Re Ntse Re Go Lebile: Computer Vision and AI Surveillance in Africa

Work in Progress Version

409 The Studios
Old Castle Brewery
6 Beach Road
Woodstock, 7925
Cape Town, South Africa
Phone: +27 21 447 6332
Fax: +27 21 447 9529

Table of Contents

1. Introduction

1.1 Overview

Computer vision is at first glance simply technology with general applications so that the political implications are not immediately apparent, unlike technologies such as bio-identity in which purpose is fused with the technology. The political valence of computer vision depends on the particular purposes for which computer vision is deployed. Although computer vision has in common with other AI technologies issues in the creation, representativity and access to datasets, not least the conditions of labour required inputs to AI systems, it has its own concerns. One area where computer vision has significant implications is for practises of surveillance. Enabling continuous visual surveillance at a scale hitherto unimaginable, computer vision (CV) is reshaping the surveillance landscape in Africa. Globally computer vision has been a topic of increasing interest and study due to its wide use in facial recognition systems, surveillance networks, virtual reality, and other similar fields. The full implications of widespread, interconnected, autonomous surveillance is not yet well understood, but they implicate human rights, particularly the rights to privacy and autonomy.

Artificial Intelligence technology has its origins in efforts to mimic human intelligence through the hardware and software of computer systems. While this goal remains elusive some AI technologies seek to emulate human abilities. Computer vision is one of several multi-purpose technologies developed under the broader category of AI. Similar multi-purpose technologies include natural language processing and decisions intelligence. As a multipurpose technology computer vision can be deployed for a number of different uses including analysing satellite or drone footage, facial recognition, gait recognition, number plate recognition and automated visual surveillance. Many African countries are increasingly introducing advanced AI surveillance tools and technologies to monitor, track and surveil their citizens. , and cities are tapping into AI technology to monitor traffic and fight crime. Yet these technologies are deployed to accomplish a range of policy objectives— many are lawful, whereas some have an unclear mandate and hidden from public scrutiny.

The basis of computer vision is the development of technologies that have transitioned from analogue cameras that use coaxial cables to transfer data to a DVR (Digital Video Recorder) to digital IP cameras (capable of transmitting data over signals to be stored in the network). IP cameras can also be associated with features such as: cloud storage, wireless connections and remote sensing (also referred to as intelligent video content analytics). Together these constitute “smart CCTV cameras” powered with “AI

surveillance" (BIS Research, 2019). While smart CCTV networks are powered through video surveillance capable of analysing data, (BIS Research, 2019) describes this terminology as "a technology that processes a digital video signal using a special algorithm to perform a security-related function".

Commentators (Swart & Munoriyarwa, 2020) paint a general picture of Africa's AI-powered surveillance landscape — characterised by: facial recognition and digital analytics, using technologies mainly imported from foreign countries by big technology firms e.g (Swart, 2018b). An important factor influencing the deployment of AI surveillance technologies is technology companies capitalises lobbying (BIS Research, 2019) claiming; to meet demand by governments to improve public safety and to reduced costs on policing and interaction with police and citizens, government Interest in data processing and ownership and growing interest in AI surveillance tools due to pervasiveness of crime, developing smart cities and automating processes. An additional political dimension of this pervasive technologies is that political regimes tend to swiftly deploy surveillance technologies more quickly and assume control of these technologies that results in greater exclusion (Khan & Roy, 2019).

Many countries still lack adequate data protection laws, a prerequisite for the introduction of Artificial Intelligence and Machine Learning technologies using as they do vast amount of data, for many applications. If there are policies governing AI, they are often too broad to account for the context-specific impact of technology on human and citizen rights, or they quickly become outdated. There are also concerns about companies' access to personal data - particularly through partnerships with the government. In addition to the impact of bias on decision making, there is the problem of the quality of data that has been incorporated into AI (Plantinga et al., 2019). Accordingly, the current expansion of AI surveillance in Africa requires urgent consideration of the following potential benefits and limitations in society (Buolamwini & Gebru, 2018b): accessibility, privacy and trust, explainability and accountability.

Computer vision has introduced new challenges, opening up debates about how society engages with the legality of surveillance technology and its potential effects. Are African countries ready for computer vision? Readiness of a state for computer vision is more than just a government plan to purchase and install new technologies or to encourage or observe corporations using computer vision. The transformative power of AI technologies necessitates creation of capacity in a number of critical areas. To capitalise on AI's potential for development, the government would need a strategy for retooling related internal processes, upskilling or recruiting key employees, optimising approaches to collaboration, and building the necessary data and technological infrastructure to implement AI.

When it comes to Africa's AI readiness and technology scene, the 2020 Government AI Readiness Index tells a similar story. Only one African country is in the top 50, and only ten African countries (out of the 54

in the continent) are in the top 100 of the lists. The top five African governments — Mauritius (45th), South Africa (59th), Seychelles (68th), Kenya (71st), and Rwanda (87th) – reflect these countries' improvements in technological developments. Overall, African countries have made progress in data and infrastructure, governance, and technical advancements (Oxford Insights, 2020). Given the different waves of technological revolutions that African countries have "leapfrogged," the continent still to faces difficulties capturing the benefits of new technologies. In this instance the rate of technological development seems likely to outpace the skills needed to 'leapfrog' including AI skills.

1.2 Computer Vision Technologies

This research adopts the following working definition of computer vision: ***Computer vision*** *is defined in this study as a set of approaches, techniques, methods, and practices used to create computer systems with the ability to perceive imagery, detect patterns in imagery and model imagery, and thus assist human or computer systems in making decisions.*

Computer vision has been around as a field of theory and practice in computer science for over five decades and computer vision applications are ubiquitous in computing and daily life. Computer vision is used in a multitude of applications including: scanning documents, optical character recognition (OCR), barcodes, QR codes; when we clean up and manipulate imagery, in the steering of unmanned vehicles such as drones and in biometrics. The current general objective of advanced and cutting-edge computer vision is to teach machines to perform tasks that are in response to the visual world and associated with human intelligence. This is commonly expressed as teaching machines to perceive the visual world. Fei-Fei Li has expressed the objective of computer vision as "to teach the machines to see just like we do: naming objects, identifying people, inferring geometry of things, understanding relations, emotions, actions, and intentions" (Li, 2015). There are three categories of computer analytics relevant to computer vision (Norman, 2017)): fixed algorithm analytics, AI learning algorithms and facial Recognition systems. Safety and security are public goods. The phrase 'public goods' refers to two attributes of a good: that others cannot be excluded from the good and that it is not necessary for someone to be denied access to the good for someone else to enjoy the good. For safety and security, it is not necessary for some to be excluded from the benefits of policing for others to benefit, instead apprehending and convicting criminals benefits everyone in a society. But safety and security are localised public goods so that benefits are localised unlike universal public goods such as knowledge.

Although the techniques of computer vision have changed over the decades, computer vision has been a field of theory and practice in both computer science and engineering since at least the 1970s (Szeliski, 2011). In the 1970s computer vision was initially conceived of as an important component of both Artificial Intelligence (AI), and automated systems (Szeliski, 2011). The problems presented by computer vision proved harder to solve - i.e., there are still no systems that are better at recognising images than for example a two year old (Szeliski, 2011).[1] Computer vision is still conceived of as a subfield of AI (Li, 2015). A definition of computer vision is "a subset of mainstream artificial intelligence that deals with the science of making computers or machines visually enabled, i.e., they can analyze and understand an image" (Mishra, 2019).

Computer vision can be deployed for purposes other than surveillance. One of the most development friendly deployments of computer vision is analysing drone footage for agricultural purposes. This is illustrated by Aerotel, a successful South African agri-tech company operating in hundreds of farms in 18 countries across the world including in the US and Australia (Fast Company, n.d.; Lyudvig, 2020). Aerobotics, founded in 2014 in Cape Town (Jackson, 2020), makes use of drone and satellite imagery, artificial intelligence algorithms and proprietary software to monitoring the state of agricultural crops, in order to assist farmers to increase the quality and quantity of their yield (Fast Company, n.d.; Jackson, 2020a). Aerobotics has received two rounds of funding from Naspers; 5,5 million USD in May 2020, and 16,5 million/17 million* in December 2020 (Jackson, 2020a, 2020b; Space in Africa, 2021). Data collated by Aeroview or any other app is not sold or shared with any third parties (Aerobotics, n.d.-a).

Clients have the right to have their data expunged from the system on request. It is unlikely that most of the data processed by Aerobotics is personal data nor does the processing seem likely to implicate fundamental rights. Aerobotics seems to be an example of a successful deployment of computer vision technologies that enable development. Farmers will be able to not only forecast but prove likely crop yields, a crucial prerequisite for both planning and obtaining capital. Aggregated data would enable governments and aid agencies to predict crop yields, an important aspect of food security. Aerobotics illustrates computer vision technology may be deployed in ways that enable development. As demonstrated by the case studies discussed later computer vision may also be deployed in ways that are more ambivalent such as surveillance.

1 A two year old can apply abstract concepts to an image, create a model of the image, and fill in missing details in order to correctly identify it. This is why, for example, a child can see both a photography and an illustration of for example a tshongololo, or rabbit, and correctly identify both the photograph and cartoon image. This recognition of imagery with abstract dimensions and missing details is a challenge that computer vision systems equipped with Neural Network and deep learning algorithms are still struggling to do.

1.3 The Politics of Computer Vision production

1.3.1 Politics of Datasets

A large amount of human labour is frequently required to train neural networks. This is because for processes such as machine learning neural networks need to be provided with large amounts of data that has been labelled both in terms of the inputs and expected outputs. The Imagenet database, a database of labelled images used to train computer vision algorithms required a large amount of human labour to create. Fourteen million images were hand annotated in the creation of the Imagenet database ("New computer vision challenge wants to teach robots to see in 3D").

While building computer vision systems requires data, Machine Learning systems that are supervised often use labelled dataset to train algorithms and classify data to predict accurate results. Postulating further on this, Crawford and Paglen (Crawford & Paglen, 2019), highlight an important point that: “training sets, then, are the foundation on which contemporary machine-learning systems are built” and “are central to how AI systems recognise and interpret the world. These datasets shape the epistemic boundaries governing how AI systems operate, and thus are an essential part of understanding socially significant questions about AI”. Training sets for computer vision systems “consist of a collection of images that have been labelled in various ways and sorted into categories. As such, we can describe their overall architecture as generally consisting of three layers: the overall taxonomy (the aggregate of classes and their hierarchical nesting, if applicable), the individual classes (the singular categories that images are organized into, e.g., “apple,”), and each individually labelled image (i.e., an individual picture that has been labelled an apple).” Crawford and Paglen's “contention is that every layer of a given training set’s architecture is infused with politics.”

In the process of the creation and labelling of datasets, societal biases can be transferred to AI systems. Datasets for training can be labelled with terms that encompass societal biases and reinforce societal inequalities. Algorithms may learn societal biases by learning from historical datasets (e.g. a sentencing or parole algorithm in the US may learn that black males get higher sentences and stricter parole traditions, or am employment algorithm may learn a preference to hire white males). Diversity in datasets can also imbue biases in systems and affect quality of outcomes. For example, Boulamwini and Gebru investigated major commercial facial recognition systems and demonstrated that these systems were less accurate at recognising black faces, in particular in recognising black women’s faces.

1.4 Privacy and Surveillance

1.4.1 Computer Vision Surveillance Technologies

Computer vision enables an array of surveillance applications including facial recognition, biometrics, gait recognition and number plate tracking. AI surveillance technologies are deployed by governments for various functions including Smart City / Safe City, Facial Recognition Systems and Smart Policing (Feldstein, 2019a) . 'Smart policing' is data-driven analytic technology used to facilitate investigations and police response; some systems incorporate algorithmic analysis to make predictions about future crimes. 'Smart cities' can make use of facial recognition systems, as can smart policing. Smart cities may include smart policing but need not do so.

Applying sophisticated smart analytics and algorithms in AI helps automate the whole process of surveillance by detecting events as they happen and predict behavioural changes to improve security. These methods are even adopted by law enforcement agencies for deployment at large scale private enterprises. Traditionally video surveillance only offered a reactive action (analysing video footage to get an outcome), but with smart analytics, it adds an element of proactivity. In addition, smart analytics only focuses on critical events for storing data, which reduces storage capacity and consumes low bandwidth. Analytics demands lots of computational power, which puts pressure on data centres (Carew, 2019).

These technologies while demanding capital and skills investment change the calculus of surveillance for states. In particular they enable mass surveillance that was not possible before. Consequently, issues of privacy can no longer be viewed as primarily about the rights of individuals but instead of a shift in power relations. As noted in the AI Global Surveillance Index (AIGS), the proliferation of AI technologies ultimately means a shift in state-to-private-sector power ties (Feldstein, 2019a), a paradigm shift with implications for privacy and security, data ownership and accountability.

1.4.2 Politics of Privacy and Surveillance

Driving computer vision surveillance technology is the incentive to reduce human interaction in the analysis pf large-scale video streams, to achieve optimal system efficiency. The demand for big video data has expanded in the form of increased number of cameras mounted in public spaces, resulting in mining large data stream from public surveillance that is easily exploitable by the police force for community policing and public safety. Intelligent video surveillance works effectively in this case by embedding computer vision technologies, together with networked cameras deployed in public spaces, enabling systems to identify, classify and track individuals, and to analyse the behaviour of individuals and groups. If the

activity takes place in a public space, why characterise it as surveillance? Should the resultant issues be viewed only as issues of ethics or of both ethics and human rights?

Given the importance of privacy addressing these questions, this paper asserts that the concerns to privacy posed by AI-augmented surveillance technology must be considered. While both of these highlights key issues, privacy laws are complex already even without including all of the social and political issues that can emerge from data exploitation. To assess the impact of AI surveillance on privacy, it is crucial to differentiate between data concerns that are common to all AI, such as the occurrence of false positives and negatives or generalization to patterns, and those that are unique to the usage of personal data.This argument focuses on algorithmic bias and the possibility for algorithms to cause unlawful outcomes or prejudice in the judgments to which they relate. These are key concerns in a human rights setting and individual citizens that represent marginalized populations.

The debate about whether to use a human rights framework or an ethical framework when considering AI governance extends beyond the discourse of AI surveillance. On this subject, there is a broader debate in AI governance circles between governments, the private sector, and other relevant stakeholders. It is true that there are concerns against using a strictly human rights-based approach when it comes to AI surveillance because it is arguably too restrictive and fails to properly understand all of the various impacts that comes with automation, digitisation and datafication in AI systems on humans and societies.

While most sectors' regulatory frameworks are founded on a legal, rights-based approach, the debate concerning AI has to date rather unusually been mostly centred on ethics. Corporate strategies fail to align with international human rights laws for instance, the United Nations Guiding Principles on Business and Human Rights (“the Principles”), which serve as a set of principles for nations and companies to “prevent, address, and remedy human rights abuses committed in business operations,”. Although the guiding principles make no reference to AI ethics they require corporations avoid the consequences, they should thus be used to judge the outcomes of AI ethics. International human rights and legal frameworks must serve as a strong basis for developing, assessing, and revising ethical frameworks for machine learning, including measures for transparency and recourse.

Researchers from Harvard University's Berkman Klein Center identified eight key thematic areas in relation to AI principles in their report titled “mapping consensus in ethical and rights-based approaches to principles for AI” which includes the following: “privacy, accountability, safety and security, transparency and explainability, fairness and non-discrimination, human control of technology, professional responsibility, and the promotion of human values”. These provide some insight into the underlying criteria for

what ethical and human-rights-respecting AI would look like (Fjeld et al., 2020). The themes should help bridge the gap between high level rights and principles and application to technologies.

1.4.3 Surveillance

Consequently, the concept of surveillance is essential to our research. Since at least the 1950s scholars have paid attention to surveillance as requiring attention, currently through surveillance studies (Ball et al., 2012; Beckman, 2016). Interest in surveillance is connected to greater recognition within democratic communities of issues connected to human rights violations, racism, imperialism, communism and anti-democratic conduct. Surveillance is approached in a multi-disciplinary way including from political theory, social security, law and culture, and criminology.

Surveillance has routinely been linked to crime reduction measures. Rapid developments in this field reflects the importance of human rights, privacy concerns and the emerging social science controversies of maintaining public safety and mass surveillance. Presenting surveillance as a hierarchy, “watching over” or “social control” is insufficient.

The broad definition provided by Gary T Marx has been widely quoted: "Surveillance if human (although not always interchangeable with human surveillance) can be defined as regard for attendance to a person or factors presumed to be associated with a person." (Marx, 2015). This definition does not build upon the control objective, nor does it specify directionality (Marx, 2015) (New surveillance methods can be defined as scrutiny of people, groups, and contexts through the use of technical means to extract or create information. The use of 'technical means' to extract and generate the data in this definition implies the ability to go beyond what is naturally offered or voluntarily reported to the senses and minds unsupported by technology.

