Proceedings of the American Society for Engineering Management 2023 International Annual Conference
G. Natarajan, H. Zhang, and E.H. Ng eds

RECOMMENDED TECHNOLOGY MANAGEMENT OF SMART POLICING ROBOCOPS FOR AI ETHICS AND CYBERSECURITY

Clovia Hamilton, Ph.D.*
Indiana University

Sira Maliphol, Ph.D.
SUNY Korea in affiliation with Stony Brook University

Lisa English-Dowdell, DIT
National Louis University and Joliet Community College

***hamilcl@iu.edu**

Abstract

The videotaped murders of George Floyd and Tyre Nichols in the United States have raised awareness worldwide of police misconduct. Police and citizens now distrust and fear each other because of the prevalence of instances of police brutality. Numerous incidents of police brutality indicate that policing requires a radical redesign that takes human rights into account. There is a greater need for smart policing technology management research as a result of new, increasingly ubiquitous technologies. Robotics and surveillance cameras are examples of smart policing. In several jurisdictions worldwide, currently robocops are on patrol and some can be armed, e.g., the recent approval for use in San Francisco. Given its perceived inherit technical objectivity, well managed smart technology has the potential to improve policing and ethical outcomes. With adequate technology management, smart policing can potentially alleviate law enforcement racial bias and abuse. This critically appraised topic study finds that there are few studies that address this issue. The defund the police movement calls for the reallocation of funds toward community services and community policing. In 2021, there was also a call for the US Congress to approve the George Floyd Justice in Policing Act. This research revealed that there are few studies that tackle this problem. With this critically appraised topic literature review, we make seven (7) recommendations on how resources can be effectively spent toward efficient law enforcement that leads to long overdue police reform using smart policing robocops.

Keywords

smart policing, robocops, AI ethics, AI bias, privacy, surveillance, cybersecurity, risk management, technology management, law enforcement

Introduction

Smart policing includes the use of drones, gunfire detection systems, body cameras, license plate readers, facial recognition, and robocops. Some detection systems alert police of gunfire and others use predictive policing artificially intelligent (AI) software that attempt to identify where crimes will most likely occur (Abril, 2022). We conducted a comprehensive critical appraisal of managing Robocops in smart policing technically and ethically published in 2022. That study was motivated by the police murder of George Floyd which resulted in protests worldwide against police brutality. The study concluded that while smart policing is pursued for the benefit of its efficiencies, the ethical issues and related demands from citizens go unmet. Thus, although smart policing has its benefits, police should not ignore the impact of technology on society and the need for Smart Justice (Maliphol & Hamilton, 2022). The George Floyd Justice in Policing Act H.R. 1280 was to boost transparency, improve data collection, hold law enforcement officers more accountable for misconduct, and establish best practices and training. The bill passed the U.S. House of Representatives on March 3, 2021, and was introduced to the Senate. However, no further action was taken ("George Floyd Justice in Policing Act," 2021) as negotiations broke down in September 2021 (Greve, 2023).

Smart policing is used by countries such as India (Swetha, Muneshwara, Praveen, & Danti, 2022), Africa (Nakasole, Chitsuro, & Hamunyela, 2022), the United Arab Emirates (UAE) (Ekaabi, Khalid, & Davidson, 2020), South Korea (Escalona, 2020; Moon, Choi, Lee, & Lee, 2017) the Philippines (Escalona, 2020), China (Murali, 2018; Ng, 2017; Williams, 2016), Poland (Murali, 2018), Israel (Glaser, 2016; Murali, 2018; Orbach, 2020), and Russia (Murali, 2018; Page, 2017). In Africa, Kenya, South Africa, and Uganda have adopted surveillance technology using CCTV, body-worn cameras, and facial recognition technologies (Jili, 2022; Stone, 2018). In the United States of America, it is being deployed in states including, but not limited to, Texas (Silverman, 2016), California (Wu, 2022), Colorado, New Jersey (Kann, 2017), New York (ABC News, 2023), Hawaii (Abril, 2022), and Massachusetts (Har & Lauer, 2022).

The implication of this research for engineering managers is that the more technological innovations are deployed to support law enforcement, the more there will be a need for engineers and sound engineering management. Sound engineering management of technology in smart policing needs to include AI ethics.

There are both pros and cons to deploying robotics in policing. For example, there are several privacy concern with deploying robocops. These robots collect a vast amount of data about citizens, their location, activities, and movement. Thus, the police could use this data to track people and later predict their movement and behavior. Another concern is over how this data will be shared and stored securely. Further, if the data is used for prediction, the robocops could be programmed with AI decision making algorithms that might be biased against under-represented populations including people of color or the disabled. We have seen evidence of these inherent biased crime prediction models with the practices of the Chicago Police Department (CPD) where they have used modeled data to create highly controversial lists of individuals considered likely to commit violent crimes. Using the "Strategic Subject List", officers target the people on the list, which could be viewed as harassment based on a biased assumption (Hvistendahl, 2016). Another issue with robots generally is that some fear they can be used to replace human police officers.

