerts and resulted in her supervisor responding to the scene and back-up being dispatched. The officer directs the drone to announce her presence and that the crowd is under video surveillance. The drone conveys the demands of the officer for the crowd to disperse, in both English and Spanish. The noise of the crowd is growing. The officer directs the drone to sound a loud blast of noise and warn that, if necessary, the drone will release a round of pepper spray into the crowd. This decision by the officer resulted in a second backup car being dispatched to the scene. The officer was gaining control of the situation just as the supervisor and back-up arrived.

The audio and video information captured by all the officers from the time the first officer was dispatched to clearing the scene is automatically compiled by software and produces a timeline and a digital report that also captures the officers' reactions and any known offenders present at the scene. The supervisor reviews the report and asks the officer to dictate a few sentences that explains how she reacted to the situation and why she

[9] Some computer-aided dispatch (CAD) systems have been programmed to identify addresses with a history of calls for police service or which are being addressed by other officers as problem locations.
[10] Electronic databases such as the Problem-Oriented Guides for Police, CrimeSolutions.gov, the Oregon Knowledge Bank, the Evidence-Based Policing Matrix, and the JDiBriefs are among the policing information repositories currently available.
[11] New York City announced that it will deploy facial recognition software and license plate readers at sensitive points on bridges and tunnels leading into the city (Lee 2017).
[12] Smart fabrics are available now that can constantly track heart rate and even monitor emotions (Sawh 2017).
[13] NYPD said they would help evaluate and assess designs submitted to the Smart Gun Design Competition (Carrega 2017).

felt it necessary to warn about the use of pepper spray. The officer dictated the additions to the report and the supervisor digitally approved the report.

Because tensions in this neighborhood have been high over the past months, analysts at the Real Time Crime Center begin running all the data obtained – videos, audios, facial recognition, social media communication occurring in that location and during that time, and drone footage. This analysis is then fed into a computer program that produces known connections among identified individuals[14]. This analysis will produce a list of people for the neighborhood officers to contact and work with to ease the tensions.

While the above scenario might sound farfetched, all of the technology mentioned in it exists. The U.S. Department of Homeland Security Science & Technology, the Pacific Northwest National Laboratory, and the private innovation design firm Continuum are already presenting many of these technologies as part of their future view of law enforcement technology[15].

The question is not whether the technology described above will exist, but rather should police use it when it becomes available. Just because they can, should they? And, if so, how should it be used? The answers to these questions should be driven by a digital ethics framework and a set of guiding principles.

Digital Ethics and Principles

Digital Ethics Framework

Some companies are discussing the social impact of technology innovations (Shingles, Briggs, O'Dwyer, 2016) and how to develop and keep consumer trust through digital ethics (Accenture, 2016). "Organizations should consider the ethics and morality of applying technologies – beyond traditional risk concerns of security, privacy, regulatory, compliance, safety, and quality" (Shingles, et al., 2016, 113). For these authors, successful businesses must understand the role that their emerging technology has on driving transformative social change and how it can be built and used for positive social impact. They argue that a social impact mind-set is necessary to ensure growth and longevity of a company because it helps to protect and create value. Such an orientation also requires exploring the unintended social and ethical consequences of new technology and mitigating those consequences as needed. We suggest that, whereas this is arguably necessary for business, it is inescapably true for the public sector, particularly the police.

The premise behind digital ethics is that "new products and services must be ethical- and secure-by-design" (Accenture, 2016, 58). Businesses that get not just digital security but also digital ethics right will create high levels of consumer trust and loyalty. Digital ethics is more than data ethics. Data ethics refers to governance of data integrity, handling, control, and source of data. The regulations governing the capture and use of crime and arrest data already provide police executives the basics of data ethics and similar governance is often applied to new technology data. However, digital ethics is broader and includes how technology and the

[14] The Chicago Police Department worked with Dr. Papachristos, who used social network analysis, to identify the people who were most likely to shoot someone or to be shot (McDonald, 2013).
[15] See www.futureoffirstresponse.net for further information.

data are used and the outcomes of that use. Figure 1 illustrates the difference between data ethics and digital ethics.