1.4.4 Privacy

Does the right to privacy conflict with automated visual observation in a public space? How do smart camera networks intersect with the right to privacy? The right to privacy is protected by international human rights law and in many constitutions. But how does it relate to automated cameras in public or semi-public place? Increasingly private companies are advancing their data-related capabilities and government acquiring new technologies and integrating AI surveillance into policing communities (Adrienn, 2016). The right to privacy is a basic human right and a fundamental right in many constitutional democracies, but its precise contours vary according to the dominant social characteristics, values and norms, and economic circumstances of modern times. While the notion of privacy has a lengthy historical context dating back to the 19th century, it also must be elucidated to fit into the narrative of modern-day surveillance technologies and be examined in their current (Schoeman, 1984).

The judgement of the United States Supreme Court in the *Katz* case (*Katz vs United States*, 1967)) has proven influential in developing the right to privacy well beyond the legal jurisdiction of the court. The court ruled that an individual must have a 'reasonable expectation of privacy' in order for the right of privacy to apply. Factors that are important in determining a reasonable expectation of privacy included the expectations of society and the place where the intrusion took place. Some judicial decisions have tended to lower the expectation of privacy where new technologies allow hitherto unknown ways of gathering information. Perhaps the most famous example was Barabara Streisands' unsuccessful attempt to have an arial photograph of the California coastline that included her Malibu mansion supressed. However, this places the determination of the extent of a basic human right in the hands of technologists rather than courts charged with upholding those rights.

Individuals in public spaces have a lower expectation of privacy and its currently accepted that persons in public spaces don't have a right to prevent being photographed as part of a general street scene or the like, although they may object to being singled out and publicised in certain circumstances (*Wells v Atoll Media (Pty) Ltd and Another [2009] ZAWCHC 173*, 2009). However what computer vision enables is far beyond inclusion in the background scene of a public place. Through computer vision individuals can be consistently identified as the same individuals, have their movements tracked via multiple cameras over distances and time, and have their faces, gaits and vehicles recognised. Computer vision could identify a pattern, such as that an individual routinely enters a particular building at a certain time on a certain day each week. This could lead to an inference of information that the individual would prefer to keep private such as visits to a psychotherapist or a sexually transmitted diseases clinic.

1.4.5 Sustained automated observation.

But this example does not fully convey the impact of sustained automated observation. To appreciate how profoundly computer vision may affect people Foucalt's analysis of the concept of surveillance is pertinent (Foucault, 1975). Foucalt considers the idea of a panopticon, first suggested by Jeremy Bentham. In Bentham's account a specially constructed prison would enable guards to observe prisoners at any time while prisoners would be unable to know whether they are under observation. As a consequence, the prisoner will have a constant sense of being watched and change his behaviour. The discipline attendant on being observed in Bentham's scheme is dependent on technology and confined to particular places.

According to Bentham these places could include not only prisons but hospitals for the mentally ill and schools. Foucalt argued that Western society modifies behaviour through a panoptical apparatus that is not reliant on the technologies suggested by Bentham nor confined to specific places. The observational

capacities of those in authority instil conformity. The impact of computer vision coupled with networked cameras is thus not comparable to an individual being casually photographed in public or even being followed surreptitiously by a detective. Instead, the population of a city can be subjected to continuous observation by an observation machinery with inhuman powers of recall and pattern recognition.

Even a clear set of rules that protects individual privacy in the processes of automated surveillance do not address the power imbalance introduced by automated surveillance. Bentham proposed the panopticon for the correction of social delinquents, in prisons, mental health institutions and schools. Foucalt suggested that panopticism was operating by indirect means through society however in his account the means were subtle, if pervasive. Other writers have suggested that the Internet has become a panopticon; the technology intended to spread information was repurposed to gather information. However automated surveillance of public spaces realises Bentham's vision more immediately and directly, the street is now the equivalent of Bentham's prison.

The public, in spaces monitored by networked smart cameras are subjected to a sustained gaze, unable to determine when a human operator may be alerted to them and their behaviour by an algorithm, unable even to guess what behaviour the algorithm may regard as suspicious. While the full implications of this are yet to be traced or understood its clear that personal data safeguards are inadequate to meet the profound social change. What will the effect of mass public surveillance be on people as citizens? How will it change power relationships with the state? This research cannot answer these questions. They remain important by showing what is at stake in computer vision surveillance.

2. Methodology and Research Questions

2.1 Landscape Mapping

The first phase of the Computer Vision theme of the AI4D research included a mapping exercise. which sought to identify computer vision initiatives in Africa, particularly those with public interest issues. As we try to better understand how these countries are deploying AI tools of computer vision and for what purpose, the mapping's goal is to identify how computer vision that enables mass surveillance that could potentially reshape governments' ability to monitor and track citizens or systems is being deployed in Africa. It investigates: What specific types of computer vision systems are being deployed in Africa? Which countries are deploying AI surveillance systems that rely on computer vision and for what purpose? Which companies (uses/applications) are driving import of these technologies to monitor, track and surveil people?

Public interest in this context encompasses those in the public sector, public private partnerships and those initiatives in which services or powers usually the purview of the public sector are taken on by the public sector. The term 'initiatives' was used because both the rapidly changing nature of AI technology, and the oftentimes hyperbolic claims of AI that had not yet been developed meant that the term projects would be inapt.

The mapping does is not a comprehensive scan of the computer vision or even the AI surveillance landscape in Africa. Instead, it identified a number of AI surveillance projects and confirms that computer vision AI is an emerging field in the continent. Initiatives categorised as (i) facial recognition (eight countries), (ii) smart city/safe city (seven countries), (iii) smart policing (six countries). Initiatives were classified in terms of their status as: proposed, launched, advanced or terminated. Theoretical definitions of these initiatives and descriptive approaches were often not available to enable clear characterisation that would have differentiated them from one another.

AI surveillance systems for monitoring and tracking by governments has seen widespread adoption by African countries. AI's computer vision transforms CCTV cameras from an illusion of security to a proactive tool in the battle against crime through facial and object recognition. In a public safety setting AI surveillance capability — programmed by humans and datasets trained over time —could analyse millions of datasets in a form of virtual feeds to track, monitor and warn authorities of anomalies in the public spaces.

Emerging AI based analytics video surveillance with current public safety CCTV surveillance networks shows what the future of public safety could look like. It is positioned to potentially transform the AI surveillance ecosystem across African countries. Preliminary findings of RIA's mapping data reveals that at least fourteen out of 54 countries in Africa are actively deploying AI-powered surveillance technologies (Mudongo, 2021) which (Feldstein, 2019a, p. 8) affirms that indeed "African regions are robust adopters of these tools". However, there a paucity of publicly available data to concretely justify this arguments, many African governments often conceal information about their surveillance operations, making it extremely difficult to investigate how these tools are utilised. The risk is that it will be impossible for people to reach a court of law in the future to seek justice or recourse in cases of human rights violations as a result of surveillance. Privacy may be infringed, and individuals may be subject to surveillance without their knowledge or at least without proof. Without public knowledge of surveillance, it will be difficult to demonstrate that human rights have been violated.

2.2 Case Study Background

Technological developments have enhanced opportunities for state surveillance and interception of people's movements. Surveillance by the state facilitates the gathering and analysis of personal data, together with privately held information it can be aggregated to provide insights to information, resulting in a breach of the right to privacy. The right to privacy is a fundamental human right enshrined in international treaties. International law requires that if there is a violation of the right to privacy, it must be reasonable, legal and proportionate. There is currently a regional flurry in uptake and deployment of state-driven surveillance technologies and tools that support computer vision, South Africa is no exception to these developments (Duncan, 2018). Despite national laws regulating the usage of surveillance technologies being inadequate or non-existent, this is likely to result in illegal and unreasonable interference with people's right to privacy.

Although CCTV monitoring can be a powerful tool that improves the safety and security of the public, protection of persons and property, and the detection of crime. It may also be used as a source of coercion. Surveillance technologies could, however, be vulnerable to abuse by the state, companies and individuals as a mechanism for mass surveillance in ways that compromises human rights and privacy (Jili, 2020; Woodhams, 2020).

CCTV cameras are often found in, amongst other public areas; streets and shopping malls, outside playgrounds and outside government and private buildings. In a radio interview, a former member of the Johannesburg City Council's Police and Security Commission, Michael Sun, said that CCTV cameras appealed to local governments for 'public space security, traffic management, crowd control, predicting and managing disasters' which apparently refers to automatic facial and licence plate recognition related data will be generated by over 400 CCTV cameras in Johannesburg inner city to combat growing crime (eNCA, 2019). While most of the technical knowledge resides outside South Africa, he indicated that Chinese technology companies such as Hikvision and Huawei have approached South Africa with 'daily demos' of their products (Zama, 2019). The use of CCTV surveillance can be helpful in transforming policing and crime reduction strategies, in most cases these cameras are used for a number of purposes e.g. fighting criminal activities, policing and monitoring neighbourhoods through detecting 'abnormal' activities such as loitering. While people are concerned about their personal privacy others want surveillance technologies because they believe it combats criminal activities in their communities. This has led critical voices to lobby for bans of this technologies. For instance, in 2020 Rights2Know (R2K) launched a

campaign urging the City of Johannesburg to remove the 58 “illegal” public surveillance cameras in Lonehill neighbourhood (Mabena, 2020; Sibembe, 2019).

There is a major risk of function creep with smart surveillance technologies, which may lead to their use for purposes not originally intended. There is a significant possibility that already vulnerable populations may in the future experience increased surveillance linked to their ability to gain access to centralized government services especially social security. AI surveillance technology has the ability to intensify these risks of social sorting. South Africa is unlikely to become a fully-fledged surveillance state in the immediate future and this is due to resource constraints and government capacity to manage these technologies effectively and constitutional constraints. However, in the short term, machine learning technologies are already dominating, powered primarily by commercial players. To understand this better we selected the “Safe City” CCTV project in Botswana, and CCTV networks in South Africa (Johannesburg and Cape Town) as case studies. While both are focused on Southern Africa there are nevertheless important distinctions between them to enable the identification of both comparisons and contrasts. Both the Botswana and South African cases are putative deployments of computer vision for surveillance. But while the Botswana project has a national government mandate, local governments and private corporations operate the South African networks. Privately run networks such as the Vumacam initiative analysed in the South Africa case study purports to provide a public good, that is traditionally provided by the state, security from crime.

2.3 Case study Questions

The research primarily involved review of the scholarly and grey literature and media reports, but the research did request for information and request from the Botswana Police Services (BPS) and no information or comment was received. Huawei and ICT Dynamics, who are primary technology provider where not contacted, since the public body has responsibility for governance.

The case studies conceive of computer vision systems, as like other digital technologies that may bring benefits to developing countries but may also introduce new risks and harms peculiar to computer vision as an AI enabled technology. The context of the research is that computer vision is increasingly being used in Africa. There is also significant preparation to employ computer vision systems such as creation of automated camera networks. However, there is little formal assessment of the benefits, harms and governance of these systems. Globally there is a surge of research on AI and whether it is used ethically and beneficially. However there is comparatively little research in Africa. This trend is repeated for computer vision. While there is global research on governance, ethical and rights aspects of computer vision especially face recognition there is little research in Africa.

An AI system is trained to a specific task, there is currently no general purpose AI. Instead there is 'narrow AI' that is specific technologies that are able to carry out well defined tasks. One of these technologies is computer vision, the recognition and computerised analysis of people and objects recorded in photographic and video. While computer vision may be deployed in identification and thus overlaps with bio-id it enables other kinds of analysis and thus requires separate analysis.

The key inquiry of the case studies is: *Is governance especially regulation of computer vision sufficient to protect human rights in the emerging countries as evidenced by the study countries?*

There are two case studies: Botswana and South Africa are considered from the beginning of each initiative to March 2020. These two cases are used because there is sufficiently similarity in the jurisdictions while the one case looks at the roll out of a state system, though through a PPP, and the other a private system. The analysis considers the different implications of these two system in relation to both obligations to and rights of citizens.

The research proceeds on the following assumptions:

- Networks consisting of connected digital cameras and remote computerised storage such as those built and being built in several African countries can be used for computer vision including automated surveillance.
- Camera networks capable of supporting computer vision will be used for computer vision applications even if not immediately.
- When governments and private actors working with governments or providing public goods deploy computer vision for automated surveillance without transparency then the lack of transparency is itself a threat to human rights.
- When governments and private actors working with governments or providing public goods deploy computer vision without a clear legal basis to do so then the lack of a clear legal basis is itself a threat to human rights.
- When governments and private actors working with governments or providing public goods deploy computer vision without appropriate governance then the lack of governance is itself a threat to human rights.

The research raises the following propositions on both case studies:

- Computer vision networks capable of automated surveillance are being deployed in Botswana and South Africa without sufficient transparency.
- Computer vision networks capable of automated surveillance are being deployed in Botswana and South Africa without sufficient legal basis.
- Computer vision networks capable of automated surveillance are being deployed in Botswana and South Africa without sufficient appropriate governance.

Each case study will consider six questions:

- What are the benefits of the use of this use computer vision? Who benefits?
- What is the impact of this use of computer vision deployment on inequality? Does this use of computer vision increase or decrease inequality and exclusion?
- Does this use of computer vision introduce new inequalities or exclusions?
- What governance is in place for this use of computer vision? Are measures in place to regulate and govern this use of computer vision systems in order to circumscribe their power and autonomy over human beings, as well as their use by self-seeking actors to exercise control over others, especially the most vulnerable populations? What types of systems are required? Who owns and controls the data and algorithms underlying this use of computer vision? Is control exercised primarily through legal or other means? What are the unique challenges emerging in this respect (e.g. dominance of global players)?
- To what extent are the countries that are host to these initiatives ready for these kinds of computer vision? Do they have the resources to sustain and expand these kinds of computer vision? How reliant are they on private actors/foreign corporation?
- What are the human rights implications and realities associated with the this use of computer vision? Does computer vision affect critical service delivery and other systems? To what extent can regulation of personal data protect human rights when computer vision is used?
- What risks and potential harms accompany the deployment of this kind computer vision in the study countries and how can they be mitigated?

3. Case Study 1: Automated Surveillance in for Safe City's in Botswana

3.1 Introduction

Despite a recent surge in interest and investment in AI surveillance technologies by African states, including Botswana; existing governance and regulatory frameworks of AI surveillance technologies deployed for public surveillance and safety has not shown much level of maturity in the country. With so much data

available today, it is understandable that many critiques exhibit wariness of plans by governments and law enforcement that call for data collection and ownership, given the possibility for misuse of data (Research ICT Africa, 2021). For instance, the South African government is advocating for data sovereignty by proposing the “National Data and Cloud Policy” and these developments highlight contradictions with current international data governance principles, and the implications of this policy might well alter data usage practice across Africa (Van der Spuy, 2021).

Without any legal constraints, it could be relatively simple for the government and private companies to create databases of image data of the vast majority of people and use those databases to identify and track people in real time. An example of this scenario emerged when Cloudwalk sparked international outrage in 2018 after signing a strategic partnership deal with the Zimbabwean government to develop a mass facial recognition database and train its systems to recognize faces with darker complexion (Chutel, 2018).

Although this is no surprise especially with current regional developments of AI surveillance, what’s alarming is the manner in which these companies deploy surveillance systems is combined with their relative anonymity, which reveals just how the market for AI surveillance systems is dominated by a small number of opaque suppliers that import these systems into Botswana without any sufficient accuracy testing of the systems as they are utilized in the public areas, and without the implementation of legal safeguards to avoid internal and external misuse.

The Botswana’s Public Closed Circuit Television (CCTV) surveillance network can be noticed in both Gaborone and Francistown and while CCTV is one of the tools that can be used as a form of Situational Crime Prevention mechanism. Often times it is claimed to be associated with lowering crime by working as a form of surveillance. Despite the lack of independently verified data to support CCTV as a broad solution for crime prevention, it does have other significant advantages, such as assisting police criminal prosecutions. But to satisfy this argument, however, more research will be required to identify and decipher the specific components of efficient CCTV solutions.

There is considerable amount of evidence that points to main drivers of this technological developments in Botswana emerging from both private technology companies, particularly Huawei and ICT Dynamics along with subsidiary companies and the government of Botswana. This study shows how existing surveillance networks in Botswana are transforming the ability of the government in monitoring civilians and its implications in society by exploring the following how they operate and what the governance of the networks is.

Analysis of the networks requires attention to several inter-related questions: how are CCTV surveillance data gathered through CCTV cameras installed in public spaces and other forms of facial recognition technologies? What is government's role in collecting, storing and processing CCTV surveillance data in centralised digital databases? Is the data collected used only for the purpose for which it is collected or is it shared amongst government departments, agencies or private sector? Do CCTV surveillance practices protect citizens right to privacy and the balance for maintaining public safety? What is the role of law-makers and regulators in protecting the rights to privacy with regards to surveillance data? Does the surveillance system use facial recognition technology? Does the system use gait recognition (automatically extracting movement characteristics of the walking person in the video) technology?