The benefit to police is that robocops can be used to perform dangerous tasks like entering dangerous surroundings, approaching armed suspects, to patrol high crime areas, or to provide crowd control during protests and riots. How best to manage this technology is a complex question and this study focuses on identifying the risks, benefits, and best practices in managing this technology.

Method

The Critically Appraised Topic (CAT) was used as the research methodology. It is a kind of literature review that compiles research data based on a specific research question. The objective is to evaluate the research and state how applicable the findings are. Clinical practitioners and scholarly researchers in the healthcare industry are the main users of CATs (Sadigh, Parker, Kelly, & Cronin, 2012; Bigby, 2007; Callander et al., 2017; Sackett & Straus, 1998). A CAT is written in five (5) steps: (1) asking a specific, definable question, (2) looking for the best available evidence, (3) assessing the evidence critically for validity and applicability, (4) implementing the findings in professional practice, and (5) assessing performance after implementation. Further, the study's research question must be crucial to the subject's health and welfare. The research question in healthcare is primarily concerned with Patients, Intervention, Comparator, and Outcome (PICO) (Sadigh, Parker, Kelly, & Cronin, 2012).

Here, we are focusing on public safety as related to the AI ethics and cybersecurity concerns of using smart policing robotics. In technology management, comparator interventions include managing cybersecurity, legal, operational, financial, societal and reputational risks. Consequently, the research question of interest for this study is:

> *In relation to the rising use of robotics in policing, how does the current technology management of these devices compare with other interventions used in the risk management of technology generally?*

Results

A number of Robocops are being deployed in police departments worldwide. See Exhibit 1. However, studies on the effectiveness of smart policing service quality have not fully addressed this issue. Measuring service quality allows managers and supervisors a way to fully and methodically comprehend important aspects or factors that can prevent mistakes in smart policing activities. (Ekaabi, Khalizani, Davidson, Kamarudin, & Preece, 2020). In a study of the UAE's smart policing service quality, researchers found that the relevant constructs noted in previous research include the dimensions of responsibility, accountability, interaction, openness, and serviceability. These dimensions influence user satisfaction. Further, integrity and transparency are predominating factors (Ekaabi, Khalizani, Davidson, & Ross, 2020). In addition, the UAE is engaged in smart policing and are using Total Quality Management (TQM) best practices. Researchers concluded that managers and other decision makers in the UAE police departments and elsewhere need to make use of benchmarking, information collection and data analysis, and continuous process improvements (Fakhari & Utara, 2021).

However, it is important to note that Kalyal (2019) interviewed police leaders including 38 officers in 16 Canadian organizations and found that police departments have been slow to adopt evidence-based practices (Kalyal, 2019). The best practices that Kalyal studied included community policy, intelligence led policing, hot spot policing, the use of CompStat, and problem-oriented policing. The reasons for the lack of adoption of these best practices included lack of communication, such as the sharing of results of engaging in these best practices; cultural resistance such as the notion that the police know best; and risk aversion along the line of fear of failure when trying a new practice. Participants supported cultural shifts toward the adoption of best practices through education and communication and felt that a lack of resources is a problem. The police also express a belief that non-police who research policing do not understand policing. So, the police lack confidence in research findings (Kalyal, 2019).

Exhibit 1. Examples of Smart Policing Robocops.

Robots equipped with cameras	Manufacturer	Location	Source
Anbot and E-Patrol Robot Sheriff (armed with facial recognition software and stun-guns)	Shenzhen Public Security Bureau, National University of Defense Technology, and a domestic technology company	China (Shenzhen & Zhengzhou)	(Murali, 2018; Ng, 2017; Williams, 2016)
Robocop (5 ft 5 in, 100 kg) fitted with emotion detectors	PAL Robotics	Dubai	(Arabian Business, 2017; Murali, 2018; Page, 2017)
Smart Robocop	H-Bots Robotics	India (Hyderabad, Telangana)	(Murali, 2018)
Dogo (10kg, 11 inches tall; can be armed with a handgun)	General Robotics	Israel India France	(Frantzman, 2019; Glaser, 2016; Murali, 2018)
Spot	Boston Dynamics in partnership with Percepto for imaging and thermal vision drone capabilities	Israel	(Orbach, 2020)
Tamuke, Mwaluke, Kisanga (giant solar powered for traffic control)	Congolese Association of Women Engineers; Women's Technology	Republic of Congo	(France-Presse, 2015; Murali, 2018)
Final Experimental Demonstration Object Research (FEDOR)	Russian Foundation for Advanced Research Projects	Russia	(Murali, 2018; Page, 2017)
K5 robotic security guard	KnightScope	USA - CA	(Cooper, 2014)
Hp Robocop	KnightScope	USA - CA	(Flaherty, 2019)
Spot (70 pound dog)	Boston Dyanamics	USA - HI	(Abril, 2022; O'Brien & Kelleher, 2021; Stanley, 2021)
Throwbot (1 pound dumb-bell can be thrown to collect audio video data)	Recon Robotics	USA - NJ Poland	(Kann, 2017; Murali, 2018)
Digidog	Boston Dynamics	USA - NY	(ABC News, 2023; Max, 2023; Stanley, 2021)
Bomb Robots Mark 6/ Andros V-A1/HD-2	Remotec (subsidiary of Northrop Grumman)	USA - TX	(Masnick, 2016; Silverman, 2016)

