RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE FOR CRIME PREVENTION IN SOUTH AFRICA
SUMMARY

‘Smart’ technologies are being used in public policing and private security operations across the country. The opaque nature of current data collection and processing activities, and a lack of policy direction on the use of emerging technologies in crime prevention, means that government officials and the wider public have limited guidance on what are acceptable practices in this space. This Topical Guide provides examples of the use of surveillance technologies for crime prevention in South Africa, and comments on the social and legal implications of data-driven technologies, such as artificial intelligence (AI), for these applications.

The Guide also reviews policy material that advocates for the use of technology in law enforcement and highlights critical issues to consider in the operationalisation of these technologies.

These issues include potential infringements on the right to privacy and freedom of movement, the possible risks of state-sanctioned discrimination, and the criminalisation of communities. Achieving a more ethical, legally sound and socially responsible use of data and AI for crime prevention will require: stronger alignment between criminal procedure and protection of information legislation, a better understanding of privacy in public spaces, and the adoption of measures and standard procedures to mitigate against biased and unlawful use of these technologies.
ABOUT THE AUTHOR

Kelly Stone is a Policy Development and Research Advisor specialising in the intersection between safety, gender and development, with a particular focus on policing and human rights. Email: kellyestone@outlook.com.

ABOUT THIS TOPICAL GUIDE

This series of PAN Topical Guides seeks to provide key research insights and policy considerations for policy-makers, and other interested stakeholders, on how these technologies need to be developed, used and safeguarded in a manner that aligns with the transformation objectives of South Africa. In addition, each Guide outlines ways in which South Africa may respond to the growth of data-driven systems and technologies, including AI, to foster and inculcate a more inclusive and equitable society, rather than deepen divides.

The series is curated by the Policy Action Network (PAN), a project by the Human Sciences Research Council (HSRC) supported by the Department of Science and Innovation (DSI); and the University of Pretoria (UP) South African Sustainable Development Goals (SDG) Hub and Data Science for Social Impact Research Group, under the ABSA UP Chair of Data Science.

Publication date: March 2020
Innovations in communications and information technology have been recognised as a positive development in South Africa’s efforts to reduce crime and violence, with ‘Smart’ closed-circuit television (CCTV) cameras, body worn cameras (BWCs), automated number plate recognition (ANPR), and even aerial drones being deployed across the country.¹ Unlike the variability of witness statements or incident reports, which may be vulnerable to language or literacy barriers, or subject to ulterior motives and personal agendas, information generated by surveillance technology and artificial intelligence (AI) is broadly treated as a reliable source of evidence that can assist in the detection, investigation and prevention of crime.² In light of law enforcement’s significant resource constraints, technically-driven solutions offer state agencies like the South African Police Service (SAPS) and Metropolitan Police Service (MPS) critical tools for strengthening the effectiveness of crime prevention interventions.

Operationalising these technologies into practice, however, requires an approach that recognises the complexity of the context in which they are to be deployed and the due diligence necessary to alleviate possible human rights violations. Indeed, the roll-out of surveillance technologies and AI in public spaces poses a threat to peoples’ constitutional rights to privacy and freedom of movement³, in particular, and raises critical questions about whether our desire ‘to feel and be safe’ means that we also have to consent to the omnipresent eye and hand of private security corporations or a ‘surveillance state’.⁴ We also need to be cognisant of the origins of state-led surveillance under Apartheid as well as historically-embedded assumptions about the inherent criminality of certain ‘types’ of people based on what they look like and where they come from. These notions have been used to legitimise racial profiling and constrain peoples’ freedom of movement, leading to social control and the marginalisation of communities from social and economic opportunities. Despite these limitations, technology can offer law enforcement cost-effective solutions for addressing short-falls in capacity. However, rather than outsourcing critical decision-making processes to intelligent systems, we need to consider whether AI and data are supporting the development of a professional police service with credible leadership and accountability, including improved relationships with communities.
Surveillance technology is the use of electronic equipment to monitor and collect information on the behaviour or activities of someone (or something) for purposes of intelligence gathering; preventing, detecting, or investigating crime; or protecting a person, property, or process. The underlying assumption is that surveillance technology deters crime by making law enforcement operations more effective. Evidence suggests, however, that surveillance technology has the alternative effective of just displacing crime into other areas. In South Africa, surveillance technology is used by both public and private actors and includes imaging devices, location-tracking technologies, and communications; and provides a source of data inputs for AI systems, specifically ones used in crime-intelligence operations.