3.2 Defining the Case Study

3.2.1 Stated Purpose

The "Safe City Project" is the product of the Safer City program announced by former President Ian Khama during the 2015 State of the Nation address to create capability for policing by means of CCTV cameras (Mdalani, 2015). The President stated that such a programme would address the reliability of the response systems as well as speed up the prosecution and prevention of crime.

We understand that Huawei as a main partner of this project its main objective is to develop smart cities globally is centred around sustainable economic development and growth (Huawei, 2016). Besides ICT use at the core of driving the success of smart cities, governance, data management, and partnership models are widely considered to be Huawei's area of interest in the development of non-ICT related factors. In contrast with these core elements, Botswana's main purpose for this project is to deliver public security and create a safe space by using surveillance systems that prevent violence and respond more effectively to public emergencies.

Yet again the President attributes the reduction of crime as a result of the current CCTV deployment during his state of the nation address speech. Given this argument, the use of CCTV surveillance by local authority still shows granular data which makes it difficult to assess the current investments into this intervention:

> "…4.4% in violent and intrusive crimes from 7,629 to 7,295 and a 4.7% decrease in serious crimes from 5,566 to 5,304 cases reported in 2019 vs. 2018" (Republic of Botswana, 2020)

Huawei claims that achieving the objectives of a Smart City/Safe City will need a holistic approach to design, where each architectural component above may be interlinked, thus retaining the capacity to achieve the required capabilities. Huawei also says it will utilise advanced analytics and new

technologies that help emergency management services in the context of developing smart/safe cities in creating “healthy and liveable neighbourhoods” (McGinty, 2017).

3.2.2 Technology

The “Safe City Project” is a CCTV surveillance network deployed in Botswana's two main cities (Francistown and Gaborone) and led by Huawei Technologies. The Botswana Police Service (BPS) released a statement to validate more on the details on the project, saying it is a:

> “…multinational monitoring network of high standards that would include, high-definition cameras, traffic signals installed along busy roads and at busy highway intersections, high-value intelligence lenses around strategic corporate enclaves and sophisticated software package” (Ramaphane, 2017)

In a 2016 publicly available white paper, Huawei describes its Safe City model as a “suite of technology that includes video surveillance, emergent video communication, integrated incident command and control, big data, mobile, and secured public safety cloud” to support local law enforcement and policing. It is not clear whether Huawei’s safe city solutions incorporate AI-powered facial recognition technology in the CCTV surveillance network of the Safe City project in Botswana. It is well known globally though that Huawei’s CCTV cameras do support “facial recognition” (T. Wilson & Murgia, 2019), a biometric system that uses cameras, both video and still images, to align individuals' saved or live footage with database images (Kaspersky, 2021).

Safe City or “Smart City” technologies as well-known from Huawei are focused on universal connectivity, interoperability of information (both exchange and aggregation of information), and inter-departmental cooperation. Our knowledge of the Safe City project in Botswana is largely based on limited data in understanding what dataset Huawei and the government of Botswana use to train models in the CCTV surveillance network, or how data analytics and algorithms will be used for potential policing activities. More recent evidence from (Molepo et al., 2020, p. 152) reveals that the CCTV surveillance network features the following:

- Fixed cameras that rely on a single view and pan-tilt-zoom (PTZ) CCTV camera models that have complex intelligence systems mounted operating in them, such as number plate or face recognition.
- Optic fibre transmission embedded for network connectivity with various site models configured for different users to support the national monitoring system.

- High resolution camera-powered video surveillance which allows improved tracking and dispatch which has effective administration.

While disclosure of the project's technical requirements are limited, in a publication Botswana Police Services (BPS) revealed that the surveillance network will be of "international standards" including "high definition cameras" and "intelligent lenses'', this may suggest that the system infrastructure support AI surveillance capabilities (Ramaphane, 2017). In addition, the surveillance cameras are cross-sectional and at "strategic corporate enclaves of high economic value". In addition, the system would also incorporate "software packages and monitoring computers with secured databases and other world-class security surveillance tools used globally in leading international cities" are also reportedly included in the project (Swart & Munoriyarwa, 2020, p. 39).

BPS Senior Superintendent Near Bagali issued a press release stating that the CCTV surveillance cameras would allow the police force to track city activities in real-time and that the systems would be operated from a centralised location. In an effort to minimise road injuries and fatalities, CCTV surveillance cameras have also been mounted at traffic intersections to arrest traffic offenders. In criminal inquiries, they will also assist in arresting motorists who vandalize traffic lights and "provide evidence of pedestrians, motorists and road infrastructure vandalism in cases of hit and run". BPS reported in this press release that some pilot tests were already underway at established locations and that the results showed some positive outcomes (Republic of Botswana, 2018).

Some additional functionalities of the surveillance network deployed in Francistown were identified in a separate publication in June 2019. The CCTV network is revealed to be linked through fibre optic network connected to the command centre established at Kutlwano Police Station and satellite surveillance

vehicles. Gaboletswe Dimeko, BPS Senior Assistant Commissioner, in his interview mentioned that “over 500 cameras inserted with facial recognition features…will be placed in 195 sites around Francistown” (Kebotse, 2019). This would appear to indicate that the government had begun to establish an integrated local data center that would incorporate safety and protection, as well as law enforcement and traffic management. This is likely to have some implications towards how data is classified to organise people and policing activities around prediction and real-time awareness on the ground which might produce flawed outcomes.

3.2.3 Business Model and Funding: Public Private Partnership

In the announcement of the project the construction costs for this project were not stated, other than being a "multi-million Pula" undertaking (Mdalani, 2015), no final figure has been subsequently stated. Following the initial project deployment in the capital city (Gaborone), in addition to the budget there were reports in August 2019 that Huawei collaborated with the City of Francistown (Botswana's second-largest city) to deploy similar systems (RWR Advisory Group, 2019). The Senior Assistant Commissioner of BPS announced that that Huawei Technologies Botswana is in communication with two local companies to implement the Francistown surveillance network, which will cost the city more than BWP 200 million (US$18.4 million) in total (Kebotse, 2019; Mmolawa, 2019).

During the financial year 2020/2021 the Minister of Defence, Justice and Protection requested an additional fee of P77.7 million (USD 7.2 million) from the Parliamentary Committee to be channelled into this project (Nkani, 2020). Although Huawei Technologies Botswana and ICT Dynamix are responsible for the procurement, distribution, activation, setup and commissioning of additional cameras to provide a safer city solution it is not clear if the government would request these private firms to invest in the project by equity or other forms of loans under the PPP business model. It is important to note that while compiling this report, there has never been any official announcement from the City councils of Francistown and Gaborone regarding the completion of this project.

The business model of the "Safe City Project" in Botswana can be assumed to be a form of Public-Private Partnership (PPP). The reason for this rather is not entirely clear because no further documentation both from the government and the above mentioned companies reveal this information. But because of the nature of the stated business model, often times a PPP business model arrangement, the government owns the public service mission, but engages the private sector to construct, renovate, manage and sustain the facilities and in some cases run the operation. In return the private partner is either paid directly or receives some other benefit such as exclusive use of data generated from the infrastructure (Maier, 2015).

The alliance of Huawei with the Botswana government dates back many years ago. Huawei has played an essential role in the advancement of information and communications technology (ICT) infrastructure in Botswana, having been in the ICT infrastructure business since 1998. Botswana Fibre Networks Ltd (BoFiNet), a state-owned corporate entity established by Botswana's parliament in 2012 to support and manage the country's national communications network infrastructure, specifically the countries backbone fiber network, had partnered with Huawei as a major player to develop the countries network infrastructure (Botswana Fibre Networks, 2017, 2018; Churu, 2016).

First declared by President Xi Jinping in 2013, China's Belt and Road Initiative (BRI) aims to extend the Chinese economy by promoting comprehensive trade through Eurasia and Africa (Huaxia, 2019). Publications note an existing official Chinese government report that established the “Digital Silk Road” (DSR) in 2015 as a centrepiece of the Belt and Road Initiative (BRI) (Triolo & Greene, 2020; Yong, 2019). Now that Huawei is classified as a component of the DSR effort, its increasing pervasive influence through its AI surveillance technologies, as well as its grandiose hyperbole around the BRI/DSR has been gaining more global traction. In addition, a total of 40 out of 55 African Union member states have signed a Memorandum of Understanding (MoU) with China on the BRI including the Botswana government to fund its prospects for a modern infrastructure (Dahir, 2019; Dennis, 2021; ENCA, 2016) (Feldstein, 2019b, 2019c). In this sense, these partnerships can also be viewed as alternatives to developing significant institutional endowments in the African region order to achieve public interest results. It identifies innovative AI technologies implemented by private enterprises as an opportunity that can be expanded through public-private partnerships, co-operatives, or other commons efforts (Gillwald, 2020).

The digital Silk Road, which is the result of digital economic integration with the Belt and Road Initiative (BRI), will assist the BRI through digital technology transformation. It can be thus suggested that indirectly China could be funding various "Safe City" initiatives through the BRI to improve security in the beneficiary countries by offering soft, low-interest loans and promoting the participation of Chinese State Owned Enterprises (SOEs) which gives an upper hand to financial support to private companies like Huawei. There are currently no official figures for total investment by Huawei or the Chinese government shared for the Safe City project in Botswana, but a recent report from the China Africa Research Initiative (CARI) at Johns Hopkins University puts a total concessional loan of about $5 billion per year in African countries that have signed the BRI MoU (Hornby & Hancock, 2018; Layton, n.d.). Ultimately these loans provide monetary value needed for national developments but in the long term it could establish new forms of profit-making dominance and threat to sovereignty.

3.3 Background and Context

3.3.1 Benefits: Public Safety

Despite the lack of data on the quantity of CCTV surveillance cameras nationwide deployed by the government. This study can reveal some noticeable developments in two major cities (Gaborone and Botswana) of surveillance technologies, especially at major intersections and in the Central Business District (CBD). Both small and large retailers are also using CCTV monitoring to deter, track, stop and control crime. Private security companies dominate CCTV surveillance in both large and small corporate establishments. This is evidenced by the high prevalence of CCTV monitoring systems deployed in private businesses (banks, retailers, warehouses, etc.). This has also recently been deployed in suburbs and private homes to mitigate social crime, community policing and personal protection (Molepo et al., 2020). The escalation of crime in the society and illegal activities such as burglaries, and theft typically has had an impact towards the need to transform government policing strategies.

Orthodox police tactics, such as neighbourhood watch or foot patrols that used to be effective now have little effect in reducing societal crimes even in developed countries (Goold, 2004). This has pushed many countries to revamp their policing methods using sophisticated technologies to keep up with high crime rates. For example, the United Kingdom's capital London uses Closed Circuit Television (CCTV) surveillance technology, to make it the most-surveiled cities globally (IFSEC Global, 2020).

Crimes such as smashing-and-grabbing, snatching, traffic law and administrative breaches have been reported as the most prevalent illegal practices in the Botswana (Overseas Security Advisory Council, 2020; Statistics Botswana, 2018). These opportunistic criminal activities require continuous monitoring, which is not always feasible. To counter this challenge, President Mokgweetsi Masisi announced during his 2020 State of the Nation Address that:

> "The Government has deployed cutting-edge crime-fighting technology geared towards enhancing police capabilities. In particular, the Closed Circuit Television (CCTV) surveillance system deployed in Gaborone… [lead to a decrease in criminal activities] 4.4% in violent and intrusive crimes from 7,629 to 7,295 and a decline of 4.7% in serious crimes from 5,566 to 5,304 reported cases in 2019 against 2018" (Republic of Botswana, 2020, p. 65).

Although crimes seem to have decreased there is no independent data to verify a decrease of crime or more significantly the cause of any decrease. There is no public data that we know of that the reduction of crime is due to deterrence or to more effective policing through identification and prosecution of crimes.

3.3.2 Surveillance Landscape

According to the British Security Industry Association (BSIA), the government in the United Kingdom has around 4 million CCTV cameras. By comparison, in the United States it is believed that there are more than 70 million installed in the country (BBC News, 2015; Ivanova, 2019). Despite this prevalence of surveillance cameras used in monitoring people in developed nations like United Kingdom and United States, in Botswana this remains a nascent sector.

While surveillance systems have always been widely used in domestic or in-home security, commercial and industrial applications for some time in Botswana, the deployment of large-scale CCTV surveillance started in the mining industry back in the 2000s. With the first the first and largest surveillance project established in the diamond mine of Debswana (Booyens, 2013), to mitigate diamond and equipment theft and to ensure safety risks in and around the process plant. While the growing network of CCTV systems used by private security companies began gaining traction and developing a market niche in the country, in 2019 more domestic and international companies penetrated the marked to launch new additional CCTV surveillance systems (RADWIN, 2019).

In Botswana's metropolitan cities (Gaborone and Francistown), the deployment and operation of CCTV surveillance cameras are widespread and as in the rest of Africa this issue is topical (Jili, 2020; Ramaphane, 2017). This surveillance network spreads across busy junctions (Kebotse, 2019), in the inner city's main streets and closer to private residences. There is no publicly available data suggested supported public investment initiative has benefited businesses or residents.

Although the presumption may be that Botswana's economic status has always enabled it to perform hidden surveillance operations, it is assumed that global technology companies have succeeded in importing other forms of surveillance-driven tools in the past. For example, Citizen Lab reported in December 2020 that Botswana had deployed a surveillance software technology produced by cyber espionage firm Circles (Marczak et al., 2020).

Other investigative reports indicate that former President Ian Khama had secured state-of-the-art surveillance equipment with spying capabilities on the internet and telephone from Israeli companies in the run-up to the 2014 general election (Sunday Standard, 2018). Secret documents revealed that FinSpy Mobile and FinSpy PC were installed by Directorate of Intelligence and Security Services (DISS) to monitor political opponents including members of opposition parties, journalists and citizens criticising the government in February 2015. In addition, the documents revealed that DISS had spent USD 64.7 million on a German company for surveillance equipment (Botswana Guardian, 2015).

3.3.3 Private sector surveillance

As much as a concern as the deployment of surveillance tools in Botswana is the lack of transparency by private companies doing business with government and also oversight mechanisms that are non-existing. There is no code of practice in place for the operationalisation of CCTV surveillance in public space. Facial recognition technology is being deployed without guidelines reconciling the imperatives of public safety and protection with the fundamental rights to personal privacy.

The 2018 Data Protection (DPA) Act is not yet in force. Achieving a balance between rights and compliance mechanisms with data privacy regulations is necessary yet balance will be difficult to maintain. In cooperation with the Parliamentary Security Committee, the Communications Regulator (BOCRA) should propose and establish effective CCTV mass surveillance legislation and implement a set of law-compliant norms and standards to avoid these possible risks and harms.

CCTV surveillance can be a valuable tool for providing public safety and protection, and public crime investigation. As a mechanism for mass surveillance, however, these systems are vulnerable to misuse by states and technology companies. The resulting power dynamics primarily threaten 'privacy' that is privacy of people vis a vis power actor such as the state or corporations. Such systems can also affect privacy from one's peers. For example, a policeman with access to an urban CCTV system could use it to monitor a former romantic partner. However, computer vision surveillance raises privacy concerns only because of that individual's position in relationship to the hierarchy instantiated by computer vision powered network.

3.4 Analysis

3.4.1 Constitutional and Legislative Framework

The Constitution of Botswana, , refers to privacy twice. Section 3 sets out the importance of fundamental rights of individuals, including in s3 (c) protection for the privacy of his or her home and other property"". Fundamental rights are subject to limitations required by the rights and freedoms of others and the public interest. Section 9", entitled 'Protection for privacy of home and other property' articulates the right to privacy" in s9(1) "Except with his or her own consent, no person shall be subjected to the search of his or her person or his or her property or the entry by others on his or her premises." The right does not explicitly extend beyond the specific prohibition on search. However the right to privacy has been interpreted as extending beyond the specifics of s9(1), and thus international human rights and comparative constitutional law should inform its interpretation (Balule & Otlhogile, 2016). It is thus an open

constitutional question whether mass public surveillance through computer vision enabled networks is permissible in Botswana.

Section 9(2) of the Constitution permits limitation of the right to privacy for certain interests including “defence, public safety, public order, public morality, public health, town and country planning”, however the limitation must be in terms of a law, legitimately for a purpose listed in s9(2) and reasonably justifiable in a democratic society. As a consequence, while mass public surveillance may be constitutional it depends largely on the uses to which it is put, the extent to which the incursion is justified by the purpose and safeguards to prevent abuse. Unfortunately, beyond references to prevention of crime the authorities have not been forthcoming about the purpose and efficacy of the network and what safeguards, if any, are in place to protect privacy.

