STRIKING A BALANCE BETWEEN CCTV SURVEILLANCE AND THE DIGITAL RIGHT TO PRIVACY IN SOUTH AFRICA

CONSIDERATIONS FOR THE INFORMATION REGULATOR

Dorcas Basimanyane and Dumisani Gandhi

APCOF
RESEARCH PAPER
SERIES 27
DECEMBER 2019

APCOF RESEARCH SERIES 2019

1. INTRODUCTION

The rollout of closed-circuit television (CCTV) surveillance cameras in private and public spaces in South African metropolitan areas is commonplace and topical. These CCTV surveillance cameras are usually found on highways, in malls, workplaces, public transport systems and private dwellings. CCTV surveillance can be a useful tool that contributes to public safety and security, the protection of people and property and the investigation of crime. It can also be a source of evidence used in criminal trials. However, as a tool for mass surveillance, CCTV surveillance systems can be prone to abuse by the State, corporates and individuals in ways that increase the likelihood of interfering with the right to privacy.

The rollout of CCTV cameras is currently not regulated in South Africa and there is no CCTV camera surveillance code of practice in place. To date, CCTV surveillance has been installed without clear guidelines on how to balance public safety and security imperatives with fundamental rights to privacy. There have been vague disclaimers emphasising compliance with privacy laws including the not yet fully operational Protection of Personal Information (POPI) Act of 2013. The Information Regulator (South Africa) will have to address the absence of clear regulations for CCTV mass surveillance in South Africa and enforce a set of norms and standards.

It is against this background that this paper seeks to explore the intersection between CCTV surveillance practices and the right to privacy in South Africa. It will also look at the role that the Information Regulator, created under the POPI Act, can play in protecting the right to privacy with reference to CCTV surveillance. The first section briefly explores a historical context of CCTV usage in South Africa and looks at the footprint of CCTV surveillance in South Africa. The next section attempts to understand what constitutes the right to privacy. The paper then analyses the POPI Act and regulations under the Act in relation to internationally recognised standards for regulating CCTV surveillance for the protection of human rights. This includes comparative analyses with practices in jurisdictions such as the European Union and the United Kingdom. The paper ends with recommendations for regulating CCTV surveillance in South Africa in the future.

2. HISTORICAL CONTEXT OF CCTV IN SOUTH AFRICA

CCTV installations in South Africa may not be comparable in number to those of western countries, such as the United States, Canada and the United Kingdom. However, there is a growing network of CCTV systems driven mainly by public authorities (e.g. municipalities and provincial governments), the business sector and private security companies. This development has led civil society and academics to fear a growing dystopian surveillance state that is perceived to be slowly eroding citizens' right to privacy.[1]

According to Minnaar, the use of CCTV in South Africa can be traced back to the 1970s when it was used in the mining sector – especially in diamond mines and gold refineries – to prevent the smuggling and pilfering of minerals.[2] In the 1990s and early 2000s, CCTV usage spread into the central business districts (CBDs) of most cities where both small and big retailers used CCTV surveillance ostensibly to prevent, detect, deter and control crime.[3] This is evidenced by the high prevalence of CCTV camera systems in private businesses (banks, retailers, warehouses, etc.). Security concerns around the 2010 World Cup soccer tournament in South Africa provided fresh impetus that drove public-funded expansion of CCTV on highways, sports stadiums and shopping malls.[4] Recently this has spread into neighbourhoods and private households for social crime prevention, community policing and personal safety.

3. THE SOUTH AFRICAN CCTV CAMERA SURVEILLANCE FOOTPRINT

Considering the largely unregulated manner of the installations and the myriad number of players involved, it is difficult to estimate the number of existing CCTV systems in the country. However, it is clear that CCTV coverage is popular and expanding based on a belief that it is effective in detecting and deterring crime. According to the Private Security Industry Regulatory Authority (PSIRA), CCTV is the third most sought after security equipment by clients of private security companies at 55.8% of clients.[5] In Tshwane secondary schools, 59% of pupils indicated that CCTV cameras were one of the numerous security measures present at their schools.[6] CCTV camera systems in South Africa are typically used in public spaces (roads, highways, malls, shopping centres, parks, bus stops, airports, warehouses, and along railway lines), businesses (shops, fuel service stations, ATMs), gated communities, community neighbourhoods, schools and private homes. Below are the general patterns of CCTV surveillance installations in South Africa and an assessment of the extent of CCTV usage, the key stakeholders, where the installations are deployed, by whom and for what purposes.

CCTV surveillance in CBDs and on urban highways

All major metropolitan areas in South Africa have CCTV camera systems in operation. Hundreds of kilometres of busy highways and roads in the CBDs and around South Africa's major cities are covered by an ever-expanding network of CCTV funded by the South African National Roads Agency (SANRAL) and municipal and provincial governments. According to SANRAL's 2018 Annual Report,[7] the agency has installed 289 high-tech CCTV cameras on over 200 km of Johannesburg's main highways linking with Pretoria[8], 146 high-tech CCTV cameras covering 120 km of Durban's highways[9] and 239 CCTV cameras monitoring more than 160 km of Cape Town's busiest freeways.[10] The City of Cape Town has an additional 713 cameras in its Integrated Rapid Transit System. These have been placed at all stations on busy routes as well as in the transport vehicles themselves.[11] An additional 513 cameras have been registered, as required under Cape Town City's by-laws, pushing the total number of CCTV cameras in Cape Town to in excess of 2 100.[12]