Benefits

The benefits related to the protection of individuals through policing include increased efficiency in policing, the protection of citizens, and protection policy development. Robots can be deployed in dangerous situations and can help law enforcement see what is going on in real time (Kann, 2017). Here are some examples:

- In 2016, a sniper who opened fire on police was found and killed in Dallas (Har & Lauer, 2022; Wu, 2022). The police attached a pound of C4 explosive to the remotely controlled robot. This was the first-time police combined lethal force with the use of robotics (Joh, 2016a, 2016b). The robot was a size of a lawn mower and its use for lethal force has been debated (Silverman, 2016). For example, a representative of Boston Dynamics which manufacturers robocops stated that its business prohibits weaponization in its acceptable usage policies for their robots (O'Brien & Kelleher, 2021).
- The use of a robotic dog can help police officers track tagged vehicles remotely and avoid high risk vehicular pursuits (ABC News, 2023).
- In Mountain View California, homeowners called the police about a man armed with a knife. The police used drones to capture live stream video to locate the suspect. The video also helped the police de-escalate the situation without the use of force. The St. Petersburg, Florida police department also believes that robotic police dogs can be used to de-escalate situations and avoid the use of force (Abril, 2022).
- Another example is where in a manhunt, a robot was deployed to raise up a tarp in order to protect the police from a bombing suspect. This occurred in the Boston Marathon manhunt in 2013 (Har & Lauer, 2022).

Digital innovations may result in architectures that couple layers of devices, networks, and services (Yoo, Henfridsson, & Lyytinen, 2010). Police departments are also deploying e-policing which incorporates the internet of things (IoT). Some departments are providing portals for information sharing – i.e. citizens can share their camera photo shots and videos with police. However, in a study of the Laoag police station in the Philippines, a lack of trained personnel in the use of the technology is problematic (Escalona, 2020). San Francisco is thinking about expanding government access to its residents' private cameras, which is a practice it restricted in 2019 (Abril, 2022). In another example, for access to information obtained from *Ring* security devices, many police agencies collaborated with the *Ring* video doorbell manufacturer (Marr, 2022). Further, researchers in Namibia studied smart policing to combat cybersecurity crimes. They found that deploying AI is essential in combatting cybercrimes and the creation of mobile phone apps and portals whereby private citizens can assist police with sharing their information is important (Nakasole, Chitsuro, & Hamunyela, 2022).

Researchers have also studied the establishment of an e-police station in India. Data can be fed by citizens using mobile and/or web applications. The researchers concluded that this system would help police use their workforce more efficiently and the collection of statistics will help with upgrading policing locations (Swetha, Muneshwara, Praveen, & Danti, 2022) Further, an architecture for combining AI and the IoT has been proposed for policing (Huang, Chou, & Wu, 2021).

Robots have been used in the City of San Francisco's Police Departments (SFPD) since 2010. However, they have never used lethal force (Rogers, 2022). San Francisco's Board of Supervisors authorized the moderate use of remote-controlled smart policing devices including allowing police to arm the devices with explosives in extreme situations. This controversial city policy was put before the board in response to the passage of California Assembly Bill 481 that "requires police to inventory military-grade equipment such as flashbang grenades, assault rifles and armored vehicles, and seek approval for their use." More than 500 police departments are requesting authorization for their military-grade weapons policies for use. This addresses a desire to give citizens more transparency from law enforcement (Har & Lauer, 2022; Heater, 2022).

As lawmakers in San Francisco wrangled with lethal force language, by November 2022, their proposal stated that "robots will only be used as a deadly force option when risk of loss of life to members of the public or officers are imminent and outweigh any other force option available to the SFPD (Shapiro & Scott, 2022). In contrast, Oakland abandoned their idea to weaponize their robots and they armed them with only pepper spray as an alternative (Har & Lauer, 2022).