Botswana has invested in increasing cyber resilience and fostering multi-stakeholder approaches to cyberspace governance in the region, including through public education campaigns. By the end of 2019, Botswana established its national cyber policy strategy and is still at a drafting stage of developing a cybersecurity bill (Calandro & Berglund, 2019).

The enactment of the Electronic Communications and Transactions Act [Act 14 of 2014] is primarily significant in terms of facilitating e-commerce in Botswana, mainly because it grants legal recognition and legitimacy to electronic communications and transactions. Section 5 of the Act indicates that unless proven otherwise, an electronic record is assumed to accurately replicate the contents of the original record. It supports the assumption that a computer system used was operating properly at all material times and that that electronic record systems are accurate and therefore legitimate. It allows the Communications Regulator, BOCRA, to assist in giving evidence before a Judge.

The Electronic Records (Evidence) Act 2014 provides for the admissibility of electronic records as evidence in legal proceedings and authentication of digital records. Despite being broad, this Act does not specifically address the issue of CCTV surveillance information which can also be used in a legal proceeding. The definition of "electronic record" is "data that is recorded or stored in any medium in or by a computer system or other similar devices and the can be read or perceived by a person or computer system or other similar devices and includes a printout or other output of that data". This is highly likely to be interpreted as including data from a smart camera.

3.4.2 Data Protection

The Botswana Parliament adopted the Data Protection Act (*Data Protection Act (Pendlex)*, 2018). but it has not been implemented yet (BOCRA, 2018). Although Section 14 specifies that personal data should be protected by fair security protections against risks such as loss, unauthorised access, damage, usage, alteration, or disclosure. It does not explicitly specify any data related to surveillance footage and does not provide any exceptions to police activities. The Data Protection provides comprehensive clauses for state functions, but with limited exemptions. It establishes an Information and Data Protection Commission, with a Commissioner and Deputy Commissioner. The independence of the Commission is limited by the ability of the Minister to give general or specific directions consistent with the Act (Greenleaf & Cottier, 2020).

The public deserves to be notified about CCTV surveillance in public areas and government should be explicit when warning citizens about surveillance activities (Blackhall Publishing, n.d.). 87% of roadside CCTV cameras in Gaborone did not have warning labels, while 13% had warning labels (Molepo et al., 2020). While observing some of the CCTV surveillance cameras deployed, the researchers found out that most cameras had warning signs written in Setswana as follows: "TLHAGISO! Re Ntse Re Go Lebile" and accompanied by the English translation "ALERT! We Are Watching You".

It seems that data is collected, transmitted, and stored in the designated data centre but there is no public disclosure of how user data is being processed. Considering the geographical placement of the surveillance cameras, there is a lack of control and measures addressing sensitivities surrounding individual privacy and vulnerable groups such as children, while balancing public safety and protection (Molepo et al., 2020). The DPA emphasises that "any operation or a set of operations which is taken in regard to personal data, whether or not it occurs by automatic"...means, "processing should be construed accordingly" (BOCRA, 2018).

AI-driven technologies including the CCTV surveillance network, puts privacy into the spotlight as a national public policy issue. The constitutional right to privacy is discussed in the next section. Surveillance and interception of private communication is provided for under the Intelligence and Security Service Act 2007 (ISSA). Section 22 (1) states that:

> "Where the Director-General believes, on reasonable grounds, that a warrant under this section is required to enable the Directorate to investigate any threat to national security or to

perform any of its functions under this Act, the Director-General shall apply to a senior magistrate or judge of the High Court for a warrant in accordance with this section…"

However, the analysis of the ISSA private communications interception authority reveals inadequacies in the law which does not comply with the principle of proportionality. It does not offer effective private communications interception monitoring and control mechanisms and therefore does not guarantee that interception is the least intrusive and proportionate to the security of interest. Even the ISSA only authorises the Security Services to engage in interception, the police and other authorities are not authorised.

However, the lack of law enforcement by the information regulator since its authorising legislation is not yet in force leaves citizen data exposed and their right to privacy vulnerable to abuse. Now the broader question is: 'how will the Data Commissioner comply with Section 32 of the Act, which allows exemptions from legislation to regulate under the Act for processing of data for national security or public interest purposes? Will exemptions for collecting data for public interest purposes constrain oversight institutions? For instance, will regulation provide the Commissioner with clarification as to when such exemptions may or may not be appropriate? And is the Commissioner going to be forced to act accordingly?

Despite the above laws, there is no general law that regulates surveillance by law enforcement agencies of private communications. Specific gaps in legislation in respect of AI enabled surveillance include transparency and accountability concerning the retention and disclosure to authorities and third parties of user information from surveillance activities.

3.4.3 Human Rights

Botswana is bound by several international, continental and regional instruments, such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and Peoples' Rights (ACHPR), which guarantee freedom of expression, the right to privacy and the right to information (Government of Botswana, 2018).

The African Convention on Cyber Security and Personal Data Protection of 2014 also known as the Malabo Convention imposes obligations on signatories to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime (African Union, 2020). Botswana is not a signatory to the convention,[2] however the Convention establish the basic normative framework for the continent. As discussed earlier the right to privacy in can only be limited to protect other rights and be reasonably justifiable in a democratic society founded on individual dignity, equality and freedom is fair and

[2] See African Union Convention on Cyber Security and Personal Data Protection for status list: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

justifiable (Fombad, 2004). The Universal Declaration of Human Rights test of proportionality demands that all legislation concerning human rights must be proportionate or reasonable (Brown, 2016).

Some interpretations of Section 9(1) understand it as encompassing 'informational autonomy' (Balule & Otlhogile, 2016). Informational autonomy may extend to a right against unjustified surveillance in public places. The UN's Guiding Principles on Business and Human Rights implement the 'Protect, Respect and Redress' structure and emphasises corporate responsibility. Private businesses have a responsibility to uphold human rights, and where people's rights have been infringed, the person must have access to a remedy (Ruggie, 2009, p. 282). While these are guidelines are not binding, they can be used to benchmark the extent to which privacy is protected in Botswana by businesses. Controlling crime and policing strategies geared towards maintaining public order through mass surveillance have the potential to violate the right to privacy. In the absence of appropriate justification by the state, including transparency and public oversight it seems likely that using AI surveillance technologies will be judges as not proportionate with the Botswana Constitution.

3.4.4 Potential Harms

While there are advantages of deploying CCTV surveillance networks by technology companies are said to be capacities to "predict, prevent, and reduce crime" and "address new and emerging threats" (Huawei, 2016). Potential harms can be associated with collecting and storing surveillance data, including its manipulation by state security for nefarious agenda towards citizens (Feldstein, 2019) or non-citizens. Data-driven surveillance tools which are increasingly networked, like smart CCTV surveillance systems are often exposed to vulnerabilities. This involves manipulating the systems —resulting in stealing, deletion or loss of vast amounts of data.

Facial recognition technologies are often marketed through claims of monitoring and the deterrent impact of surveillance that purportedly decreases crime rates. This is focused on the mantra that states subsequently lower crimes in the community while reducing policing costs and resource consumption. In order to ensure that CCTV monitoring does not open up a scramble for benefit while unfairly interfering with fundamental human rights, such as the right to privacy, this motivation must be factored into impact evaluations of surveillance technologies against such rhetoric.

With no laws governing access to and use of database that stores captured images from facial recognition cameras. How the state use data gathered, duration towards its storage, and whether state security has access to the central database — are obscured issues and may differ according to the approach of jurisdiction. The government is likely to face more litigations in the future if state security pays no

regards to constitutional means by accessing personal data illegally. In comparison, a magistrate or judge is the only designated person who may issue a warrant under Section 22 of ISSA to gain access to personal data. Accordingly, the deployment of CCTV surveillance technologies needs rigorous measures, for example, to alleviate both cyber threats and malicious use of data by government security forces, foreign state actors or technology companies.

Given the limited technological skilled workforce and knowledge of the government managing the CCTV surveillance network in terms of operational capacity, it seems likely that Botswana must rely upon much of its capabilities on foreign suppliers in some instances (RWR Advisory Group, 2019). The potential harms of computer vision surveillance specifically in Botswana include non-transparent data gathering processes and cross-border transfers. Huawei supplies the surveillance technology underpinning CCTV surveillance deployment, so how data governance and data processing is being addressed demands clarity on both the government and Huawei.

The few public pronouncements by the government of Botswana and Huawei do not acknowledge that there is an important human rights dimension to discussions around AI surveillance. The depth of subsequent public engagement in the human rights framework and its application to AI surveillance varies considerably. Indeed, in most cases where human rights and data privacy issues are referenced, this is a passing mention, or simply a nod to the government's general commitment to human rights, with little or no further discussion of potential harms as a result of mass surveillance. While this reality is more nuanced, the fact remains that personal data forms part of the connected centralized networks, and the government has more opportunity to exploit AI surveillance networks by potentially profiling citizens to achieve a malicious objective.

Despite the significant coverage given to China and its digital technology engagements in Africa, there has been more concrete evidence of their investments in the surveillance technology sector (Andersen, 2020; Gagliardone, 2021). Against this rhetorical analysis, evidence revealed that Chinese corporations such as Huawei are at the forefront of constructing global national surveillance systems and exporting them to countries where democratic systems are unstable or non-existent, like in most African countries (Feldstein, 2019a). Other observations would seem to suggest that from the standpoint of Chinese companies, branding their global expansion in the digital technology as part of the DSR even in the absence of Chinese government support has been their go-to market strategy – similar to embracing 'political correctness'.

3.4.5 Public-Private Dimension

In 2018, in collaboration with the Chinese technology giant, Huawei, and the Botswana government launched one of the largest state-led CCTV surveillance initiatives, the "Safe City Project" driven primarily by public bodies (e.g. city councils and Botswana Police Service). A tender for Botswana Police Services (BPS) was approved by the Public Procurement and Asset Disposal Board (PPADB) to directly appoint Huawei Technologies Botswana (a subsidiary of technology giant Huawei) and its local partner company, ICT Dynamix, to supply, deliver, install, configure and implement additional CCTV cameras for a safer city solution.

The proliferation of AI-powered surveillance networks in public spaces is a regional phenomenon, and Botswana is no exception to these issues (Feldstein, 2019; Kwet, 2019; Olander, 2019). With African governments increasingly depending on private companies to assist them with mass surveillance, this study emphasizes the growing power of this technology companies as well as the need to develop a system of accountability to curb mass surveillance and data collection. According to civil society organisations, these surveillance systems reinforce the robustness of authoritarian regimes, trigger anticipatory shift in people's actions in favour of the government's roles, and severely compromise human rights (Woodhams, 2020), ultimately increasing a dystopian state of surveillance likely to erode citizens' privacy rights (CIPESA, 2019).

As discussed in 3.2.3 due to the relatively obscure nature of the deployments and the plethora of players involved in deploying computer vision technologies estimating the number of existing CCTV systems in Botswana remains unclear. The expansion of CCTV surveillance systems in the country should be accompanied by legal standards. Globally the legal requirements needed to perform surveillance lawfully are generally high, and even governments with mature data protection laws struggle to comply with them. However, despite these comparable efforts Botswana has either not completed or ratified its Data Protection Act (DPA), with the remaining AI strategies lacking entirely, which potentially may empower other systems of repression in the future (Jili, 2020).

This two-year MoU between Huawei and Botswana Police Service (BPS) in 2017 to deploy CCTV surveillance cameras present a solid formal plan where surveillance provisions are shifted from the public to the private sector in the form of public-private collaboration. Police Commissioner Keabetswe Makgophe stated that the project would help provide efficient policing services through the use of surveillance cameras (Ramaphane, 2017). Public-private collaborations can be used to adopt governance structures for new disruptive technologies that ultimately compromise ethics and governance requirements that might otherwise be binding.

If the Botswana government and Huawei consider the B2B business model effective in their partnership, the long-term priorities may be compromised leading to increased public and private capacity to use data intensive computation , enhanced machine learning and algorithmic usability, and advanced data processing. Notwithstanding the key issues emerging from this business model which relates to data privacy and security: whether Huawei's dominance in the global surveillance technology sector continues to grow or not.

3.4.6 Social-Political-Economic Contestation

The reach of public-private collaboration between Botswana government and Huawei may be compounded by skwed international market competition, an issue of trade rather than national competition regulation . Private firms like Huawei have rapidly expanded into the African market with the competitive advantage of China's unwavering support for its state-owned enterprises (SOEs). The PPDAB when it announces the award of the contract to Huawei, they did not publicly specify the procurement process that had been followed. This demonstrates the power dynamics of big tech companies at play backed by state support (China). For Botswana, the total public expenditure for this project is not yet publicly known. And the consequence of this obscured monopolistic arrangement might be a long-term commitment to pay for the supply, maintenance and rental costs of CCTV surveillance systems which gives a profit-making advantage to Huawei in the long term.

Given the commitment of several African governments, including Botswana, building so-called "Smart/Safe Cities" and Huawei's dominance in supplying facial recognition technologies. The private sector's role in importing and deploying surveillance technology and government role as a consumer needs to be closely monitored and regulated by the communications regulator. Beyond fostering socio-economic growth through partnerships, Huawei's global dominance and more significantly political influence versus the West (Feldstein, 2019, p. 8; Kwet, 2019).

However, deploying surveillance technologies for profit by technology companies must be contrasted with how the profit-motive impacts the ethics of new digital technologies. This technological financing and extension processes are part of the persuasion to consider 'outsource' policing services to private companies by the state (Molomo & Maundeni, 2015). Extending this operation in a highly business-driven and competitive environment may raise difficulties in enforcing the Data Protection (DPA) Act 2018. Although the justification for adopting surveillance technologies is based on crime reduction and maintaining public safety (Republic of Botswana, 2018), the often-muted benefit incentive may be a significant rights concern that calls for oversight to avoid unnecessary and unjustified mass surveillance of people.

The notion that CCTV surveillance networks will help deter crime and maintain public safety is not supported by empirical data, bringing into question the government claims about the effectiveness of the technology and the necessity of deploying the system without internal capacity to manage the network. In promoting law enforcement and policing strategies, the use of facial recognition in public areas may be necessary. Some of these tools have tracking capabilities such as identification of license plates, predictive policing and facial recognition.

These can intensify the risk of hacking private personal information, thus harming the reputation and appearance of the subjects of that information (Crawford et al., 2019). Due to the lack of substantive stakeholder engagement in the launch of the “Safe City Project” and deploying CCTV surveillance cameras in Botswana are likely to expose people to political surveillance, violating human rights and political freedom. Critics point to previous political surveillance and oppression violating human rights and freedom of expression as making surveillance more likely (Botswana Guardian, 2015; Kanono, 2020).

3.5 Botswana Case Study Conclusion

The evidence from this study, the government of Botswana supports the deployment of CCTV surveillance technology and its benefits in the Safe City project as a means of improving the effectiveness of policing activities and combating criminal elements. While the government sees benefits of this technological capabilities, they have attributed a decline in crime rates to the use of CCTV cameras, but there is still a dearth of data to prove if computer vision surveillance systems serve their purpose or are worth the investment in the country.

Our study uncovered the existence of the Data Protection Act in Botswana, while currently on notice and pending implementation, it aims to govern, protection of personal information and secure individuals' privacy in regard to their personal data. There are currently no regulations in place to govern the usage of computer vision systems. The report suggests that the Botswana government invest in developing its national AI policy, which focuses on model frameworks for data governance, privacy, and security, that incorporates ethical use of computer vision technologies by both private firms and the state.

Given the government of Botswana's lack of clarity on whether it will take ownership of the "Safe City" project or hand it over to another private entity once it is fully launched. The terms of processing video surveillance data, managing its data command centres, and who has access to this data under what jurisdiction, as well as general technical maintenance of the entire CCTV network remains unclear. Therefore, we believe the state is underequipped for this endeavour due to a lack of a qualified local workforce in the AI area. Botswana is ranked 33.3rd out of 121 in the 2020 AI governance readiness assessment. This

reflects the country's incapacity to adopt AI technology to facilitate digital transformation. While recently the government of Botswana is starting to recognize the potential of AI, the President has been pushing for the 4IR program forward, using the capabilities of AI and digital technology inside various government organizations institutions. Also, various institutions have started debates around AI and exploring possibilities where it may help drive the country towards the fourth industrial revolution (4IR).

We confirmed in this report that the right to privacy in Botswana is guaranteed under Section 9 (1) of the Constitution, and while it is not absolute, there is a limitation under Section 9 (2). Despite these limitations, we believe the government should emphasise that any infringement with the personal privacy caused by the use of AI technologies should be governed by the overriding criteria of legitimacy, need, and fairness. Our findings support the necessity for a human-rights-based approach in the development of all AI surveillance technologies, therefore private companies developing these tools need to outline the steps followed to achieve it (including human rights by design and human rights impact assessments) prior to launching their technologies.