Figure 1: Data Ethics vs. Digital Ethics[16]

- Data Ethics is the governance of data including integrity, security, and control of data.
- Digital Ethics is the governance of the use of technology, the data and the resulting information.
- Data and digital ethics combined helps to increase digital trust within the organization and with stakeholders.

Data Ethics

Digital Ethics

Digital Trust

- ✓ Data Integrity
- ✓ Device Security
- ✓ Application Security
- ✓ Infrastructure Security
- ✓ Identity Management
- ✓ Cyber Defense
- ✓ Governance and Compliance

- ✓ Code of Digital Ethics
- ✓ Ethical Decisions in Use
- ✓ Ethical Algorithms
- ✓ Transparency
- ✓ Data Sharing Governance
- ✓ Privacy
- ✓ Implications for Harm

Digital ethics involves the implementation of ethical controls on the technology and the use of data. It raises the questions of accessing the impact of new technology, the ethical development and use of algorithms, transparency, data sharing, anonymity and data sharing, and privacy. These are not new issues but the importance of these issues is raised to new levels. Police must continue to improve efforts to ensure security of the data they capture and the integrity of that data. But beyond ensuring the integrity of data collected, police must also assure the public that the data they collect is truly necessary for promoting public safety and security. Police leaders must also begin thinking about digital ethics for policing. Digital ethics address what data is transformed into information, how that information is used, and the results of its use.

How private companies handle these issues will affect their relationships with police. We have already seen the implications of digital ethics as they hit against the use of technology for public safety. The Apple Corporation's effort to keep from having to unlock smart devices for law enforcement is one example. Apple argued in federal court that, "forcing Apple

[16] This framework was developed by Accenture (2016).

to extract data could threaten the trust between Apple and its customers and substantially tarnish the Apple brand" (Raymond, 2015). Apple's digital ethics gave greater weight to ensuring anonymity when sharing data with law enforcement and the privacy of its customers than to the potential benefits to law enforcement.

Geofeedia, a social-media monitoring platform that reportedly was used by more than 500 U.S. law enforcement agencies also was compelled to address digital ethics. The American Civil Liberties Union (ACLU) published a report in October 2016 that the Chicago Police Department and others used Geofeedia to track protests and other large events. Shortly after the ACLU report was released, Facebook, Instagram, and Twitter cut off Geofeedia's access to specialized feeds (Cameron 2016). This resulted in police losing a useful tool and Geofeedia laying off half of its staff in November of 2016 and refocusing their business (Elahi 2016).

Digital ethics are not just a side issue that leads a company to thwart the use of its technology for public-safety interests. They are already shaping relationships between companies and police departments. The New York City Police Department (NYPD) is battling with the firm Palantir about obtaining the analysis used by the Palantir's software (Alden 2017). The NYPD decided to cancel the Palantir contract and go with another vendor. Palantir maintains that releasing the analysis or algorithm that produces the information to the NYPD would compromise its intellectual-property interests. The issue appears to be one of the NYPD understanding how the software analyzes the data provided as well as the portability of the data and analysis. These issues will be more common as companies bundle hardware, software, data storage, and analysis services.

As we move further into the 21st century, digital ethics will become a primary issue for police with regard to all the data being collected, how that data will be used, the analysis produced and used, and what technology will be used to advance policing. Not only must police agencies have a set of digital ethics but they also need to ensure that the companies they deal with have a compatible set of ethics. The poor use of data and analytics by a police department will erode the public trust and make it even more difficult to police effectively in the 21st Century. Police leaders must begin now to understand digital ethics and their implications for their organizations and profession. A Digital Ethic Framework similar to the one presented here needs to be explored, developed, and used by police leaders and organizations. Meanwhile, the guiding principles below can provide a first step.