Artificial intelligence (AI) is often defined as the ability of a computer or machine ‘to perform tasks commonly associated with intelligent beings’. What distinguishes AI from other forms of technology is its capacity to engage with, and respond to, a particular set of stimuli by synthesising data inputs, and then, using a series of algorithms, draw a conclusion and decide on a particular course of action based on its interpretation of that data. The rationale for mainstreaming use of AI in crime prevention efforts is that its systems are programmed to be ‘intelligent’, meaning their decision-making processes are accurate and logically sound, based on the presumption that: (1) data inputs meet a baseline for data integrity; and (2) that algorithmic programming is rational and free of bias.

Crime prevention, as traditionally defined, refers to ‘the anticipation, recognition and appraisal of a crime risk and the initiation of some action to remove or reduce it’. Crime, in this regard, refers to both violent and non-violent forms of crime, the commission of which is punishable by law and falls within the mandate of law enforcement. It is also essential to note that while certain types of crime are violent and certain forms of violence are crimes, they are two separate and distinct social phenomena; therefore, the terms ‘crime’ and ‘violence’ cannot be used interchangeably when engaging in discussions on safety in South Africa.

‘Smart’ technology in this Guide refers to technology that has been adapted to collect and transmit vast amounts of data for further interpretation and analysis by AI systems that can be used for various reasons including identifying and tracking specific individuals or groups. For example, ‘Smart’ CCTV surveillance cameras use machine learning (a sub-field of AI) to conduct video analytics to isolate objects or to categorise certain behaviours or characteristics determined to be ‘suspicious’. However, such systems may mistake embedded bias for actual criminal behaviour.

Surveillance technology is the use of electronic equipment to monitor and collect information on the behaviour or activities of someone (or something) for purposes of intelligence gathering; preventing, detecting, or investigating crime; or protecting a person, property, or process. The underlying assumption is that surveillance technology deters crime by making law enforcement operations more effective. Evidence suggests, however, that surveillance technology has the alternative effective of just displacing crime into other areas. In South Africa, surveillance technology is used by both public and private actors and includes imaging devices, location-tracking technologies, and communications; and provides a source of data inputs for AI systems, specifically ones used in crime-intelligence operations.
The South African public’s demand for safety, including for more ‘boots on the ground’ and harsher sentences for violent crimes, means that communities are arguably ripe for the mainstreaming use of surveillance technology equipped with AI-based intelligence. This desire for safety seems to outweigh a desire for personal freedoms and protections. We also need to consider the implications of large-scale, AI-enabled surveillance on policies and programmes aimed at social cohesion, spatial integration and inclusive economic development.

**Johannesburg’s Integrated Intelligence Operations Centre and ‘Smart’ CCTVs**

In May 2019, the City of Johannesburg launched its Integrated Intelligence Operations Centre (IIOC) Reaction Unit as part of its Smart City Programme to serve as the city’s ‘nerve centre’ for municipal data. In addition to hosting the city’s CCTV network, the IIOC uses facial and license plate recognition systems to improve crime detection and investigations and to inform the deployment of municipal resources. During its first month of operation, the IIOC reported a ‘notable crime reduction’ in the inner city, with its rapid-response systems assisting the Johannesburg Metro Police Department (JMPD) in increasing the number of arrests made for crimes ranging from robbery, to drug and firearm possession, to common assault.

Concerns have been raised about which sources of information the IIOC has access to, given the City’s close relationship with law enforcement and the fact that the Reaction Unit is located in JMPD’s headquarters. These concerns are especially relevant in light of Vumacam’s plans to install more than 15 000 ‘Smart’ CCTV across the metro area.
This will have the effect of placing entire sections of the city under mass surveillance, mainly in business districts and higher income areas. In addition, although Vumacam requires a case number or court order before providing its surveillance footage to law enforcement, once information is transferred to third parties, Vumacam loses control over how the data is managed, making it easier for various other public and private entities to access.

**Cape Town’s Emergency Policing & Incident Command and Domestic Drones**

In its effort to become a ‘Smart and Safe City’, the City of Cape Town established the Emergency Policing and Incident Command (EPIC) in 2017 to coordinate responses to public safety concerns by creating an integrated data management platform to roll-out ‘effective, efficient and equitable policing methodologies’ across the metro area. In addition to EPIC, Cape Town Metro Police Department (CTMPD) has adopted other AI systems, such as Crime Mapping (software that pulls data from various sources – including EPIC – to detect, map and respond to crime), Shot Spotter (real-time gunshot detection system that uses geo-location technology), and ANPR to assist with the ‘apprehension of wanted persons and recovery of stolen vehicles’. In addition, the City has established a Camera Response Unit (CRU) to monitor footage from 594 CCTV cameras located across the city, and which is ‘operationally directed by what the network detects’, suggesting that the CRU relies on automated systems to identify which behaviours constitute as ‘suspicious’ and direct its deployment accordingly.