The findings of this study indicate to the potential harms connected with AI surveillance technologies, associated with collection and processing of surveillance data, as well as its manipulation by state security for malicious agendas directed towards individuals. There are also reasons to be concerned that these sophisticated systems, as well as the unlawful and social profiling techniques may be utilized, leading to abuses of human right.

While these novel violations of privacy are noteworthy: privacy is essential for the enjoyment of a variety of human rights, including freedom of expression and assembly, as well as personal freedom of choice including wider community values and norms.

To avoid falling victim to biases associated to AI surveillance technologies, it is necessary to investigate how current discourses, such as human rights legislation, privacy laws, and research ethics, connect to various AI surveillance deployments and approaches.

The goal of this case study was to assess the governance of computer vision technologies that use CCTV in public spaces as a feature of the “Safe City Project” driven by the government of Botswana in partnership with Huawei and ICT Dynamics. This study raised a number of questions about facial recognition. To begin, only a few rules regulate access to and use of image databases (repositories that store captured images from CCTV surveillance cameras). How the government of Botswana uses this data, how long images are kept, and where authorities acquire such images in the first place are all murky issues that differ by jurisdiction. This study recommends additional scholarly research to assess and analyse the efficacy

of facial recognition technology in Botswana for crime reduction and then map out systems that guarantee public safety and privacy.

The use of facial recognition technology is projected to continue to expand especially in the field of public spatial surveillance. It is also likely that in Botswana either without as is currently the case or with weak data protection laws, in future, could become a testing ground for emerging surveillance technologies. There is currently no law in Botswana explicitly regulating CCTV surveillance nor mechanisms to inspect the algorithms used for facial recognition purposes nor restrictions on technology companies attempting to gather surveillance data for commercial benefit. Botswana should consider a co-regulation model that draws on private sector expertise to create good practice models for the use of facial recognition technology as a form of public and mass surveillance, considering the concentration of skills and experience in the private sector.

Botswana’s information regulator must urgently develop standards to regulate the use of CCTV surveillance, with critical analysis on facial recognition, and inform these policies with comprehensive study. Regulating both facial recognition and AI analysis is best way to meet the concerns set out. An efficient way to do so would be to add these regulations to the current data protection regulatory regime, and to strengthen the data regulator to ensure compliance.

In this study we have raised the complexity and size of the problem related to CCTV surveillance usage in public areas, demonstrating how the industry's lack of legal standards and bias issues in AI systems are interconnected facets of the same problem. In the past, these issues were often studied separately, but new research indicates that they are inextricably linked. By digging deeper into these links, we will find new ways to address imbalances and harms.

Computer vision surveillance technologies violate individual's right to free association and speech. Three principles of international human rights law are important in determining the legality of a specific surveillance action when instituted by government. Botswana’s legal provisions should not be vague or overbroad allowing the government unrestricted discretion. The legal system itself should be open to the public, transparent and legal rulings should be non-discriminatory.

Based on the developments discussed, if African policymakers and people ignore the developing situation, then a techno-dystopian future is possible. Digital authoritarianism is on the increase, both in Africa and beyond. To protect human rights and precarious experiments in democracy, protecting data privacy and internet freedom against these novel modes of surveillance is fundamental(Shahbaz, 2018). The underlying regimes on surveillance might be lacking; also potential harms of AI built on top of surveillance practices cannot guarantee mitigation for the existing risks. Consequently, even ethical or well-governed

AI practices can have negative consequences. Data protection laws and regulatory standards for accountability and transparency, may be able to mitigate some of the worst known privacy violations today, but as AI technology becomes more advanced and spreads into other fields, more work is required to protect human rights.

4. Case Study 2: Automated Surveillance in South Africa

4.1 Introduction

In the metropolitan areas of South Africa, streets and highways are lined up with (CCTV) surveillance cameras including both private and public spaces which has grown as a significant and mainstream issue currently (Kwet, 2019a). Usually, these CCTV security cameras are mounted on roads, shopping malls, offices, mass transportation hubs, and in private residences.

The South African CCTV surveillance market began gaining traction in the late 1970s particularly in the mining industry (diamond mines and gold refineries) to deter illegal activities (Minnaar, 2012). Around the 1990s and early 2000s, CCTV surveillance began to spread to metropoli-tan parts of most cities, including Pretoria, Johannesburg, Cape Town, and Durban, where both small and major establishments (banks, stores etc) purportedly deployed CCTV to prevent, detect, and manage crime (Minnaar, 2012, p. 103). Around 2010 when South Africa hosted the World Cup football tournament, emerging public security issues brought opportunities and justification on why the deployment of state-driven CCTV surveillance networks on the country's highways, sports amenities and large shopping centres (Hosken, 2008). These developments continue to grow and now this has recently extended to suburbs and private households for the reduction of social crime, community protection and personal protection.

Despite the relatively large number of technology and private companies involved, it remains unclear as to what the exact numbers of existing CCTV systems in the country are. However, it is evident that CCTV deployment is gaining traction and is expanding on the basis of the assumption that it is successful in preventing and deterring crime. According to the Private Protection Industry Regulatory Authority (PSIRA), CCTV surveillance is the third most sought-after security tool of private security companies with 55.8% of customers (PSiRA, 2019, p. 12).

The deployment of CCTV cameras is not currently explicitly regulated in South Africa although some laws do bear on the practise. There is no code of conduct for surveillance activities in place. The Western Cape plans to become the first province to enact legislation to restrict the use of CCTV cameras in public and private spaces (Adams, 2020). To date, CCTV monitoring has been developed without specific guidance

for how to reconcile public safety and protection imperatives with constitutional rights to privacy, except ambiguous disclaimers. Also highlighting the compliance with privacy regulations, including the Protection of Personal Information (POPI) Act of 2013 that recently came into full force. The Information Regulator (South Africa) will have to resolve the lack of specific CCTV mass surveillance legislation and introduce a set of norms and standards with the goal to safeguard privacy and human rights.

The study demonstrates how modern surveillance technologies deployed by tech companies like Vumacam and Hikvision and the South African government are controlling and tracking citizens. The first section discusses the variety of computer vision networks in South Africa operated by both private operators and government in two large cities: Cape Town and Johannesburg. The purpose, financing, technology and deployment are discussed in respect of each section. The next section discusses the implications of human and fundamental rights for these computer vision surveillance networks. It then delineates the readiness and governance challenges, risks and harms, and the inequality and exclusion issues. It then examines the public-partnership dimensions of one of the networks.

4.2 Defining the Case Study

4.2.1 Private Networks

Privately Funded CCTV Surveillance Networks in Cape Town

A total of 513 private CCTV surveillance cameras were recorded within the City of Cape Town at the end of 2018 (City of Cape Town, 2016; Swart, 2018c), all apparently in accordance with bylaws. However, the provincial government has confirmed that it does not integrate privately owned CCTV networks into its public surveillance structure. Through correspondence with the city official, the Media and Democracy report confirms that the CCTV surveillance network does not have analytical capability, such as facial recognition or some other type of biometric identification. It relies solely on human operators to translate data they receive (Swart & Munoriyarwa, 2020).

While much of Cape Town's middle-to-high-income communities have location specific CCTV surveillance LPR cameras mounted at major convergences and are monitored from control hubs in neighbourhoods. These more prosperous neighbourhoods funded their entire CCTV surveillance system deployment through private donations from residents. In an interview with a representative of the Cape Town LPR User Group, they confirmed that numerous sub-networks are linked to each other, and it is possible for several control rooms to synchronise data with each other (Observatory Improvement District, 2019; Technews Publishing (Pty) Ltd, 2016). A large portion of the infrastructure is cloud-based and can be reached in real time from different forms of computing devices connecting to the Internet, including

laptops and mobile phones. This network was built up by a South African corporation named iTrack (News24, 2015b) .

There is presently no provincial legislation in effect to regulate private CCTV surveillance networks and the data is regulated, processed and handled mainly by private neighbourhood organizations (Adams, 2020). Data is exchanged with law enforcement agencies and private security firms for the reduction of violent crimes.

There is a lack of public information on the magnitude and types of equipment being used to support surveillance in Cape Town in this case study. However, open-source information available indicates that the May 2015 press release on the Hikvision website claimed that 42 day/night Hikvision CCTV surveillance cameras were mounted in the Sea Point suburb of Cape Town (Hikvision, n.d.). In October 2018, a CCTV expert who was interested in the construction of the first CCTV installations in Cape Town also told researchers from Media and Democracy that the initial Cape Town infrastructure had been installed with Geutebrück cameras, a German security CCTV camera maker (Swart & Munoriyarwa, 2020, p. 48).

Privately Funded Surveillance Projects in Johannesburg: Vumacam

Residents of a wealthy Johannesburg neighbourhood, Parkhurst in 2015, financed a private initiative to deploy fibre-to-home broadband internet into their community with the explicit goal of providing CCTV surveillance only feasible through high-speed connectivity (vpro documentary, 2015). At the time, Vumatel, a fibre network provider, said that the data collected through the CCTV surveillance cameras would be forwarded to the data centre which would be controlled remotely. Features such as number plate recognition and facial recognition technology are included along with the cameras. Plans have also been created to mount CCTV cameras powered through GPS technology, infrared and heat source cameras to map accidents and so-called suspicious movements (Kwet, 2017) .

Vumacam, a Vumatel division specialising solely on high-definition video surveillance, declared its plan to build 15,000 high-definition surveillance cameras in February 2019. This was rendered possible by the fact that the Johannesburg region had an adequate fiber Internet infrastructure in place with a video feed capability (Intelligent Surveillance and Detection Systems (Pty) Ltd (ISDS), 2013; Kwet, 2019a; Vumacam, 2021). At a press conference held in February 2019, Vumacam informed reporters that their cameras will not support analytics for facial recognition, as this feature was only in the development phase and was not ready to be utilized (Vumacam, 2019a).

Vumacam said the cameras would be produced and assembled by China's state-owned Hikvision at the same press conference. Presumably, Hikvision and Vumacam have an exceptional partnership, especially

that Hikvision had promised to design CCTV camera equipment particularly as per Vumacam's needs. Despite the fact that Hikvision has a strong presence in the private security sector and launched a branch in South Africa in 2015, the Vumacam deal was the first large-scale implementation of its type in South Africa. Vumacam aims to extend the network to other cities of South Africa in the future (Swart, 2018b, 2019b).

> "Our friendship, our relationship is a very close one; they actually develop stuff for us. We've got a new camera that they are creating for us specifically that is a dual-lens camera, so we've got very close relationships with them." (Swart, 2019a, 2019b)

Hikvision has a controversial history in cybersecurity, including accusations that their CCTV cameras have a back door built in them. They have not made any efforts to inform their customers about such design features, nor have they issued updates to fix them. There are concerns that their cameras may be compromised easily. However, Vumacam said it had checked these 'technological errors' of Hikvision equipment to warrant they could not be compromised when questioned about the reliability of their network (Swart, 2019a).

4.2.2 Funding and Business Model

Vumacam is owned by Vumatel a fibre company in South Africa. Vumatel builds and services fibre but is not an ISP. Vumacam is a CCTV service that provides video feeds for a monthly fee (My Broadband, 2019). As with much IP-based TV or streaming services Vumacam's services rely on high bandwidth, high quality/latency connections, particularly on fibre. Vumacam's CCTV network is fibre-based and often uses the Vumatel fibre network which is operated by Vumatel, its parent company of Vumacam (My Broadband, 2019). Vumacam provides CCTV feeds, as well as value added services described in (My Broadband, 2019) as "intelligent services" such as license plate recognition. with much IP TV, especially Fibre roll-out.

Vumatel was established by Johan Pretorius, Neil Schoeman and Richard Came in 2014 (CrunchBase, n.d.). On the 14th of February 2019 it was reported that Vumacam is a joint venture between Vumatel (the fibre company) and Imfezeko Holdings with Vumacam holding 51% and Imfezeko holdings holding 49% (McCleod, 2019). Imfezeko Holdings was established in 2006 by the family of the Ricky Croock, the CEO of Vumacam (Kwet, 2019a)

Vumatel has received funding from:

- Venture Capital funding from Investec (2015).
- Vantage Capital through a debt funding round in 2016

- Community Investment Venture Holdings through a private equity funding round in 2018 (Crunchase, n.d.).

The Vumacam CCTV surveillance network generates revenue from city indwellers. Vumacam's video feed has been leased by Residents' Associations for R730 a month per camera and the cameras are owned by Vumacam (Mungadze, 2019). Residents' groups employ private security companies as contractors to monitor the video streams from local control rooms. Only the video feed from the neighbourhood they are monitoring can be surveilled by security personnel (Swart, 2018c). According to the Vumacam web-site, their CCTV cameras support license plate recognition (LPR). The license plate of a car travelling within range of a camera is collected and contrasted to a repository of checked “Vehicles of Interest” (VOI), whether or not it is on a list of suspected vehicles. The database provides records on missing cars, forged license plates, and wanted suspects by the South African Police Services. The cameras are said to register about 500 registration numbers every minute on average (PWP Neighbourhood Watch, 2015; Rangongo, 2019; Vumacam, 2021)

4.2.3 Technology

Vumacam’s parent company, Vumatel is a fibre company that lays fibre optic networks to homes throughout South Africa. Vumacam provides high definition CCTV feeds, as well as value added services described in (My Broadband, 2019; C. Wilson, 2019) as “intelligent services” such as license plate recognition. Vumacam was announced as a service by Vumatel in 2009 (My Broadband, 2019). The company has so far only provided its services in Johannesburg, but in 2019, money was set aside for expansion (My Broadband, 2019). In February 2019 Vumacam announced plans to deploy 15 000 cameras in the Johannesburg area (C. Wilson, 2019).

At the time it was estimated that the video traffic would be around 30 petabytes per month, but that this would however not affect the bandwidth of the Vumatel network. Vumacam reports that its cameras have a 96% “uptime”, 24 hours a day, 7 days a week. The CCTV cameras have night and daylight vision capability and can store data for around 14 days. The data is uncompressed, and according to Vumacam's most recent comments, the cameras produce about 30 petabytes of data every month. Teraco, a commercial corporation, hosts a third-party data centre where data is processed (Vumacam, 2019b). Vumacam's website reported at the time of writing this report that it had mounted 3032 live CCTV cameras around Johannesburg, covering an area of approximately 500 square kilometres (Vumacam, 2021).

4.2.4 Public Concerns

Interviews with Vumacam Chief Executive Officer, Ricky Crook**,** revealed that 'behavioural recognition, i.e. looking at shapes, speed, direction and movement variations,' was more widely used to offer security companies 'situational awareness.' As cameras pick up 'abnormal' motions by analysing pixel shapes, surveillance patrols may be implemented more efficiently. When asked to elaborate more about the technical operation of their cameras, Vumacam said that its cameras are not actually being used for facial recognition and that such criteria will have to be fulfilled before it could be considered:

> "They [the cameras used by Vumacam] do not have pan, tilt and zoom ability' and 'we think it is an invasion of privacy."

In addition, Vumacam also indicated that before legislation and safeguards are in effect, the firm has no intentions to implement facial recognition capabilities. However, the high-resolution digital cameras used by Vumacam, and other providers are networked. This implies that each of them is given an independent IP address and provides some functionality requiring artificial intelligence (AI) (Matiso, 2020; Newzroom Afrika, 2020). The Vumacam system does claim to check whether vehicles are stolen or have duplicate plates, referred to as 'cloning'. This requires number plate recognition, although Vumacam claim that they don't link this data to personal data such as names and identity documents. The system also includes algorithms that learn that are intended to identify suspicious behaviour such as 'running' or 'angry noise' (Matiso, 2020)

The Protection of Personal Information Act (POPIA) just recently came into partial force, Vumacam has confirmed that it complies with it in its data processing (Boksburg Advertiser, 2020; Business Tech, 2021). It claims to vet every security company that buys access to its data feed and makes them sign an arrangement that these companies will be audited by an impartial third party on a daily basis to ensure conformity to the terms.

In the case of Vumacam, having the right partners—companies that are privacy conscious, who keep themselves accountable and reject any forms of privacy violation—is one of the most crucial considerations in maintaining user privacy that this business partnership should guarantee (Independent Online, 2021). Legal analysts have cautioned, though, that since the Act is enforced, the corporation may at some point find it impossible to defend gathering and producing large vast quantities of personal data without the permission of anyone captured by their cameras (Moubray, 2019; Rabkin, 2019)

4.2.5 Government Sponsored Networks

CCTV Surveillance Networks Funded by Government in Cape Town

Due to the significant increase in crime rates in the inner city of Cape Town between 1995 and 1997 a pilot project consisting of 12 CCTV surveillance camera networks was deployed in the central business district (CBD) of the city in 1998 (Minnaar, 2007). The pilot was a collaborative project between the City of Cape Town and the local private non-governmental company group Business Against Violence and Teleste, a Finnish technology firm, assisted with the supply of CCTV surveillance equipment (City of Cape Town, 2014; hi-tech Security Solution, 2011; Western Cape Government, 2012).