Risks

Although some are trained and equipped to handle large protests, many police departments are not. This was discovered as protests systemic racism and police brutality ensued after the murder of George Floyd (Davis Jr., 2020). Further, in 2021, Capitol Police were not prepared for rioters during the infamous January 6th insurrection in America (Viswanatha & Gurman, 2021). Perhaps the use of smart policing surveillance tools can help police catch criminals engaged in looting, violence upon civilians, attacks on police, and use of excessive force by the police. The privacy watchdog organization Electronic Frontier Foundation (EFF) is concerned that robocops are equipped with surveillance cameras and can identify smartphones using IP addresses (Guariglia, 2021).

Managing the expectation that robocops can provide public safety is a challenge. Researchers studied whether robots could actually defend people. They found that there are substantial obstacles to overcome before robots can step into a situation and provide defense. Considering and examining the common assumption that robots should never harm or risk harming others, the researchers also found that their research participants accepted the idea of robot self-defense (Cooney, 2023; Duarte, 2022).

In 2020, New York City considered contracting with Boston Dynamics to make use of the Digidog robocop which is equipped with cameras and sensors. They tested a robot. However, civil rights advocates wanted to reduce police funding and protested the investment in robotics. The pushback was a reputational risk. So, NYC tabled the idea. However, the robotic police dog was reintroduced this year to patrol Time Square and the Time Square subway. Critics view it as a means for aggressive policing (ABC News, 2023; Max, 2023).

Robocop reliability is also a real issue. For example, a woman pushed an emergency alert button on a robocop in Los Angeles California and it said, “step out of the way”. It later glided forward and said, “please keep the park clean”. This woman was trying to get emergency help for victims of a fight that broke out in the parking lot of a park (Flaherty, 2019). The public has an expectation that these AI tools can provide public safety. Duncanville, Texas’ robocop stopped working and it took two months to repair it locally (Wertheimer, 2015). Thus, these devices may not be ideal for towns with limited resources. Further, responses to the Murali (2018) news article about robocops mention concern about the ease at which these robots can perhaps be easily kicked over (Murali, 2018). In fact, police caught a person knocking one over with a bike while performing a wheelie and running into the robocop (Flaherty, 2019). Meeting the general public’s expectation that these devices can provide reliable public safety is a serious societal, legal, and ethical concern.

AI biasness is a concern. For example, the use of predictive policing software was outlawed in Santa Cruz (Abril, 2022). The use of algorithms for policing is not without issues. Policing practices that are biased can add dirty data that support bias. The policing prediction approach uses machine learning where it is possible to predict crime that disproportionately targets ethnic and religious minorities as an increased risk resulting in them being singled out by police action (Dearden, 2017). According to the now debunked Broken Window Theory, CompStat was thought to be a way to prevent serious crimes by preventing minor infractions but led to discriminatory policing at the precinct level (Thomas & Wolff, 2020). Smart technology, however, offers another tool in the arsenal of improving policing outcomes by enabling standardization, oversight transparency and algorithmically defined objectivity.

Privacy is also a concern. The American Civil Liberties Union (ACLU) and Farhang Heydari, Executive Director of NYU’s School of Law’s Policing Project, are concerned about expanding access to citizens’ personal cameras as well as external third-party databases surveillance systems. The ACLU has also protested the use of license plate readers. A study showed that 35% of “hits” on license plates were misread, which could potentially lead to innocent people being pursued and arrested (Potts, 2018). A license plate reader was blamed for a Colorado family being detained and handcuffed at gunpoint due to mistaking their SUV’s license plate for that of a motorcycle’s plate from a different state (Porter, 2020). Lawmakers in Virginia, Alameda, California and Boston, Massachusetts limit the use of facial recognition (Abril, 2022). Further, in 2016, researchers surveyed 500 citizens and 161 police officers in South Korea. The police expressed that smart policing enhanced policing efficiency. However, the citizens expressed that smart policing has resulted in increased taxation and invasion of privacy. Yet, both the police and general public felt that smart policing is beneficial in cybersecurity investigations and prevention (Moon, Choi, Lee, & Lee, 2017).

Further, another problem area is the risk of hacking and data breaches. The Robotic Reconfigurable Button Basher (R2B2) was created by hackers that desire to attempt repeated passwords on locked, lost, or stolen mobile phones (Murali, 2018). If third parties can hack mobile phones, “cars or toy drones, they can certainly hack police robots” (Joh, 2016a). By connecting robocops to the internet, they also become vulnerable to cyberattacks, data leaks, and takeover by hackers around the world (Black & Lynch, 2020; Cerrudo & Apa, 2017).