Guiding Principles

Acknowledging that a somewhat different set of principles should apply to experimentation with new technologies, we propose the following set of guiding principles that police leaders ought to consider when deciding whether to adopt new policing technologies.

1. **The technology should be demonstrably effective and efficient in helping police carry out their objectives.** The police executive should be able to express how the technology increases the chances of achieving their objectives without jeopardizing other objectives. In furthering a major policing objective, technology should help pre-

vent injury and other harm to the public and police alike. For example, the police administrators must address how the technology will advance crime-control objectives without compromising the objectives of safeguarding civil liberties and building community trust. Optimally, technology should also reduce the cost of policing or at least flatten the growth of both operating and capital budgets.

2. **The use of the technology should be and seem fair to the public.** To the fullest extent practicable, the technology should safeguard people's reasonable expectations of privacy; the public should be consulted about the technology's use prior to its widespread adoption; and the known and uncertain costs of adopting the new technology should be carefully considered. Police administrators may want to establish a technology advisory group comprising knowledgeable stakeholders like technologists, government lawyers, public advocacy representatives, police practitioners, and ordinary community members. Such a group can offer police administrators a variety of perspectives and useful advice when making technology decisions. Surveying the public about police use of various technologies can likewise inform decision-making. Police administrators must also be alert to the ethical concerns relating to the financial implications of police adoption of new technology. One case in point is the public resistance to speed and red-light cameras: much of the resistance is due to a perception that the private companies selling this technology to police are profiting disproportionately from its use and that police or local-governments are employing this technology less for its public-safety benefits than for its public-finance benefits.

3. **The technology should reduce, overall, the degree of coercive force police must use to achieve their lawful objectives.** This principle addresses the social impact of technology on the relationship between the police and the community. For example, the rapid adoption of body-worn cameras came about because the evidence suggested that they increased public trust, decreased complaints, and reduced the use of force (President's Task Force on 21st Century Policing, 2015). At the other end of the continuum, we saw police departments across the country accepting and deploying surplus military equipment and technology from the U.S. Department of Defense. One consequence was the perceived militarization of policing which widened the trust gap between the police and community (Kraska, 2007).

4. **Use of the technology should be carefully regulated and monitored through training of personnel, and the setting and enforcing of policies governing its use.** Most technology is not self-activating: people must decide when and how to use it. More often than not, it is the misuse of the technology and not the technology itself that causes the greatest problems for police executives. Clear directives and operating procedures, as well as training, not only on the use of the technology, but also on the controls governing its use, and meaningful consequences for failing to follow directives must be undertaken prior to using any technology, especially technology that is likely to be controversial or otherwise ethically problematic. As stated in the President's Task Force Report on 21st Century Policing (2015): "The implementation of technology must be built on a defined policy framework with its purposes and goals clearly delineated".

5. **The technology should preserve, to the fullest extent practicable, the humanity of policing, bringing the police and community closer together, not further apart.** Policing is fundamentally about relationships between and among citizens, and between citizens and their government. We cannot allow technology to reduce our humanity. As policing becomes high tech, it must also become more high touch. As an illustration of technology with a humanizing effect, Santa Barbara, California, police developed "business" cards for its police officers which contained a QR code that allowed one to pull up on a computer a video recording made by the officer explaining his or her philosophy of and motivations for policing, as well as some personal information to allow people to know the officer as more than a badge number.

Police executives cannot just pass off these issues to their chief information officer or their professional standards unit. These important issues will drive the quality of relationships with stakeholders. Digital ethics and security must hold a primary place in the executive management of a police organization. Police leaders must demand strong ethical decisions, ensure there is strong security of systems, and build trusting relationships with technology vendors and, most importantly, with the communities they serve. By establishing a formal framework for making decisions on the possible adoption of new police technology, police administrators can speed up the adoption and implementation of useful new technology where the need has been clearly established and the implications thoroughly considered, and, conversely, slow down the process where they have not.