The City of Cape Town municipality eventually funded the whole project for 72 CCTV surveillance cameras to be deployed at approximately R8.5 million, and the entire deployment was finished in 1999. In June 2000, the City of Cape Town assumed charge of the surveillance network. Then the entire system was digitised in 2001 by Teleste. The project was extended further in 2009, with its STM1 ATM network updated to 10 Gb ethernet. Teleste worked to update the device with a subcontracted firm, South Africa's Fibre-Based Integrations (City of Cape Town, 2018; hi-tech Security Solution, 2011; Teleste, 2013).

Today, the surveillance network is responsible for monitoring a vast portion of the nearby suburbs of Cape Town, including the city's highways. Through its two control centres including a main command centre everything is controlled. Video live footage between these hubs can be switched and shared, and each centre can manage the entire monitoring separately. The Metro Police Department's Communicare Control Room in the CBD was the first centre to be instituted. The second control room was then set up at the Transport Management Hub of the city (City of Cape Town, 2018; Smith, 2019). Transport Telematics Africa, a South African corporation, mounted an additional 32 surveillance cameras in the CBD in 2010 (Transport Telematics Africa Pty Ltd, 2010). In a report published by Media and Democracy, it is reported that the city had a total of 1,578 cameras on its whole network by the end of 2018 (Swart & Munoriyarwa, 2020, p. 46).

According to city of Cape Town officials, as reported by Media and Democracy, the City's Interconnected Rapid Transit System (the city's public transport network that comprises MyCiti Bus Routes and Bus Stations) has 713 security cameras. The City's Freeway Management System includes an additional 239 CCTV surveillance cameras used mainly to track traffic on major roads and highways of the city. The network helps the city to transmit succinct messages to "overhead variable signals" along the road to warn road users of collisions, emergencies, construction or unfavorable weather conditions along the road (Swart & Munoriyarwa, 2020).

The CCTV surveillance network managed by the Metro Police Strategic Surveillance Unit is responsible for the detection of violent crimes (City of Cape Town, 2014). Of its 626 CCTV surveillance cameras, approximately 514 have pan, tilt and zoom (PTZ) capability according to cited by Media and Democracy report. In the report, while the researchers were communicating with the city officials, they stated that approximately 514 of these are fitted with both PTZ capabilities and license plate recognition technologies or LPR. PTZ cameras feature a keyboard that enables the user to shift the camera lens up, down or sideways and to concentrate on a certain angle. It is also possible for the camera lens to stay fixed on the moving object (BirdDog, 2019). As long as the object stays within the boundaries of the surveillance network, their movements may be monitored in real-time (Transport Telematics Africa Pty Ltd, 2010).

The license plate recognition device digitally records the identification number of the vehicle. The vehicle and the number plate are photographed, and the optical recognition program helps the device to recognise the identification number of the car on the number plate. The identification number will then be linked to the number plate database. The data is then stored and can be analysed later in order to chart human driving trends retrospectively (Hikvision, n.d.; Observatory Improvement District, 2019).

Identification number plate details can be inserted into the database in order to retrieve the data obtained by the monitoring device for a particular car. This usually involves a collection of images of the front of the car, the position of each camera that captured each picture, and the period each photo was taken. The CCTV network is linked to eNatis, South Africa's Official Electronic National Traffic Management System, which enables network operators to view the personal data of the car owner attached to the vehicle registration code (Department of Transport, 2018). The devices can even be designed to alert the authorities when a suspect car is identified. LPR cameras are also used in roadblocks to flag motorists with unpaid penalties. They are often used to impose speed-over-distance traffic penalties and to catch license plates of cars unlawfully travelling on the city's bus lanes during prohibited hours (Business Tech, 2019; Mzantsi, 2014; Mzekandaba, 2016b).

The Cape Town CCTV surveillance network runs 24 hours a day. The video footage is registered and stored for 30 days and has a storage space of 1.4 petabytes (Swart, 2018b). At the end of 2019, the City of Cape Town agreed to install an extra 44 CCTV surveillance cameras in the subnetwork. The cameras are to be fitted with LPR functionality. This extension was rendered feasible by financial support from districts – regions demarcated by a municipality in which neighbourhoods are served by a dedicated ward councillor (Independent Online, 2019).

Government Funded Surveillance Projects in Johannesburg

The first CCTV surveillance network in the City of Johannesburg was deployed in 1999 in the central business district. Cueincident, a South African based company was then allocated the contract by the city administration to lead the deployment. Established under the Business Against Crime (BAC) Initiative, Cueincident through BAC then partnered with the City of Cape Town to also to establish its first CCTV surveillance network in 1998. In 2004, Cueincident would later set up the first CCTV surveillance network in Pretoria (Czernowalow, 2005; Intelligent Transport Society South Africa, 2008; Larsen, 2006)

In 2008, Omega Risk Solutions, a Mauritian company, was given a tender by the City of Johannesburg to introduce auxiliary CCTV surveillance cameras to the already existing 109-camera network, taking over operations and maintenance from their predecessor Cueincident. Deploying similar surveillance systems in countries like Angola, Ghana, Namibia, Mozambique, Nigeria, Zambia, and Iraq, Omega Risk Solutions has a wide track record of implementing surveillance projects (Business Tech, 2018; Swart, 2018b). After it expired in April 2017, the City of Johannesburg did not renew Omega Risk Solutions' contract. The operation and maintenance of the network and the control centre were instead taken over by the city itself. Following this, there have been news reports that the Johannesburg CCTV system is not fully functional, although the city has denied the allegations (Slabbert, 2017; Swart, 2018a).

The Johannesburg Metropolitan Police Department (JMPD) attached an extra 50 CCTV surveillance cameras to the 450 already in service in its inner-city monitoring network in July 2018. (At least 318 of these 450 have PTZ capabilities. The cameras are alleged to have a wide range of up to 3 km to zoom in and capture accurate images) The City of Johannesburg then indicated that the new cameras will support facial recognition technology and predict movements of objects (an analytical feature through which the software identifies motion that is "suspicious" and then sends an alert to the human operator). The added 50 cameras were said to be able to pivot 360 degrees, disentangling "blind spots'' — spots that fall outside the camera's view. The police spokesman said at the time that the new cameras had a visual range of up to one kilometre, although no specific camera range and resolution details were provided (Business Tech, 2018; Defence Web, 2009; News24, 2015a).

The Johannesburg CCTV surveillance network data is stored at the city’s advanced Intelligence Operations Center of the Region (IIOC). The IIOC is part of the transformation of Johannesburg as a "smart city". The centre was established in May 2019. The IIOC aims to improve the coordination between local emergency and law enforcement services by integrating all municipal data in a centralised location. The network relies on a 900 km fibre-optic network. The city is reported to have invested more than R1.3 billion on its development to benefit its internal communication strategy. The long term goal of this

strategy is to have data from all city-owned agencies channelled into the IIOC data centre which provides for easier integration of resources, including emergency response services and health care services. Subsequently, the JMPD launched a new squad of 80 undercover police officers committed to emergency response to crimes covered by the CCTV surveillance network in May 2019 (Moyo, 2019; Mzekandaba, 2016a).

4.3 Analysis

4.3.1 Right to Privacy and Legal Frameworks for Data Protection in South Africa

The South African Bill of Rights sets out a right to privacy:

> Everyone has the right to privacy, which includes the right not to have
>
> a. their person or home searched;
>
> b. their property searched;
>
> c. their possessions seized; or
>
> d. the privacy of their communications infringed.
>
> (Constitution 103 of 1996, s14)

Although the right to be free of surveillance in public places is not explicitly enumerated the right to privacy is open ended. As a result a court may rule that the right to privacy prohibits general public surveillance. In the case of (*AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others [2021] ZACC 3*, 2021) the Constitutional Court dealt with the right to privacy and surveillance. The court found aspects of the Regulation of Interception of Communications and Provision of Communication Related Information Act to be unconstitutional. That legislation dealt with the interception and monitoring of telecommunications, and this squarely with the right of privacy of communications.

The court ruled on the lawfulness of bulk surveillance of Internet traffic. Bulk surveillance of Internet traffic involves searching almost all Internet traffic for keywords or specific images. The court held that such surveillance is the exercise of a public power. To be lawful the exercise of a public power must have a basis in law, that is a statute, regulation or case should give those engaged in the surveillance a power to do so. The court also held that there is no law authorising bulk communications surveillance, therefore it is invalid and unlawful. The court was unconvinced by comparison with other jurisdictions in which such practises are purportedly lawful.

There are differences between mass visual surveillance in public places through networked cameras and interception of Internet traffic that includes communications. Courts seized with the issue may find that members of the public have a lower expectation of privacy. However, in *AmaBhangane* the court emphasised how the right to privacy in South Africa is informed by a past in which forms of surveillance were deployed to uphold an oppressive state. It is thus suggestive that mass public visual surveillance through networked cameras may be found to be unconstitutional and thus unlawful in South Africa. The question has not however been addressed by the courts.

The Protection of Personal Information Act 2013 regulates the collection and use of 'personal information'. Personal information is defined as “information relating to an identifiable, living, natural person" and includes " biometric information". Biometric information is information gathered through biometrics " a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition". Using these definitions network cameras gathering live and recording the actions and movements of people is not necessarily the capture of personal information. However, if the system or persons operating the networked cameras identifies a person then video of an identified person becomes personal data. Identification could be through linking video to a person's name, identity number of similar identification information. But it can also take place through assigning identification to a person even if the name of the person is unknown. If there is a persistent identification of a person for example through face recognition or gait recognition, then data gathered on the person may be regarded as personal information.

The gathering, recording and other use of personally identified information must be in accordance with the requirements of POPIA. Thus, as soon as anyone recorded by networked cameras are identified the operators of the cameras must apply POPIA. This requires that there must be a lawful cause for gathering and retaining the data, that its use must be restricted, that the data subjects be made aware that their data is being processed, that the data be secured, and that the data may not be transmitted outside of South Africa.

Merely capturing video with cameras or analysing it with an AI without correlating the footage with personal information such as a name or a persisten identifier for an individual seems to fall outside POPIA at least as it is currently understood. Video without individual identification of those show in it does not seem to be personal data as currently defined. But if AI is used to identify individuals either through connection with existing identifiable information or by assigning a persistent identification to data as referring to an individual then POPIA will apply. This does not mean that it the surveillance is unlawful but

that the operator of the network will have to comply with POPIA including by justifying the collection and retention of the data, and by enabling those persons whose data are held to required correction or deletion. AI computer vision could be used in other ways, for example to analyse foot traffic patterns.

If AI is used to analyse personal data then the provisions of POPIA on automated decision making apply. When personal information is processed by automated means, such as by an AI, to provide a profile that relates to that person's location and conduct, that cannot be used to make a decision that has legal consequences for that person or that affects the person to a substantial degree. If a computer vision system was used to identify a person as suspicious so that they were denied access to a public place or place generally accessible by the public that would be prohibited. Similarly, if computer vision were used to single out an identifiable person for investigation by the police that may be the basis for a search or an arrest unless other protections for the person are in place.

In order to install networked cameras on sidewalks and other public areas private actors requires permission from the municipal authority designated to co-ordinate the actors installing wires, fibre, pipes and the like in public spaces. Permission to install infrastructure is referred to as 'way leave'. In the case of (*Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others*, 2020) a single judge in the Johannesburg High Court dealt with a dispute between Vumacam and the municipal body authorised to grant way leaves, the Johannesburg Road Agency (JRA). The JRA had previously granted way leaves to Vumacam enabling it to install cameras in public places. However, it refused new applications, contending that installation and operation of the cameras infringed the right to privacy. The applicable law did not give it a discretion whether to grant way leaves or not but merely to ascertain whether administrative requirements were met. The JRA contended that it was compelled to refuse the way leaves until appropriate legislation was passed empowering it to take issues such as privacy into account. In a formalist judgement the judge dismissed the JRA's arguments and ordered that the JRA grant the way leave. The JRA applied for leave to appeal but the judge refused leave. Whether the judgement is in accordance with the requirements of the South African constitution will be discussed in the next section.

4.3.2 Human Rights Concerns

In South Africa, the accountability of the private sector engaged in surveillance activities is currently a major concern. This is due to the fact that most monitoring practices, including CCTV camera surveillance, are carried out by the private sector and the government without revealing the full scope of the surveillance activities. International human rights laws do not hold companies like Vumacam legally responsible for safeguarding individuals' rights recognised and protected in South Africa, including the digital right to privacy. Under international human rights law the government of South Africa has the

primary responsibility to ensure that both privacy and the rule of law is maintained within its territory. The government has the obligation to ensure that private businesses follow the law and are kept responsible for violations of fundamental rights under domestic law. The UN's guiding principles on business and human rights apply the UN's "protect, respect, and remedy" framework into effect. This framework acknowledges that private companies bear the responsibility to uphold human rights, and that the government also protects them, when people need access to a remedy if their rights are violated (UNHRC, 2008, p. 3). These are, however, standards that the government can use as a guide, and they are not legally binding.

However, the South African Bill of Rights applies to actions by the private sector. Section 8(2) provides that the rights in the Bill of Rights bind non-state actors when required by the nature of the right and the duty imposed by the right. The right to privacy binds non-state actors. If a corporation has an office or assets in South Africa, then South African courts can exercise jurisdiction over it and compel compliance with its legal obligations. Thus, private companies that deploy networked cameras and automated surveillance are obliged to uphold the right to privacy, failure to do so can result in a court ordering both changes in behaviour and monetary compensation.

Section 7(a)of the Companies Act states that one of the Act's purposes is to encourage conformity with the South African Constitution's Bill of Rights (Gwanyanya, 2015). Is this section sufficient to requires companies to be held responsible for human rights abuses? Public sector and private companies that deal with personal data are liable under Section 8 of the POPI Act to deal with personal information in accordance with the Act. This is a crucial for the security of personal information because if a person does not know who is collecting their personal data, they may not have the resources to correct inaccuracies or request the deletion of that information, as provided for in Section 24 of the POPI Act. According to the above, it is the Information Regulator's duty to ensure that public and private bodies engaged in CCTV surveillance activities are in line with the POPI Act, and that proper checks must be performed in those companies.

There are a number of state actors that could potentially regulate automated surveillance, yet none have taken up the role. While the Information Authority is one such actor, local authorities such as city councils and courts could also play a part. However, an oversight role by either may be prevented by the judgement in (*Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others*, 2020). In that case the Johannesburg not only failed to protect the right to privacy but prevented local government from doing so. In a narrow formalistic decision Judge Valy stated that the local government agency that gave permission for cameras to be installed could not refuse the demands of a corporation. This despite the provisions of the

Bill of Rights which override any other law. Section 8 (1) of the Bill of Rights states that "This Bill of Rights applies to all law and binds the legislature, the executive, the judiciary and all organs of state." The Bill of Rights thus applies to both local government and court itself, both are part of the state which according to Section 7(2) "must respect, promote and fulfil the rights in the Bill of Rights".

In interpreting the law in respect of way leaves the court was under a clear obligation to interpret that law in accordance with the Bill of Rights. If the law could not be interpreted to conform with the Bill of Rights, then it should have been struck down as unconstitutional. Section 2 of the Constitution states: "This Constitution is the supreme law of the Republic, law or conduct inconsistent with it is invalid and the obligations imposed by it must be fulfilled." Why the judge chose a formalist approach at odds with the constitutional order that began in 1993 is unclear from the judgement. Judges in South Africa's other eight provinces can rule differently on the same question. Even a judge in the same province could rule differently if she believed the decision to be wrong. Since the judgement is concerned with such important issues as the constitutionally protected right to privacy a judge who believes that the decision is wrong should have no hesitation in finding differently. The local government, the Johannesburg City Council, could amend its own bylaws to either prohibit the giving of way leave for installing cameras or imposing privacy protection rules on those to whom it grants way leaves.

4.3.3 Readiness and Governance Challenges

Aside from the documented infrastructure constraints and inconsistencies in ICT policy and regulatory failure (Gillwald et al., 2019), South Africa does not yet have a national AI strategy. However, the Report of the Presidential Commission on the Fourth Industrial Revolution to develop a strategic plan for South Africa's 4IR vision suggests that the government is thinking about how to regulate and use AI (RSA 2020). The then Department of Science and Technology, in the meantime had sponsored the establishment of South Africa's Centre for the Fourth Industrial Revolution which is part of the World Economic Forum's Centre for the Fourth Industrial Revolution Network for Global Technology Governance, at Council for Scientific and Industrial Research, which aims to establish policies and governance mechanisms that will enable South Africa to use AI responsibly (C4IR, 2017).