The militarization of policing is a concern. According to a study by Bard College’s Center for the Study of the Drone, between 2003 and May 2016, 987 robots transferred from the US military to police forces around the country; and in the first six months of 2016, 201 robots. California received most of these transfers (Kann, 2017). In relation to the use of lethal force, in 2021, the ACLU expressed uneasiness over the weaponization of these devices (Stanley, 2021). One of the three Asimov laws of robotics is that a robot may not harm a human or, by doing nothing, permit a human to suffer injury. Salge (2017) recommends that with regard to reining in a robots’ behavior, the ethical approach is to code robots to make the best choice taking into account context and an evaluation of scenarios. Salge provides the example that instead of a robot being coded to not push a human, the robot should “still be able to push them out of the way of a falling object. The human might still be harmed but less so than if the robot didn’t push them” (Salge, 2017). Militarization is of particular concern for armed robocops which are feared by the general public. For example, after Russia’s Deputy Prime Minister Dmitry Rogozin posted a video showing a robot armed with two guns, he apologized and explained that the intent was not to create a terminator but rather to train the robot to make decisions in dire situations (Murali, 2018).

In 2015, police militarization with the use of drones was a hot topic. ACLU communications director Kelly Jones Sharp shared that drones need to be properly used, monitored, and given public scrutiny in order to address privacy concerns (Slabaugh, 2015). In 2018, in response to school shootings, the City of Bloomington, Indiana attempted to purchase a Lenco BearCat counter assault vehicle. This was very controversial and citing the social psychology phenomenon called the 'Weapons Effect', critics felt that the militarization of policing would increase community violence. The idea is that military equipment is a stimulant that is associated with violence and the role of the police might shift. The police might respond to the public like a soldier would and treat the public like an enemy force (The Herald Times, 2018).

Another issue that was raised in this critical appraisal of the literature is the potential for robotics to dehumanize the homeless. For example, the ACLU has expressed concern about Hawaii using COVID relief funds to buy the Spot robot. They used Spot in a tent city occupied by the homeless to scan their eyes for whether they had fevers. Hawaii defended this practice by stating that it was intended to protect the police, homeless shelter staff and general public. The Vice President of Business Development at Boston Dynamics stated that their robotics acceptable use guidelines prohibit practices that would go against civil rights or privacy legislation (O'Brien & Kelleher, 2021). Whether Hawaii violated civil rights or privacy legislation needs to be reviewed.

As illustrated in the anecdotal robocop stories presented herein, the technology management of robocops is imperative. And when managing technology, according to Rutgers University Edward J. Bloustein School of Planning and Public Policy Local Government Research Center Senior Fellow and Assistant Director Marc Pfeiffer, there are six (6) types of technology risks: cybersecurity, legal, operational, financial, societal, and reputational (Pfeiffer, 2015).

Recommendations

As aforementioned, the reasonable *George Floyd Justice in Policing Act* goals were to improve data collection, transparency, and accountability for improper behavior by law enforcement in order to develop best practices and training. This would be beneficial worldwide and can be achieved with the use of AI tools such as smart policing because technology has the potential to reduce civilian-police interactions and the escalation of minor crimes into fatalities. However, this will require proper technology management.

Herein, we are coining the phrase and acronym *Total Quality Tech Management* (TQTM). Based on the results of this CAT literature review, the following seven (7) recommendations for TQTM are made:

1. Police departments need comprehensive training in the use of these devices before they implement them.
2. There is a need for transparency in what these robots are capable of, their shortcomings in performing public safety. This can be achieved with implementing a public education strategic plan.
3. There is a need for transparent information sharing using an e-policing platform and community policing principles. It is recommended that smart policing include public private partnerships whereby the police departments include means to gather camera footage from private citizens from their mobile phones, private homes or businesses.
4. There is a need to analyze the data collected through citizen portals. This is especially imperative when crime predictive tools are utilized. Data collected should be utilized for investigative purposes.
5. There has to be adequate resources for robot coding, maintenance, monitoring, and remote control. In all four of these areas, a managerial manual of guidance of clear procedures would be helpful in providing clarity on aligning these work tasks to legal and police departmental policies.
6. Technology managers need to be mindful of design quality control given that these robots should be formidable in weight and have other safeguarding features so that they cannot easily be kicked over, stolen, hacked, or otherwise vandalized.
7. Each police department that deploy robocops needs to hire an AI ethics czar whose job is to ensure awareness internally and externally on the benefits and potential dangers of using these devices, and to ensure that policies and procedural guides address AI ethical issues and related risk management.

Conclusion

As technological change proceeds at an increasingly fast pace, smart policing capabilities are expanding around the world through the use of IoT-enabled sensors, drones, and recorded surveillance. Robocops are being used for surveillance and communication with the general public. The new capabilities enhance the safety, efficiency, and institutions of policing. Police officers benefit by reduced exposure to dangerous situations and by focusing on activities that cannot be replicated through digital technologies. The citizenry also benefits from improved policing and from improved capabilities to enforce proper implementation of policing standards and institutions.