Plans for expansion of EPIC seem to be underway, with news outlets reporting that the City has invested R500 000 in domestic drones to be used ‘to combat crimes of different magnitudes’. JP Smith, the city’s Mayoral Committee Member for Safety & Security, has stated that the drones will be operated by trained individuals in the city’s Safety Directorate and ‘deployed as seen fit’ over areas that have been ‘earmarked for monitoring’ for various reasons, including high incidences of crime. Similar to Vumacam’s expansion of CCTV cameras in Johannesburg, the deployment of drones will take place over entire areas of Cape Town under mass surveillance; however, unlike Johannesburg, where the chief purpose is to secure areas deemed to be worthy of protection, Cape Town’s purpose is to target and identify offenders by criminalising entire communities.
National Development Plan

In 2012, after evaluating successes and weaknesses in the first two decades of South Africa’s democratic transition, the government adopted the National Development Plan 2030: Our future - make it work (NDP), which identified twelve strategic areas to dismantle centuries of racial, social and structural inequality. Building safer communities was, and remains, a key feature of the NDP, with Chapter 12 not only recognising how crime and violence has hindered South Africa’s economic growth, but also how most South Africans do not enjoy their right to be free from violence.

As a consequence, Chapter 12 identifies five priorities for making South Africa safer, including, amongst others: (1) strengthening the criminal justice system by using technology to address inefficiencies in the prevention of crime and in the analysis of ‘current and future threats to safety’; (2) professionalising the police into one that is modern and ‘intelligence-led’; and (3) improving safety using an approach that is integrated, developmental and ‘knowledge-based’.

White Paper on Policing and White Paper on Safety and Security

In 2016, national government adopted two key policy instruments to advance the objectives of Chapter 12, namely the White Paper on Policing (WPP) and the White Paper on Safety and Security (WPSS). These policies were designed to work together to clarify the responsibilities of government departments in building safer communities. While the WPP articulates a vision for professionalising the police into one that is ‘information driven, analytically sound, and evidence and intelligence-led’, the WPSS provides a framework for strengthening the criminal justice system using a ‘knowledge-based approach’ that relies on integrated systems of information and data management. In this regard, both policies recognise the value of technology to embed data-driven and logically-sound decision-making processes, and to increase access to information across government departments.

The WPP, however, places more emphasis on technology, highlighting the potential of tech-driven solutions to enhance the functioning of police services, specifically in crime detection and investigation, and in informing the strategic deployment of resources. Accordingly, the WPP demands that technology ‘support proactive policing and allow for improved efficiency in terms of crime investigation and the analysis of current and future trends’, and offer solutions for information-sharing across the criminal justice systems, including in e-docket and case management systems. The WPP also identifies ‘the ability to proficiently use technology’ as a key quality for police officers, as well as calling on government to identify new types of applicable technology and to ensure an enabling legislative framework for optimising use across law enforcement.

While the WPP focuses on the potential of technology to improve the performance of the police, the WPSS focuses on the need to build systems of integrated data and information management to enhance the effectiveness of crime and violence prevention operations. In this regard, the WPSS aims to embed a knowledge-based approach, which not only requires interventions to be grounded in evidence-based methodologies, but also demands decisions be predicated upon accurate information. The policy thus calls for the establishment of integrated data systems to: (1) collect data in real-time on types,
prevalence, and location of crime; (2) conduct an ongoing comprehensive analysis of crime patterns and trends; and (3) facilitate access to information across the criminal justice system.33

**White Paper on Science, Technology and Innovation and the National Integrated ICT Policy**

Although not directly related to crime prevention, the White Paper on Science, Technology and Innovation (WPSTI)34 and the National Integrated ICT Policy (NIIP)35 identify technology and innovation as key enablers of the NDP’s priorities, including those espoused in Chapter 12. While the WPP discussed earlier calls for the integration of technology in crime prevention operations, it also notes the need for law enforcement officials to use these systems proficiently. Furthermore, although the WPSS is silent about how crime-related data should be collected, it still emphasises the need for such data to be accurate. Accordingly, the WPSTI, NIIP and associated multi-year departmental plans could be useful frameworks for operationalising use of surveillance technology and AI in crime prevention by informing key aspects of system development, training and technology governance in this sector.