One candidate for regulating the deployment computer vision technologies for mass visual surveillance is the Information Regulator is established in terms of the Protection of Personal Information Act 4 of 2013 (POPIA). However, the regulator only had power to regulate fully from mid-2020 when the majority of POPIA came into force. It is primarily concerned with information that can be linked to the identity of a person. Thus, the mere tracking of an individual through networked cameras may not fall in the ambit of POPIA. However, picking out an individual as suspicious to subject to further surveillance or some other

measure it if is through an automated process likely falls outside of POPIA mandate. Is the Information Regulator sufficiently resourced to regulate these practises? Issues that deal with surveillance are seen as the purview of other actors, not least the departments of justice, the police and state security agency. While the judicial oversight to which these have subject is insufficient it may be the courts will prove a more robust guardian of the fundamental right to privacy.

4.3.4 Potential Risks and Harms

The risks of the deployment of computer vision surveillance networks in South Africa include the consequences of clearly legal activities, of questionably legal activities and of illegal activities. The most salient harm is that the privacy of individuals may be infringed through the collection, use and retention of their personal information. Failure to comply with POPIA would harm an individual's privacy. However even activities compliant with POPIA may infringe the constitutional right to privacy, either because POPIA does not set a sufficiently high standard and does not comply with the constitutional right or because the activity is outside the scope of POPIA but implicates privacy.

The use of computer vision for automated surveillance encompasses several possible applications, not only facial recognition but gait recognition and number plate recognition. These applications identify individuals, or for number plate recognition, vehicles linked to individuals. To the extent that individuals are identified these applications will be regulated by protection of personal data laws. But what of applications that have an impact on individuals even if they are not identified? Efforts to detect 'suspicious behaviour' also referred to as 'anomalous activity'. This can result in a reaction by security personnel or the police. In countries such as South Africa where any encounter with the police carries personal risk of violence or false arrest and imprisonment merely because an algorithm identified one's behaviour as 'anomalous', potentially infringes fundamental rights including the right to freedom and security of the person. Algorithms deployed for other purposes have been found to exhibit bias (Buolamwini & Gebru, 2018a). If a 'suspicious behaviour' algorithm exhibits bias including racial bias, then security or police action will offend the rights to equality and dignity.

While privacy of identifiable individuals is one concern it is not the only possible harm. There is also a risk that mass surveillance will have a repressive effect on the population, shifting power from people to the corporate and governments actors that watch without being watched. This is a potential threat to democracy. In a rights framework it involves infringement of the rights of freedoms of movement, association and expression. Yet another set of harms involve inequality and exclusion.

4.3.5 Inequality and Exclusion

The Aadhaar identity system in India has been controversial both for concerns around privacy and for excluding persons from obtaining identity documentation. In Kenya the Huduma Namba government identity scheme prompted a judgement from the Kenyan Hight Court that the government must introduce personal data protection together with the identity schemes (Jain, 2019; Privacy International, 2020).

The growing use of artificial intelligence (AI) surveillance technologies in South Africa poses serious concerns ranging from privacy to exclusion (Mungai, 2019; Silvia Masiero, 2019; Swart & Munoriyarwa, 2020). The ability for social security systems to condition access to public services on state and private surveillance demonstrate not only the fact that technologies are not impartial, but also how they can potentially differentially affect groups of people based on their gender, skin colour, and social status (Kwet, 2017, 2019). While the divide between rich and poor continues to grow, Southern Africa remains the world's most unequal region (Gillwald, 2017). According to the Research ICT Africa After Access study, there are significant regional disparities between socio-economic levels in areas such as digital literacy, digital divide, and access to safe education. Thus, the continent's high levels of inequality have a direct impact on the well-being of its inhabitants, growth capacity, and exercise of fundamental rights (Gillwald et al., 2018).

Recent research in the South African setting shows that AI-driven technologies have a history of entrenching social divisions and exacerbating social inequality, particularly among traditionally marginalized groups (Kwet, 2017, 2019). Our analysis of the literature suggests that this trend persists also on a global scale, and that low-and middle-income countries may be more vulnerable to the negative social effects of AI while being less likely to benefit from the associated benefits (Dand, 2019; Raji et al., 2020). A better understanding of AI's social effects in various social settings is a prerequisite for the creation, implementation, and monitoring of responsible and beneficial AI technologies, as well as the foundation for effective regulation of these technologies.

4.3.6 Public-Private Partnerships Smart CCTV Surveillance

The rapid emergence of disruptive technologies like artificial intelligence (AI) surveillance technologies in South Africa necessitates the development of new governance structures to ensure safety and ethics in their deployment process, mitigating risks while maximizing their benefits to the society. AI governance should encompass the collaboration of all stakeholders including the government and private sector who are the main drivers. Several organisations have called out big tech companies for their lack of public oversight to ensure that emerging technology such as AI are used ethically (Allen, 2020; Ruttkamp-Bloem, 2021), and others have been banned as high-risk in countries like US and UK, such as facial

recognition for law enforcement before a suitable regulatory system is in place (Chee, 2020; Peters, 2020). Though collaboration between the South African government and big technology companies is crucial for developing creative governance solutions that can be adapted as technology progress not only to promote innovation and commercial implementation but also to provide strong guardrails that safeguard human rights and social values.

The role of big technology companies such as Vumacam while deploying smart surveillance technologies will need to be closely monitored by the South African Information Regulator. The proliferation of CCTV in South Africa has gained traction within the private sector through public-private partnerships, especially by security companies and big technology firms along with the government (Slabbert, 2017; Swart, 2018c). Although crime prevention and maintaining public safety are cited as the primary reasons for the expansion of these technologies, they are often-masked profit motives that emerge as a major ethical problem that requires investigation in order to avoid unnecessary and unwarranted monitoring of individuals.

4.4 Case Study South Africa Conclusion

However, the adoption of smart surveillance technologies is expected to grow steadily, particularly in public space surveillance as the South African government shows interest. It is also likely that South Africa considering its fragile regulatory environment may serve as testing grounds for emerging AI surveillance technologies. If people are to agree to give up more personal privacy for the sake of protection, facial recognition technology must be used in a trusting environment.

In South Africa although there are no laws explicitly regulating the use of CCTV surveillance technologies the constitutional right to privacy and POPIA do apply to the use of CCTV technologies, however application is still being determined and seems to some extent dependent on social acceptance of mass visual surveillance. Furthermore, there are no mechanisms auditing algorithms used for facial recognition systems, nor are there any penalties in place for technology companies that attempt to ‘harvest' or ‘scrape' user data. Given the dominance of the private sector in deploying smart surveillance technologies, designing good practice frameworks for the use of AI surveillance technology for mass surveillance in public spaces should be a co-regulation model.

5. Thematic analysis

5.1 More than Privacy

The use of computer vision for automated surveillance encompasses a number of possible applications, not only facial recognition but gait recognition and number plate recognition. These applications identify individuals, or for number plate recognition, vehicles linked to individuals. To the extent that individuals are identified these applications will be regulated by protection of personal data laws, at least where such laws are in force. But what of applications that have an impact on individuals even if they are not identified? Efforts to detect 'suspicious behaviour' also referred to as 'anomalous activity'. This can result in a reaction by security personnel or the police. In countries such as South Africa where any encounter with the police carries personal risk of violence or false arrest and imprisonment merely because an algorithm identified one's behaviour as 'anomalous' potentially infringes fundamental rights including the right to freedom and security of the person. Algorithms deployed for other purposes have been found to exhibit bias (Buolamwini & Gebru, 2018a). If a 'suspicious behaviour' algorithm exhibits bias including racial bias then it will offend the rights to equality and dignity.

This raises the issue of data sovereignty problems regarding laws regulating the gathering or transmission of data from outside Botswana territory through surveillance technologies which (Zuboff, 2018) describes as a form of “Surveillance Capitalism”. However there is very little publicly available information about transmission of data between China and Botswana that may result from Huawei’s activities as a major partner of the Safe City project, especially since Huawei, which is closely connected to the Chinese government (Swart & Munoriyarwa, 2020).

5.1.1 Algorithmic Bias

Simply put, an algorithm can be defined as a series of rules controlling a specific operation (Techterms, 2013), it is common that these biases develop when a machine learning algorithm generates outcomes that are systemically biased as a result of erroneous assumptions from the output of a computer system. The analysis of this study did not show any significant biases in the Safe City project but historically, the United States experience with surveillance technologies may provide valuable lessons for Botswana on the potential for bias in AI surveillance, especially on facial recognition technology. For instance, in several tests performed by a US based non-regulatory government agency, the National Institutes of Standards and Technology (NIST) has revealed the various social biases found into real-world AI surveillance systems (NIST, 2019). These biases and other related inaccuracies in automated systems have been

attributed to harmful outcomes that discriminate against people of colour, particularly black women which has diminished public trust in technology.

Facial recognition technologies rely on comparing images against a vast pool of other images, often not always obtained in demographically diverse contexts from which the technology is used. A lack of representative datasets is an issue for many technology companies looking to develop diverse facial recognition systems. As stated in the introduction of the Botswana case study an AI facial recognition startup company, Cloudwalk were given access to millions of images of black faces of Zimbabwean citizens as a model test subject for their facial recognition system (Bulelani, 2019; Chutel, 2018).As a result of these findings, our research shows the possibility for discrimination emerging from these systems, making surveillance more than just a problem of personal privacy, but also a question of social justice. Interestingly, this correlation is related to how CloudWalk uses facial recognition and AI-powered technologies for mass surveillance in China targeting ethnic minority groups “social sorting”. For these reasons, we believe that the lack of inclusion in facial recognition databases holds as much danger as perpetuating exclusion. Therefore, to counter algorithmic bias, both privacy and equality must be recognized and framed as human rights.

5.1.2 Inequality and Exclusion

Research findings reveals disparities in error rates across demographic groups associated with facial recognition technologies, with female, Black, and 18-30-year-old subjects consistently having the lowest accuracy (Furl et al., 2002; Klare et al., 2012). An intersectional approach was used to evaluate three gender classification algorithms, including those developed by IBM and Microsoft, in the 2018 “Gender Shades” project. Darker-skinned females, darker-skinned males, lighter-skinned females, and lighter-skinned males were divided into four classes. All three algorithms performed poorly on darker-skinned females, with error rates up to 34% higher than on lighter-skinned males (Buolamwini & Gebru, 2018).

The National Institute of Standards and Technology (NIST) verified these findings, discovering that facial recognition technologies across 189 algorithms are the least accurate on women of colour (Grother et al., 2011). Subsequent NIST studies presented 'empirical evidence' of 'demographic disparities' about age, gender and race (Harwell, 2019). In addition, Renee Cummings, a US criminologist and influential ethical AI advocate told an Institute for Security Studies (ISS) seminar that algorithmic architecture is crucial in influencing biases (Institute for Security Studies, 2020).

Despite the fact that there is a substantial risk that facial recognition technology will violate data privacy and fundamental rights, the implementation of these technologies has proceeded without adequate checks and balances. Mass surveillance through facial recognition technology jeopardizes not only the right to privacy, but also democracy, independence, and perpetuates inequality and exclusion for minority groups in society.

Botswana govt provide the public good of safety using private companies and in South Africa private companies have start proving public goods with little government other than in some cases with the blessing of local government and in other cases opposition by government but the connivance of a court.

While automated surveillance may possibly decrease crime, although that has not been proven, and increase public perceptions of security it does so at a cost to privacy. The goods the automated surveillance is intended to produce; public safety and security are public goods. However their provision is partially privatised in many instances, wholly so in the case of Vumacam. This is cause for concern, both in respect of equitable provision of public goods and with increasing dependence of the state on profit motivated private actors. It would be facile to claim that computer vision is somehow neutral, its outcomes dependant only on the ends to which it is deployed. Such a claim would obscure the significance of computer vision, how systems can enable a few people to monitor and analyse massive amounts of data in a way that was simply impossible until very recently. This constitutes a significant concentration of power, whatever its purpose.

6. Thematic conclusions and recommendations

This research illustrates that analysing the implications of a particular technology for development is in many ways less revealing than to examining a technological phenomenon that has fused with its raison de'etre such as bio-id. However, a number of conclusions can be drawn from these two case studies:

First of these is that the existing legal and governance frameworks for the use of computer vision for automated surveillance are inadequate. The use of facial recognition technologies can be expected to increase steadily, especially in the realm of public space surveillance. It is also possible that many countries in Africa with weak regulation can become testing grounds for emerging biometric technologies. Since governance is inadequate in constitutional democracies such as Botswana and South Africa it seems extremely unlikely that they are adequate elsewhere in Africa and our research does not suggest otherwise. Legal and governance frameworks are inadequate in at least three respects. They lack clarity as to how the right to privacy extends to being observed in a public space. They don't require transparency or reporting on the uses or possible abuses of automated surveillance. They also fail to impose clear

duties on private profit driven actors using public spaces and providing public goods. The one exception to this is personal data protection regimes, although that in Botswana is not yet operational and in South Africa it is not yet fully operational.

However, guidelines or regulations from a personal data protection agency, or even legislation on automated surveillance of the public are unlikely to be sufficient on their own. That is because at least some state actors don't seem to have internalised importance of privacy as is dramatically illustrated by the refusal of the court to protect privacy in the Vumacam case discussed. To be effective a governance regime must re-orientate the priorities of the actors, especially the actors overseeing the regime towards the protection of privacy. For data protection and privacy to be realised in practise, the requisite skills must be developed in the commercial crimes' unit of the police, the national prosecuting authority and the general public. If citizens are to agree to surrender more personal privacy for the sake of security, computer vision technologies must be deployed in a climate of trust. Far greater transparency, accountability and explainability will be required to create such a climate.

Globally publics are is becoming even more aware of algorithmic bias in AI training datasets and its negative effect on predictive policing analytics and other law enforcement computational resources. While advanced AI surveillance technologies continue to hold great promise, the abrupt deployment of surveillance systems without proper evaluation, transparency, and oversight will lead to serious risks. Will African publics exhibit similar awareness as computer vision surveillance increases in the continent?

Making surveillance more visible and comprehensible hardly guarantees a just and equitable society, but it is certainly a necessary condition for one. The main goal of surveillance networks is monitoring movements of people. The gathering and processing of personal data in centralised databases may aid policing but poses security, governance, human rights and privacy challenges. This study has gone some way towards enhancing our understanding of how African governments deploy facial recognition and AI surveillance systems, some believed to be deployed for spying citizens and political opponents (Chin, 2019). Many African countries share these similar concerns about the implementation of public-driven AI surveillance systems. These observations have several implications towards political structures, and while the priorities for the deployment of CCTV surveillance systems often vary, in most of the times these imported surveillance technologies pose challenges to existing democratic norms and practices.

Another important conclusion is that despite its name 'computer vision' these systems do not equate to human vision. On the contrary while they may take in light waves, convert these to digital data and analyse them this does not equate to the ways that humans and other animals see. Instead, these systems remain unable to see in context as humans do. While machine data acquisition and analysis remain

useful it is important that these systems are not independent of human power relationships nor is there anything inevitable about the shape as they are developed.