To fully appreciated these benefits, however, it is necessary to address the limitations that have also presented themselves. While there are typical management issues of operations and financial resources, emerging technologies for smart policing create additional risks. New forms of digital crime require new cybersecurity. Also, legal and ethical complications may arise through increased, automated weaponization. Further, societal challenges must be addressed when applying these new technologies to make sure that both the benefits and risks are evenly borne. Reputational risks may hinder the adoption and support of new technologies. We may never be able to fully encode human judgment, compassion, or discretion into autonomous robots. Despite the costs associated with the attempts to do so, we may still try to design technologies and related policies to ameliorate these negative impacts.

As with any new technology, several aspects of smart policing technology need to be enhanced to ensure that it is trustworthy for the public. The reliability of technology still needs to be improved through continued technological advancements. Moreover, many of the limitations stem from cultural institutions that have entrenched biases that can become embedded into the technology or algorithms that make decisions regarding policing. In addition, there is another form of bias in the form of reluctance to accept new technology.

Smart policing is likely to lead to policing harm, especially as new technologies, policies, and practices are developed. Flawed algorithms in facial recognition have already led to mistaken and wrongful arrests (Johnson, 2022; AP 2023). AI algorithms in predictive policing have been found to embed biases and increase policing harms, especially against minority and vulnerable populations (Benbouzid, 2019; Hanink, 2013). Additionally, the question of liability is still left unanswered and requires further research to address the question: who will be held accountable in the event that smart policing through AI-enabled robotics or drones leads to extensive policing harm or fatalities? Given how controversial the San Francisco's policy for use of armed robotics was, it seems that local governments realize that they can be held liable for policing harms. Whether manufacturers will also be held liable will depend on the government regulations that get enacted and on existing liability codes and statutes at the state and local government levels and court case precedence.

For these reasons, we propose seven (7) recommendations to develop *Total Quality Tech Management* (TQTM) to address these challenges and to ensure that smart policing technologies are trustworthy to use in the public and to ensure the safe and effective adoption of these new technologies to the benefit of everyone in society. Furthermore, these recommendations should evolve as the technologies and the institutions that govern them evolve, i.e., AI governance. With the introduction of ever more advanced technologies and the capabilities they represent, even greater care must be given to prevent unintended consequences that lead to privacy breaches, material and physical harm, and the erosion of societal bonds. TQTM is a first step in designing the framework to ensure these principles are in place.

Acknowledgment

This work was supported in part by the South Korea government MSIT supported National Research Foundation of Korea (NRF) grant No. 2022R1G1A1006464.

References

ABC News. (2023, April 11). Mayor Adams and NYPD roll out high-tech crime fighting tools in Time Square. *ABC7 New York*.

Abril, D. (2022, March 9). Drones, robots, license plate readers: Police grapple with community concerns as they turn to tech for their jobs. *Washington Post*.

Arabian Business. (2017). World's first 'Robocop' joins Dubai police force. *Arabian Business*.

Associated Press (AP). (2023, Jan 5). Facial recognition tool led to mistaken arrest, lawyer says. NBC News. https://www.nbcnews.com/tech/security/facial-recognition-tool-led-mistaken-arrest-lawyer-says-rcna64270

Benbouzid, B. (2019). To predict and to manage. Predictive policing in the United States. Big Data & Society, 6(1), 2053951719861703.

Bigby, M. (2007). Evidence-based dermatology section welcomes a new feature: critically appraised topic. Archives of Dermatology, 143(9), 1185-1186.

Black, J., Lynch, A. (2020). Cyberthreats to NATO from a Multi-domain Perspective. In Ertan, A., Floyd, K., Pernik, P., & Stevens, T. (Eds.). *Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO Cooperative Cyber Defence Centre of Excellence*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications.

Callander, J., Anstey, A. V., Ingram, J. R., Limpens, J., Flohr, C., & Spuls, P. I. (2017). How to write a Critically Appraised Topic: evidence to underpin routine clinical practice. *British Journal of Dermatology*, 177(4), 1007-1013.

Cerrudo, C., Apa, L. (2017). Hacking Robots before Skynet. Cybersecurity Insight. IOActive.

Cooney, M., Shiomi, M., Duarte, E. K., Vinel, A. (2023). A broad view on robot self-defense: rapid scoping review and cultural comparison. *Robotics, 12*(43).

Cooper, Q. (2014). Myth of the 'Real life Robocop'. *BBC Future*.

Davis Jr., E. (2020, June 8). Experts fear smaller cities are ill-equipped to handle George Floyd protests. *US News*.

Dearden, L. (2017, October 7). How big data can now be used to predict where crime will happen. *Independent*. Retrieved from http://www.independent.co.uk/news/uk/home-news/police-big-data-technology-predict-crime-hotspot-mapping-rusi-report-research-minority-report-a7963706.html

Duarte, E. K., Shiomi, M., Vinel, A., Cooney, M. (2022). *Robot self-defense: Robots can use force on human attackers to defend victims*. Paper presented at the 2022 31st IEEE International Conference on Robot and Human Interactive Communication (RO-MAN) August 29- September 2, 2022, Naples, Italy.