Next Steps

Nothing about the future is certain, but it is very likely that police will rely increasingly on technology in carrying out their duties. Police leaders need to learn from early efforts of implementing such technology as automated license plate readers, predictive policing, and digital data interceptors, and the unintended impact they have had on community trust. They must broaden their conversations with vendors about not only price and functionality but also about their digital ethics. Police executives should understand how vendors will profit from the sale and use of the technology, how they will use the data they are given, and what assumptions lie behind the analysis that produces the information police practitioners rely on to make deployment, tactical, and strategic decisions. Police departments have an important role to play in the future of police technology. They are the consumers, coordinators, and implementation partners for future police technology.

As Ramsey and Milgram (2017) so clearly stated, "Now more than ever, it is critical that we bring together the best in technology and science to create a new generation of tools that are accurate, transparent and community-informed." We believe that the next step in meeting this challenge is to develop a formal digital ethical framework that police leaders and their stakeholders can use when developing, evaluating and using new technology, collecting data and analyzing it to create actionable information, and understanding the consequences of using that technology or information for tactical and strategic purposes.

References

Accenture (2016). Digital Trust. *Accenture Technology Vision 2016. People First: The Primacy of People in a Digital Age.* Accenture Consulting, 57-65. Accessed July 10, 2017 at https://www.accenture.com/t20160314T114937__w__/us-en/_acnmedia/Accenture/Omobono/TechnologyVision/pdf/Technology-Trends-Technology-Vision-2016.PDF

Alden, W. (2017). There's a fight brewing between the NYPD and Silicon Valley's Palantir. *BuzzFeed*, June 28, 2017. Accesses July 14, 2017 at https://www.buzzfeed.com/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley?utm_term=.loYW0vGqVq#.sob3z9N5b5

Cameron, D. (2016). Dozens of police-spying tools remain after Facebook, Twitter crack down on Geofeedia. *The Daily Dot.* Accessed July 10, 2017 at https://www.dailydot.com/layer8/geofeedia-twitter-facebook-instagram-social-media-surveillance/

Carrega, C. (2017). Five finalists in running for Brooklyn's Smart Gun Design Competition. *Daily News*, August 1, 2017. Accessed August 10, 2017 http://www.nydailynews.com/new-york/finalists-running-brooklyn-smart-gun-design-contest-article-1.3375395

Coppola, M. (2015). Camera system provides panoramic view for police. *PoliceOne.com*, March 1, 2015. Accessed August 10, 2017 https://www.policeone.com/Patrol-Video/articles/8697739-Camera-system-provides-panoramic-view-for-police/

Elahi, A. (2016). Geofeedia cuts half of staff after losing access to Twitter, Facebook. *Chicago Tribune.* Accessed July 10, 2017 at http://www.chicagotribune.com/bluesky/originals/ct-geofeedia-cuts-jobs-surveillance-bsi-20161121-story.html

Kraska, P. (2007). Militarization and policing—Its Relevance to 21st Century Police. *Policing* 1(4): 501-13.

Lee, J. (2017). NYC to deploy facial recognition technology, license plate readers. *Biometric Update.Com*, January 16, 2017. Accessed on August 12, 2017 at http://www.biometricupdate.com/201701/nyc-to-deploy-facial-recognition-technology-license-plate-readers

Leonard, M. (2016). DHS nurtures wearable tech for responders. *GCN*, October 10, 2016. Accessed August 10, 2017 https://gcn.com/articles/2016/10/10/dhs-emerge-wearable-startups.aspx

Long, J. (2010). The Importance of Mobile Radiation Detection for Homeland Security. *EHS Today*, May 1, 2010. Accessed August 10, 2017 http://www.ehstoday.com/industrial_hygiene/instrumentation/importance-mobile-radiation-detection-homeland-security-0510

McDonald, A. (2013). Study Finds social networks are key to city violence. *YaleNews*, November 14, 2013. Accessed on August 10, 2017 at https://news.yale.edu/2013/11/14/study-finds-social-networks-are-key-city-violence

Miller, B. (2017). Predictive policing startup publishes code online, seeks to address bias. *Government Technology,* March 20.