**What about the constitutional rights to privacy and freedom of movement?**

Neither the NDP, nor the WPP, nor the WPSS refer to the right to privacy or to freedom of movement. To an extent, this indicates the extent to which government has failed to prioritise civil rights against the call to reduce levels of crime and violence. It is important to note, however, that policy does not supersede law, and that South Africa’s Constitution not only requires limitations on the rights in Chapter 2 to be the least restrictive means necessary for achieving the security objectives of the State, but also for limitations to be conducted in a manner consistent with human dignity.36 Nevertheless, the absence of the right to privacy and freedom of movement from these policies is cause for concern, as it may reflect an embedded perception of civil rights being ‘luxuries’ to aspire to, rather than safeguards against the return of a police state. The WPSTI and NIIP are currently the only policies that include a reference to privacy, and could therefore be an important guide for balancing safety concerns with the protection of civil rights in how technology is developed and used, read together with the Protection of Personal Information Act (POPIA) which sets out a framework for the lawful processing of personal information. However, as noted below, additional measures will need to be taken to protect the right to freedom of movement and the interdependence of rights since this is not at the fore within the broader policy architecture.
RESEARCH PERSPECTIVES AND KEY ISSUES FOR CONSIDERATION

Globally, there is increasing use of advanced data processing and AI technologies for crime prevention. In the European Union, police forces from ten out of twenty-five countries use facial recognition, amongst other predictive policing technologies, with several more likely to do so in the coming year. In many cases, the choice of technology reflects an underlying theory of policing, from targeting hotspots to problem or community-oriented policing, with implications for the police’s relationship with residents and intra-community friction. Some cities and countries have implemented laws to prevent the use of specific technologies or established agencies and guides to regulate their use, such as the UK’s Surveillance Camera Commissioner (SCC) and associated code of practice. However, many concerns have been raised about the inability of existing regulations and codes to remain current, the broader impact of these technologies on society, and the lack of thorough legal frameworks providing oversight on and accountability for their use in crime prevention. These concerns, particularly as they relate to the South African context, are described below.

Infringements on the Right to Privacy and Freedom of Movement

Predominant discourse on the tension between privacy rights and technology relies on the assumption that because people do not enjoy a ‘legitimate expectation of privacy’ in public spaces, the use of surveillance technology does not violate a person’s right to privacy. This position has been reported to have been reiterated and endorsed by the newly established Information Regulator, but does not acknowledge how personal information has been used and commodified by technology in recent years.

Accordingly, Jane Duncan, a professor at the University of Johannesburg, argues that the right to privacy should cover ‘locational privacy’, which is ‘the right of people to move about freely, without having their movements tracked’ given the amount of personal information it contains, including ‘personal, social and political activities’. In this regard, ‘locational privacy’ bridges the conceptual divide between the right to privacy and the right to freedom of movement, and can be useful for expanding and shifting the discourse. Further, the Apartheid government retained its power by suppressing these rights through monitoring people’s private lives and regulating their movements; hence, these technologies should be operationalised in a way that moves away from social control and values the importance of these, and all, constitutional rights.

Thus, the volume of data reflecting people’s movements should be considered ‘personal information’ under South Africa’s POPIA, and consequently protected against the unlawful collection, retention, dissemination and commercialisation by both public and private bodies. Complications arise, however, when people’s personal information is processed under the rubric of ‘national security’, which, in effect, offers law enforcement unrestricted access and subverts the need for reasonable suspicion even when this information is used in the detection and investigation of crime. Furthermore, POPIA makes no mention or reference to the Criminal Procedure Act (CPA). This is of concern in relation to the CPA’s provisions on search and seizure – including those conducted without a warrant – and the potential that such provisions disregards necessary procedural safeguards to prevent unlawful intrusions by the State on a person’s right to privacy. Lastly, as POPIA is an enabling piece of legislation for the right to privacy, it enjoys the
privilege of constitutional supremacy over the CPA.\textsuperscript{44}