Ekaabi, M. A., Khalid, K., Davidson, R. (2020). The service quality and satisfaction of smart policing in the UAE. *Cogent Business & Management, 7*(1).

Ekaabi, M. A., Khalid, K, Davidson, R., Kamarudin, A. H., Preece, C. (2020). Smart policing service quality: conceptualisation, development and validation. *Policing: An International Journal*, 707-721.

Escalona, J.-L. M. S. (2020). E-policing in the PNP Laoag City Police Station: Case Study. *International Journal of Innovative Science and Research Technology, 5*(12), 497-506.

Fakhari, N. Y. M., Utara, U. (2021). Influence of total quality management factors on the organizational performance and moderation of organizational support in Dubai police. *International Journal of Entrepreneurship, 25*.

Flaherty, K. (2019, October 4). A Robocop, a park and a fight: How expectations about robots are clashing with reality. *NBC News*.

France-Presse, A. (2015, Mar 4). Robocops being used as traffic police in Democratic Republic of Congo. *The Guardian*.

Frantzman, S. J. (2019, May 31). Watch this Israeli robot face off against a marksman in a live-fire demo. *DefenseNews*.

George Floyd Justice in Policing Act, H.R. 1280, House (2021).

Glaser, A. (2016, July 24). 11 Police Robots patrolling around the world. *Wired*.

Greve, J. A. (2023, February 6). Tyre Nichols What is the George Floyd Justice in Policing Act and is it likely to pass? *The Guardian*.

Guariglia, M. (2021). *Police robots are not a selfie opportunity, They're a privacy disaster waiting to happen*.

Hanink, P. (2013). Don't trust the police: Stop question frisk, COMPSTAT, and the high cost of statistical over-reliance in the NYPD. *Journal of the Institute of Justice & International Studies*, 13, 99-113.

Har, J., Lauer, C. (2022, December 5). US police rarely deploy deadly robots to confront suspects. *AP News*.

Heater, B. (2022, November 30). San Francisco police can now use robots to kill. *Tech Crunch*.

Huang, C.-H., Chou, T.-C., Wu, S.-H. (2021). Towards convergence of AI and IoT for Smart Policing: A case of a model edge computing-based context-aware system. *Journal of Global Information Management, 29*(6), 1-21.

Hvistendahl, M. (2016, September 28). Can 'predictive policing' prevent crime before it happens? *Science Magazine*. Retrieved from http://www.sciencemag.org/news/2016/09/can-predictive-policing-prevent-crime-it-happens

Jili, B. (2022). Africa: Regulate surveillance technologies and personal data. *Nature*, 607(7919), 445-448.

Joh, E. E. (2016a, November 16). Police robots need to be regulated to avoid potential risks. *NY Times*.

Joh, E. E. (2016b). Policing Police Robots. *UCLA Law Review*.

Johnson, K. (2022, Mar 7). How Wrongful Arrests Based on AI Derailed 3 Men's Lives. *Wired*. https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/

Kalyal, H. (2019). 'One Person's Evidence Is Another Person's Nonsense': Why police organizations resist evidence-based practices. *Policing, 14*(4), 1151-1165.

Kann, D. (2017, April 18). Why your local police force loves robots. *CNN*.

Maliphol, S., Hamilton, C. (2022). *Smart Policing: Ethical Issues & Technology Management of Robocops*. Paper presented at the 2022 Proceedings of PICMET '22: Technology Management and Leadership in Digital Transformation - Looking Ahead to Post-COVID Era, Portland, Oregon.

Marr, B. (2022, March 8). The 5 biggest tech trends in policing and law enforcement. *Forbes*.

Masnick, M. (2016, July 8). Now that we've entered the age of Robocop, how about ones that detain, rather than kill? *techdirt*.

Max, S. (2023, April 17). Robocops join NYPD, much to the dismay of some residents. *WBUR*.

Moon, H., Choi, H., Lee, J., Lee, K. S. (2017). Attitudes in Korea toward Introducing Smart Policing Technologies: Differences between the General Public and Police Officers. *Sustainability, 9*(1921), 1-17.

Murali, J. (2018, November 4). Rise of the police robots Hyderabad has launched the country's first smart policing robot called the smart Robocop. *Deccan Chronicle*.

Nakasole, N., Chitsuro, M., Hamunyela, S. I. (2022). *Analysing ICT initiatives towards Smart Policing to assist African law enforcement in combating cybercrimes.* Paper presented at the 2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT).

Ng, Y. S. (2017, February 20). China's latest robot police officer can recognise faces. *Mashable*.

O'Brien, M., Kelleher, J. S. (2021, July 30). Spot on patrol: Robotic police 'dogs' have privacy watchdogs worried. *USA Today*.