Parker, K. and Andrews, C. (2017). The connected police officer: smart public safety. *E&T Engineering and Technology*, April 19, 2017. Accessed August 10, 2017 https://eandt.theiet.org/content/articles/2017/04/the-connected-police-officer-smart-public-safety/

Perry, W., McInnis, B., Price, C., Smith, S., and Hollywood, J. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations.* Santa Monica, CA: RAND Corporation.

Potter, A. (2002). Smart car for Maryland State Police. *The Frederick News-Post,* December 30, 2002. Accessed August 9, 2017 https://www.fredericknewspost.com/archives/smart-car-for-maryland-state-police/article_2ecff371-17bb-5c75-bf9e-c62d04ea22c9.html

President's Task Force on 21st Century Policing. 2015. *Final Report of the President's Task Force on 21st Century Policing*. Washington, DC: Office of Community Oriented Policing Services.

Ramsey, C. and Milgram, A. (2017). Technology can lead the way to better policing. The Hill, July 13, 2017. Accessed July 17, 2017 at http://thehill.com/blogs/pundits-blog/crime/341920-technology-can-lead-the-way-in-better-policing

Raymond, N. (October 2015). Apple Tells U.S. Judge 'Impossible' to unlock new iPhones. *Reuters*. Accessed July 10, 2017 at http://www.reuters.com/article/us-apple-court-encryption-idUSKCN0SE2NF20151021

Reaves, B. (July 2015). Local Police Departments, 2013: Equipment and Technology. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Sawh, M. (2017). The best smart clothing: from biometric shirts to contactless payment jackets. *Wearable Tech for Your Connected Self*, June 12, 2017. Accessed August 10 at https://www.wareable.com/smart-clothing/best-smart-clothing

Shaban, H. (2017). Meet the newest recruits of Dubai's police force: Robo-cars with facial-recognition tech. *The Washington Post.* Accessed July 3, 2017 at https://www.washingtonpost.com/news/innovations/wp/2017/06/30/meet-the-newest-recruits-of-dubais-police-force-robo-cars-with-facial-recognition-tech/?utm_term=.2dafe9bc10fe

Shingles, M., Briggs, B., and O'Dwyer, J. (2016). Social impact of exponential technologies. *Tech Trends 2016 – Innovating in the digital era.* Deloitte Consulting, 113-121. Accessed July 10, 2017 at https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology/gx-tech-trends-2016-innovating-digital-era.pdf

Wilson, J. (2015). Can Predictive Policing Be Ethical and Effective? *New York Times*, November 18, 2015. Accessed July 14, 2017 at https://www.nytimes.com/roomfordebate/2015/11/18/can-predictive-policing-be-ethical-and-effective

This paper was developed by the "Image of Policing/World of the Future" initiative of the BJA Executive Session on Police Leadership.

…….

The authors are Nola Joyce (Deputy Commissioner and Chief Administrative Officer of the Philadelphia Police Department [Ret]) , Phil Lyons (Dean, College of Criminal Justice, Sam Houston State University), Michael S. Scott (University of Wisconsin Law School) and Peter Sloly (Partner and National Lead - Security & Justice/Convergence Security - Deloitte Canada).

Cite as: Joyce, N., Lyons, P., Scott, M.S. and Sloly, P. (2017) "The Future is Here and We are Already Late: Leadership Challenges with Emerging Police Technology." A paper of the BJA Executive Session on Police Leadership. Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice; and St. Petersburg, FL: Center for Public Safety Innovation, St. Petersburg College.

12/18/2017

http://bjaleader.org

This project was supported by Grant No. 2009-D2-BX-K003 and 2015-CP-BX-K003 awarded by the Bureau of Justice Assistance to St. Petersburg College. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.