7. References

Adams, N. (2020). *Cape to be first with CCTV law*. https://www.iol.co.za/weekend-argus/news/cape-to-be-first-with-cctv-law-5eec5881-c3a8-40f7-8397-b79d65452de0

Adrienn, L. (2016). *What is Privacy? The History and Definition of Privacy*. Undefined. /paper/What-is-Privacy-The-History-and-Definition-of-Adrienn/430bfacbabb89c0033b6dcceddc18ba9bbc02c5f

Allen, K. (2020, July 6). *ISS TODAY: Future of facial recognition technology in Africa examined*. Daily Maverick. https://www.dailymaverick.co.za/article/2020-07-06-future-of-facial-recognition-technology-in-africa-examined/

AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others [2021] ZACC 3, CCT 278/19, CCT 279/19 (Constitutional Court South Africa 4 February 2021). http://www.saflii.org/za/cases/ZACC/2021/3

BirdDog. (2019). *PTZ Keyboard User Guide*. https://bird-dog.tv/UG/PTZ-Keyboard_user-guide_part-1.pdf

Boksburg Advertiser. (2020, August 27). Businesses team up for a safer Ekurhuleni. *Boksburg Advertiser*. https://boksburgadvertiser.co.za/393617/makopano-and-vumacam-team-up-for-a-safer-ekurhuleni/

Business Tech. (2018). *Joburg is getting new CCTV surveillance cameras*. https://businesstech.co.za/news/business/260151/joburg-is-getting-new-cctv-surveillance-cameras/

Business Tech. (2019). *Watch: South African highway cameras used to track hijackers*. https://businesstech.co.za/news/technology/328221/watch-south-african-highway-cameras-used-to-track-hijackers/

Business Tech, S. (2021, June 30). *South Africa's new personal information laws come into effect from tomorrow*. https://businesstech.co.za/news/internet/412029/south-africas-new-personal-information-laws-come-into-effect-from-tomorrow/

C4IR. (2017). *C4IR-SA – The South African Centre for the Fourth Industrial Revolution*. https://www.c4ir-sa.co.za/

Chee, F. Y. (2020, January 16). EU mulls five-year ban on facial recognition tech in public areas. *Reuters*. https://www.reuters.com/article/uk-eu-ai-idINKBN1ZF2QN

City of Cape Town. (2014). *CAPE TOWN METROPOLITAN POLICE DEPARTMENT: ANNUAL POLICE PLAN*. https://resource.capetown.gov.za/documentcentre/Documents/City%20strategies,%20plans%20and%20frameworks/Annexure%20I%20-%20Annual%20Police%20Plan%202013%20-%202014.pdf

City of Cape Town. (2016). *REGULATION OF EXTERNAL AND PRIVATELY OWNED CCTV CAMERAS ON CITY PROPERTY POLICY – (POLICY NUMBER 21207)*.

https://resource.capetown.gov.za/documentcentre/Documents/Bylaws%20and%20policies/Regulation%20of%20External%20and%20Privately%20Owned%20CCTV%20Cameras%20on%20City%20Property%20-%20%28Policy%20number%2021207%29%20approved%20on%2025%20June%202014.pdf

City of Cape Town. (2018). *City of Cape Town Integrated Annual Report 2-18/19*. Western Cape Government. https://resource.capetown.gov.za/documentcentre/Documents/City%20research%20reports%20and%20review/CCT_Annual_Report_2018_19.pdf

Crunchase. (n.d.). *Vumatel—Crunchbase Company Profile & Funding*. Crunchbase. Retrieved 15 February 2021, from https://www.crunchbase.com/organization/vumatel

Czernowalow, M. (2005, June 27). Inner city surveillance 'a success`. *ITWeb*. https://www.itweb.co.za/content/DZQ587V6mLp7zXy2

Dand, M. (2019, May 21). The Future of AI is Ethics by Design, Diversity, and Inclusion. *Medium*. https://becominghuman.ai/the-future-of-ai-is-ethics-by-design-diversity-and-inclusion-ab3f0c8a0db2

Defence Web. (2009, December 11). Johannesburg adjudges CCTV project a success. *DefenceWeb*. https://www.defenceweb.co.za/security/civil-security/johannesburg-adjudges-cctv-project-a-success/

Department of Transport. (2018). *Publication of Draft Roads Policy for South Africa for Public Comment*. Department of Transport. https://static.pmg.org.za/1/180309draftroadspolicy.pdf

Duncan, J. (2018). How CCTV surveillance poses a threat to privacy in South Africa. *The Conversation*. http://theconversation.com/how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa-97418

Gillwald, A. (2017). *From Digital Divide to Digital Inequality: The Connectivity Paradox*. Law and Development Research Conference. https://researchictafrica.net/publications/Other_publications/2017_Gillwald_From_digital_divide_to_digital_inequality.pdf

Gillwald, A., Calandro, E., Sadeski, F., & Lacave, M. (2019). *South Africa – The potential of the 4th Industrial Revolution for Africa*. Africa Development Bank Group. http://4irpotential.africa/south-africa/

Gillwald, A., Mothobi, O., & Rademan, B. (2018). *The state of ICT in South Africa* (After Access Policy Paper No. 5, Series 5; Policy Paper Series 5: After Access-Assessing Digital Inequality in Africa). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf

Gwanyanya, M. (2015). The South African Companies Act and the realisation of corporate human rights responsibilities. *Potchefstroom Electronic Law Journal (PELJ)*, *18*(1), 3102–3131. https://doi.org/10.4314/pelj.v18i1.05

Hikvision. (n.d.). Sea Point sees two-thirds Crime Drop after Hikvision Cameras Deployed. *hiknow*. Retrieved 22 February 2021, from https://www.hikvision.com/hk/newsroom/success-stories/traffic/sea-point-sees-two-thirds-crime-drop-after-hikvision-cameras-deployed/

hi-tech Security Solution. (2011). *Securing Cape Town—CCTV Handbook 2011—Fibre Based Integrations—Hi-Tech Security Solutions*. http://www.securitysa.com/regular.aspx?pklregularid=4981

Hosken, G. (2008, September 19). *Pretoria malls among SA's most dangerous*. https://www.iol.co.za/news/south-africa/pretoria-malls-among-sas-most-dangerous-417049

Huawei. (2019). Rain and Huawei Jointly Announce the 5G Provisioning to Selected Users in South Africa. *Huawei*. https://www.huawei.com/en/news/2019/9/rain-huawei-provisioning-selected-users-south-africa

Huidong, M. (2019). Smart Cities: Building a People-Centric World. *Huawei Enterprise*. https://e.huawei.com/za/publications/global/ict_insights/201908281022/features/201911081422

Independent Online. (2019). *City of Cape Town to add dozens of CCTV cameras to surveillance network*. https://www.iol.co.za/capeargus/news/city-of-cape-town-to-add-dozens-of-cctv-cameras-to-surveillance-network-20941663

Independent Online. (2021, February 24). *Sensory surveillance and smart devices: Why we should care about the cost of convenience*. https://www.iol.co.za/technology/techsperts/sensory-surveillance-and-smart-devices-why-we-should-care-about-the-cost-of-convenience-89f6ed76-d9c8-4971-91c0-4556d6e72333

Intelligent Surveillance and Detection Systems (Pty) Ltd (ISDS). (2013, April 2). *ISentry Ultra Smart Video Analytics*. https://www.youtube.com/watch?v=iu23WQra8to

Intelligent Transport Society South Africa. (2008). *City CCTV tender in dispute | ITS South Africa*. http://itssa.org/city-cctv-tender-in-dispute/

Jili, B. (2020, November 12). Surveillance Tech in Africa Stirs Security Concerns – Africa Center. *Africa Center for Strategic Studies*. https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/

Jing, J. (2019). *China helps South Africa's telecommunications industry leapfrog development* [Press release]. http://www.gov.cn/xinwen/2019-04/16/content_5383271.htm

Kwet, M. (2017, May 3). Apartheid in the Shadows: The USA, IBM and South Africa's Digital Police State. *CounterPunch.Org*. https://www.counterpunch.org/2017/05/03/apartheid-in-the-shadows-the-usa-ibm-and-south-africas-digital-police-state/

Kwet, M. (2019a). *Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa*. https://www.vice.com/en/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa

Kwet, M. (2019b, November 22). Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa. *Motherboard (Vice)*. https://www.vice.com/en/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa

Larsen, L. (2006). *Lights, camera ... Less criminal action—December 2006—Hi-Tech Security Solutions*. http://www.securitysa.com/article.aspx?pklarticleid=4191

Matiso, S. (2020, February 9). *Vumacam explains move behind rollout of CCTV cameras in Johannesburg suburbs* [Interview]. https://www.702.co.za/articles/395116/vumacam-explains-move-behind-rollout-of-cctv-cameras-in-johannesburg-suburbs

McCloed, D. (2019, February 14). Vumatel to blanket Jo'burg in CCTV cameras—TechCentral. *TechCentral*. https://techcentral.co.za/vumacam-to-blanket-joburg-in-cctv-cameras/87458/

Minnaar, A. (2007). The implementation and impact of crime prevention / crime control open street Closed-Circuit Television surveillance in South African Central Business Districts. *Surveillance & Society*, *4*(3). https://doi.org/10.24908/ss.v4i3.3447

Minnaar, A. (2012). *Private security companies, neighbourhood watches and the use of CCTV surveillance in residential neighbourhoods: The case of Pretoria-East | Acta Criminologica: African Journal of Criminology & Victimology*. *32*(1). https://journals.co.za/doi/abs/10.10520/EJC138451

Moubray, C. (2019, October 20). PRIVATE EYES: Delays in privacy laws are costing South Africans money and security. *Daily Maverick*. https://www.dailymaverick.co.za/article/2019-10-21-delays-in-privacy-laws-are-costing-south-africans-money-and-security/

Moyo, A. (2019). *Tech makes gains in arresting crime in inner city Joburg | ITWeb*. https://www.itweb.co.za/content/dgp45MaGNGjvX9l8

Mungadze, S. (2019, March 9). *Professor decries Joburg's private surveillance networks | ITWeb*. https://www.itweb.co.za/content/Pero37ZgoYJMQb6m

Mungai, C. (2019). *Kenya's Huduma: Data commodification and government tyranny*. https://www.aljazeera.com/opinions/2019/8/6/kenyas-huduma-data-commodification-and-government-tyranny

My Broadband. (2019, February 14). *Vumacam – Vumatel's CCTV system to keep South Africa safe*. https://mybroadband.co.za/news/security/295960-vumacam-vumatels-cctv-system-to-keep-south-africa-safe.html

Mzantsi, S. (2014). *Cape Town expands CCTV footprint*. https://www.iol.co.za/news/south-africa/western-cape/cape-town-expands-cctv-footprint-1740724

Mzekandaba, S. (2016a). *Joburg drives investment in smart policing | ITWeb*. https://www.itweb.co.za/content/KwbrpOMgmpEvDLZn

Mzekandaba, S. (2016b, March 14). Cape pumps R14m into invisible policing. *ITWeb*. https://www.itweb.co.za/content/2JN1gP7OpnAMjL6m

News24. (2015a). Businesses returning to safer Joburg CBD - JMPD. *News24*. https://www.news24.com/News24/Businesses-returning-to-safer-Joburg-CBD-JMPD-20150814

News24. (2015b). Cameras zoom in on criminals in Cape suburbs | News24. *News24*. https://www.news24.com/News24/Cameras-zoom-in-on-criminals-in-Cape-suburbs-20151105

Newzroom Afrika. (2020, August 6). *NEWZROOM AFRIKA: South Africa Lockdown and crime – Vuma Secure*. https://www.vumacam.co.za/south-africa-lockdown-and-crime/

Observatory Improvement District. (2019). *Licence Plate Recognition (LPR) technology working for Observatory – OBSID*. https://obsid.org.za/licence-plate-recognition-lpr-technology-working-for-observatory/

Oxford Insights. (2020). Government AI Readiness Index 2020—Oxford Insights. *Oxford Insights*. https://www.oxfordinsights.com/government-ai-readiness-index-2020

Peters, J. (2020). *Portland passes strongest facial recognition ban in the US - The Verge*. https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology

PSiRA. (2019). *PSiRA Security Equipment Satisfactory Survey Findings*. DEMACON. https://www.psira.co.za/dmdocuments/research/PSIRA%20Integrated%20Security%20Equipment%20Report_March%202019.pdf

PWP Neighbourhood Watch. (2015). *LPR Project Information – PWP Neighbourhood Watch*. https://pwpnw.co.za/2017/01/03/lpr-project-information/

Rabkin, F. (2019, May 31). SA's suburban camera creep tests privacy—The Mail & Guardian. *Mail & Guardian*. https://mg.co.za/article/2019-05-31-00-sas-suburban-camera-creep-tests-privacy/

Raji, I. D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., & Denton, E. (2020). Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 145–151. https://doi.org/10.1145/3375627.3375820

Rangongo, T. (2019, February 15). *These Joburg suburbs are getting 15,000 CCTV cameras*. https://www.businessinsider.co.za/vumatel-launches-vumacam-cctv-security-cameras-around-johannesburg-suburbs-2019-2

Ruttkamp-Bloem. (2021). *Artificial intelligence presents a moral dilemma—The Mail & Guardian*. https://mg.co.za/opinion/2021-02-21-artificial-intelligence-presents-a-moral-dilemma/

Schoeman, F. (1984). Privacy: Philosophical Dimensions. *American Philosophical Quarterly*, *21*(3), 199–213.

SIlvia Masiero. (2019, September 12). A new layer of exclusion? Assam, Aadhaar and the NRC. *South Asia @ LSE*. https://blogs.lse.ac.uk/southasia/2019/09/12/a-new-layer-of-exclusion-assam-aadhaar-and-the-nrc/

Slabbert, A. (2017, September 1). Joburg CCTV crime fighting cameras unmanned. *Moneyweb*. https://www.moneyweb.co.za/news/south-africa/tender-intervention-sets-back-safety-in-joburg/

Smith, J. P. (2019, June 17). Right of Reply: Safety in Khayelitsha is a grave concern, any act of violence needs to be condemned in the strongest terms. *Daily Maverick*. https://www.dailymaverick.co.za/article/2019-06-17-safety-in-khayelitsha-is-a-grave-concern-any-act-of-violence-needs-to-be-condemned-in-the-strongest-terms/

Swart, H. (2018a). Activist murder reveals Joburg street cameras are 'turned off'—The Mail & Guardian. *Mail & Guardian*. https://mg.co.za/article/2018-05-10-smile-you-may-not-be-on-camera/

Swart, H. (2018b, September 28). Eye on Crime (Part 2): Joburg's new hi-tech surveillance cameras: A threat to minorities that could see the law targeting thousands of innocents. *Daily Maverick*. https://www.dailymaverick.co.za/article/2018-09-28-joburgs-new-hi-tech-surveillance-cameras-a-threat-to-minorities-that-could-see-the-law-targeting-thousands-of-innocents/

Swart, H. (2018c, October 4). Eye on Crime (Part 3): Controlling Cape Town: The real costs of CCTV cameras, and what you need to know. *Daily Maverick*. https://www.dailymaverick.co.za/article/2018-10-05-controlling-cape-town-the-real-costs-of-cctv-cameras-and-what-you-need-to-know/

Swart, H. (2019a, June 13). *Visual surveillance and weak cyber security, Part One:...* https://www.dailymaverick.co.za/article/2019-06-13-visual-surveillance-and-weak-cyber-security-part-one-when-cameras-get-dangerous/

Swart, H. (2019b, July 21). SURVEILLANCE: How China's persecuted people are paying the price for Joburg's sense of security. *Daily Maverick*. https://www.dailymaverick.co.za/article/2019-07-21-how-chinas-persecuted-people-are-paying-the-price-for-joburgs-sense-of-security/

Swart, H., & Munoriyarwa, A. (2020). *Video Surveillance In Southern Africa*. Media Policy and Democracy Project. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf

Technews Publishing (Pty) Ltd. (2016). *The role of CCTV in Cape Town's successful security strategy—March 2016—Hi-Tech Security Solutions*. http://www.securitysa.com/54014n

Teleste. (2013, December 12). *Case study: Securing the safety of people in South Africa*. https://securitynewsdesk.com/case-study-securing-safety-people-south-africa/

Transport Telematics Africa Pty Ltd. (2010). CCTV for CBD Soccer World Cup. *Transport Telematics Africa*. https://transtelafrica.co.za/portfolio/cctv-for-cbd-soccer-world-cup/

UNHRC. (2008). *OHCHR | Reports of the SRSG on human rights and transnational corporations and other business enterprises*. https://www.ohchr.org/en/issues/transnationalcorporations/pages/reports.aspx

vpro documentary. (2015, June 12). *Bringing internet to Africa—VPRO documentary—2015*. https://www.youtube.com/watch?v=qlTZetW1Sy8&feature=youtu.be&t=2162

Vumacam. (2019a). *The Facts Regarding the Integrated Smart Camera Network – Vuma Secure*. https://www.vumacam.co.za/the-facts-regarding-the-integrated-smart-camera-network/

Vumacam. (2019b, February 15). *MY BROADBAND: How Vumacam's CCTV system works – Vuma Secure*. https://www.vumacam.co.za/how-vumacams-cctv-system-works/

Vumacam. (2021). *Vuma Secure – Trust in our vision*. https://www.vumacam.co.za/

Wenjun, C. (2018). Twenty years on, China-SA relations embrace a new chapter. *BusinessLIVE*. https://www.businesslive.co.za/bd/world/asia/2018-09-25-twenty-years-on-china-sa-relations-embrace-a-new-chapter/

West, E. (2019a). SA-China trade ties get R27bn boost. *IOL*. https://www.iol.co.za/business-report/economy/sa-china-trade-ties-get-r27bn-boost-27367274

West, E. (2019b, September 8). Presidential Commission to be established on 4IR strategies for SA | IOL Business Report. *Presidential Commission to Be Established on 4IR Strategies for SA*. https://www.iol.co.za/business-report/economy/presidential-commission-to-be-established-on-4ir-strategies-for-sa-32327532

Western Cape Government. (2012). *Western Cape Provincial Broadband Programme: Integrated Master Plan*. https://www.westerncape.gov.za/sites/www.westerncape.gov.za/files/western_cape_provincial_broadband_programme_integrated_master_plan.pdf

Wilson, C. (2019, February 14). *Meet Vumacam, Vumatel's smart security play for Joburg's suburbs*. https://stuff.co.za/2019/02/14/meet-vumacam-vumatels-smart-security-play-for-joburgs-suburbs/

Woodhams, S. (2020, March 20). *Huawei says its surveillance tech will keep African cities safe but activists worry it'll be misused*. Quartz Africa. https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/

Zama, Z. (2019, July 25). *'Big Brother' helps nab more than 150 criminals in Joburg CBD* [Interview]. http://www.702.co.za/articles/355892/big-brother-helps-nab-more-than-150-criminals-in-joburg-cbd