Orbach, M. (2020, November 24). Boston Dynamics' robo-dog gets Israeli Percepto's drone capabilities. *CTECH*.

Page, T. (2017). The inevitable rise of the robocops. *CNN*.

Pfeiffer, M. H. (2015). *Managing Technology Risks through technological proficiency: Guidance for local governance*.

Porter, J. (2020, August 5). Aurora police detain Black family after mistaking their vehicle as stolen. *Denver 7 Colorado News (KMGH)*. Retrieved from https://www.denver7.com/news/local-news/aurora-police-detain-black-family-after-mistaking-their-vehicle-as-stolen

Potts, J. (2018). Reseach in brief: assessing the effectiveness of automatic license plate readers. *Police Chief*.

Rogers, Z. (2022, November 30). San Francisco police can use robots to kill in emergency situations, city says. *ABC News WCIV*.

Sackett, D. L., & Straus, S. E. (1998). Finding and applying evidence during clinical rounds: the evidence cart. *Journal of the American Medical Association*, 280(15), 1336-1338.

Sadigh, G., Parker, R., Kelly, A. M., & Cronin, P. (2012). How to Write a Critically Appraised Topic (CAT). *Academic Radiology, 19*, 872-888.

Salge, C. (2017, July 10). Asimov's Laws Won't Stop Robots from Harming Humans, So We've developed a better solution. *The Conversation*.

Shapiro, A., Scott, B. (2022, November 28). San Francisco considers allowing law enforcement robots to use lethal force. *NPR*.

Silverman, L. (2016, July 11). Robot used by Dallas police to kill gunman sparks debate. *NPR*.

Slabaugh, S. (2015, January 7). Police militarization concerns ACLU. *Star Press*.

Stanley, J. (2021, March 2). Robot police dogs are here. Should we be worried? *ACLU News & Commentary*.

Stone, K. E. (2018). Smart policing and the use of body camera technology: unpacking South Africa’s tenuous commitment to transparency. *Policing: A Journal of Policy and Practice*, 12(1), 109-115.

Swetha, M. S., Muneshwara, M. S., Praveen, N.M., Danti, R. (2022). *Developing Virtual Police Station to Receive FIR through Digital Signature*. Paper presented at the Proceedings of the Sixth International Conference on Intelligent Computing and Control Systems (ICICCS 2022).

The Herald Times. (2018, March 28). Militarization of police will lead to more violence. *The Herald-Times*.

Thomas, A. L., Wolff, K.T. (2020). Crime distortion within the NYPD: a potential method for estimating crime misclassification within CompStat statistics. *Police Practice and Research*.

Viswanatha, A., Gurman, S. (2021, January 7). Capitol police weren't prepared for rioters, authorities say. *Wall Street Journal*.

Wertheimer, L. (2015, June 30). Police in Texas needed help to get robot working. *NPR*

Williams, S. (2016, September 23). Meet the cop of the future: Robotic policeman 'Anbot' begins patrolling in China and will give trouble-makers a ruthless TASER. *Daily Mail*.

Wu, D. (2022, November 30). Can police use robots to kill? San Francisco voted yes. *Washington Post*.

Yoo, Y., Henfridsson, O., Lyytinen, K. (2010). The new organization logic of digital innovation: An agenda for information systems research. *Information Systems Research, 21*(4), 724-735.

About the Authors

Clovia Hamilton taught industrial operations management for four years at SUNY Korea and Winthrop University; and law and ethics for many years. Clovia earned a PhD in Industrial & Systems Engineering from the University of TN Knoxville in August 2016. Prior to that, she earned an MBA from Wesleyan College, JD from Atlanta’s John Marshall Law School, and LLM in Intellectual Property from the University of IL at Urbana Champaign. She is a subject matter expert in the impact of technology on society and AI ethics; and serves as a Research Fellow in Indiana University's Center for Applied Cybersecurity Research.

Sira Maliphol is a tenure-track Assistant Professor in Technology & Society at SUNY Korea/SBU and a Fellow at the Trustworthy AI Lab at Seoul National University. His research interests include technological catch-up and development, STI policy, and innovation systems. He has worked on international organizational development projects consulting with countries in Asia including Indonesia, Laos, Nepal, Thailand, and Vietnam. He has worked in the non-profit, government, and private sectors. While at non-profit and government organizations, he worked in science and technology arenas.

Lisa English-Dowdell is a retired professional with over two decades of experience in law enforcement and technology. With a background as the Director of Information Technology for the Cook County Sheriff's Office, she has a strong track record of implementing innovative technology solutions in the law enforcement sector. Notably, Lisa served as Chairperson for the Cook County Integrated Justice Information System Technical Sub-Committee, responsible for developing standards and guidelines for justice-related data exchange. She holds a Doctor of Information Technology from Capella University and currently serves as an Adjunct Professor at Joliet Community College and National Louis University.