\textbf{State-Sanctioned Discrimination and the Criminalisation of Communities}

Although ‘Smart’ technologies are presented as producing intelligent decisions free from bias or prejudice, their operationalisation does not occur in a vacuum. Rather, such technologies are both informed by, and responds to, the unwritten rules of its social, political and economic context. For example, if one of Vumacam’s network of ‘Smart’ CCTV cameras is situated in a middle-class neighbourhood made up of mostly white people, and is programmed to identify ‘suspicious’ individuals who ‘do not belong there’, people who are Black and Coloured are more likely to look like anomalies. Consequently, if there is inherent bias in the data input – such as CCTV cameras concentrated in areas of wealth and thus only recording certain types of activities and individuals – the AI systems law enforcement relies upon to direct its operations will be programmed to replicate those biases, which may instruct them to ‘over police’ certain demographics.\textsuperscript{45} Further, when these biases are validated by ‘data’ and the sources of that data are not appropriately interrogated, the net result is a body of evidence that not only criminalises certain communities, but also justifies state-sanctioned discrimination by the police.

Similar concerns have been echoed globally, including by Professor Renee Cummings who warns against algorithms that ‘encode assumptions and systematic patterns’\textsuperscript{46} about ‘who’ commits crime and ‘where’ those people come from, ultimately reinforcing embedded forms of discrimination and leading to the criminalisation of certain groups and areas. These issues are especially relevant to South Africa given its history of racism, sexism and classism as well as centuries of spatial and economic exclusion under both Apartheid and colonial systems of rule.
While different types of technologies offer many tactical advantages to the police and can reduce crime in targeted areas, they also have the potential to threaten peoples’ constitutional rights and can be a tool for subjecting certain subsets of the population to mass surveillance and exclusion, echoing the practices of Apartheid. Accordingly, the following recommendations are offered to support the use of data and AI-driven technologies in a way that is ethical, legally sound, and socially responsible.

**RECOMMENDATIONS**

1. In order to address the legal implications of technology used by law enforcement officials on the unlawful intrusions on individual right to privacy and freedom of movement, the national security exemptions under POPIA must be brought in line with provisions governing search and seizure under the CPA.

2. There is a need to broaden the ambit of the ‘right to privacy’ under POPIA to include ‘locational privacy’. Strategic litigation and the IR can play a role here in addressing this gap.

3. Take reasonable measures to ensure sources of data inputs do not reflect embedded prejudices or bias, and that algorithms are assessed by independent experts to identify risk of bias or discriminatory impact. In addition, mechanisms should be created to enable interested parties to monitor, check or critique the integrity of algorithmic systems and sources of data.

4. Ensure that investments in innovative technologies are complemented by equitable investments in professionalising the police, not only in building their technical capacities, but also by increasing the standards for hiring and introducing robust systems of performance management, in accordance with the directives of the WPP.

5. Institutionalise standard operating procedures governing use of surveillance technology, AI and ‘Smart’ technology by law enforcement agencies to ensure its scope aligns with legal parameters, specifically regarding the prevention, detection, and investigation of different types of crime, in order to avoid and address incidents of ‘function creep’.
REFERENCES


6. Ibid. Examples of AI include facial and voice recognition systems, which are programmed to analyse and compare the contours of a person’s face for purposes of confirming their identity.

7. National Crime Prevention Institute. 1972. The United Nations Office on Drugs and Crime (UNODC) has developed a definition to include ‘any activity by an individual or group, public or private, which attempts to eliminate crime prior to it occurring or before any additional activity results’; however, the definition provided by the (NCPI) is more suited to the South African context. See https://www.unodc.org/e4j/en/crime-prevention-criminal-justice/module-2/key-issues/1-definition-of-crime-prevention.html


11. These areas also happen to be those that cannot afford such technologies. See, Kwet, M. (2019).


13. eNews Channel Africa. 2019. Outraged South Africans call for death penalty. 3 September. [Interview with Kelly Stone]. https://www.youtube.com/watch?v=AHRkPUAYro


15. Ibid. It is worth noting that the number of arrests in a given area does not necessarily reflect levels of safety.

16. Vumacam is a company that uses CCTV cameras linked to intelligent processing systems, including with facial and voice recognition software, and uses a city fibre network to connect cameras across different neighbourhoods.


20. Ibid at 29- 30.


23. Constitution, at Sec 12.


13
29Ibid at 25.  
30Ibid at 22.  
31Ibid at 43.  
33Ibid.  
36Constitution at Sec 36.  
41Kwet, M. 2019.  
42Duncan, J. 2018, at 42.  
43Protection of Personal Information Act [No 4 of 2013], at Preamble.  
44Criminal Procedure Act [No 51 of 1977], at Preamble.  
45Kwet, M. 2019.  