The City of Tshwane has 319 CCTV cameras in the CBD and surrounding areas[13] and significant budgets are being allocated to further expand the network.[14] The City of Johannesburg is also

expanding its CCTV network by adding 50 high-tech cameras to the existing 450 publicly funded CCTV cameras in the city as a crime detection strategy.[15]

CCTV in gated communities and security complexes

CCTV surveillance in gated communities is largely dominated by private security companies. There is limited information available on the extent of national coverage. The expansion into private residential domains has largely been driven by the growth of security estates and villages which have attracted crimes such as car hijackings, house robberies and burglaries.[16] According to Minnaar, in 2008, 80% of security estates in Pretoria's eastern suburbs had installed CCTV cameras that record 24/7 at the entry-gate control points and a control room to monitor and control physical access.[17] In many cases, the CCTV cameras are linked to licence plate recognition technology and can also record additional details, such as the identity of individuals. The requirements for entry are in line with the estates' right of admission policies. It is believed this system is prevalent country-wide in urban areas.

CCTV in private homes and workplaces

There is no disaggregated data on how many private homes or workplaces have CCTV as a crime deterrent outside of businesses like retail venues, shopping malls and fuel service stations. It is also not clear whether private home CCTV surveillance should be regulated or not and under what circumstances. Cases of voyeuristic opportunism or the mere act of a house owner focusing their CCTV cameras beyond their perimeter fence onto public spaces or neighbours' houses could be patently illegal, as they are in jurisdictions like the United Kingdom.

The trends identified above indicate that CCTV mass surveillance will inevitably need to be balanced with the right to privacy. As observed by Jane Duncan, this is a case where technology is a long way ahead of policy.[18]

4. WHAT IS THE RIGHT TO PRIVACY?

In order to understand the ways in which CCTV surveillance intersects with the right to privacy, there is a need to explore the notion of privacy. The right to privacy remains one of the concepts of modern times which is yet to have a universally accepted definition.[19] The claim for the right to privacy remains universal, but its concrete form differs according to the prevailing societal characteristics, culture and economic circumstances of the time. Despite the fact that the notion of privacy has a long history dating back to the 19th century, it must be reinterpreted in the light of the current era and be examined in the current context.[20]

There have been various multidisciplinary attempts at coming up with a definition of privacy. Under international law, the right to privacy is protected in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Unlike other rights contained in the ICCPR, the content and scope of the right to privacy was not fully explored in terms of the specific limitations to the right.

These international law instruments do not clearly define privacy but do state that, 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence nor to unlawful attacks on his honour and reputation.'[21] The Human Rights Committee through General Comment No. 16 of 1988 also steered away from defining privacy but provided examples of actions that would impact negatively on privacy, namely surveillance, searches of home and property, and personal and bodily searches. For the first time, personal information was added as an aspect that has the right to privacy.[22]

In the absence of a universally recognised definition, many experts and commentators had attempted to provide a definition of the notion of privacy even before the Human Rights Committee's General Comment No. 16. For example, the emerging threats to individual privacy associated with modern business methods and technologies were raised by Samuel Warren and Louis Brandeis in their famous work *The right to privacy*[23] in which they advocated for an explicit legal recognition of 'the right to be let alone', a phrase originally coined by Judge Cooley.[24] However, it was only in the 19th century that information privacy was accorded legal recognition in the United States of America.[25]

Other commentators have tried to narrow it down to a more generic, all-encompassing definition. Lukács says privacy may be legally defined as, 'an individual's condition of life characterised by exclusion from publicity.'[26] This perspective bestows power and control on an individual over their personal information, allowing them to conduct their personal affairs free from unwarranted intrusions.[27] It does not solely refer to the individual's personal space, but it equally extends to the home, the family and correspondence and in certain circumstances, a person's honour and reputation.[28]

Other researchers have tried to split the concept into different elements. Balule and Otlhogile argue that the right to privacy has two facets: substantive autonomy and informational autonomy.[29] Substantive autonomy is the presumption that a person should have a private sphere with or without interaction with others, free from state intervention and from unsolicited intervention by other uninvited individuals to make choices about personal life.[30] Informational autonomy denotes that the individual's private communications should be safeguarded and kept private. This facet of privacy enables individuals to be able to communicate freely, to exchange information on a platform that is free from intrusions by the State or other individuals, and that the communications should be received only by the intended recipients without any interference.[31]

There are other forms of privacy that are rarely mentioned and hence in most cases left unregulated. For example, locational and physical privacy is very topical at the moment coupled with the advances in technology. Locational privacy refers to the right of individuals to have free and undisturbed or unmonitored movements.[32] An individual's movements form part of their personal information which they have a right to exercise control over. Through an individual's movements, their political, social and personal affiliations can easily be established. This form of privacy is a fairly new form of privacy and many jurisdictions do not legally recognise it.

The norm in most common law jurisdictions is that there is no reasonable expectation of privacy in public spaces. The challenge with this view is that the continuing unregulated rollout of CCTV cameras has become widespread. Due to technological advancements, modern CCTV cameras are more pervasive than the previous ones. For example, the current CCTV cameras can have facial recognition software and their capacity to collect massive amounts of data on individuals is extensive.

All these definitions cover elements of what should constitute the right to privacy even though there is no single universal definition. It would appear that with the development of computing power and the internet, combined with the rise of terrorism and an increase in state monitoring of citizens' communications, surveillance and personal information have become the main vehicles through which privacy is conceptualised.

5. LEGAL PROTECTION OF THE RIGHT TO PRIVACY IN SOUTH AFRICA

The right to privacy in South Africa is protected under the Constitution and common law. Section 14 of the 1996 Constitution states:

> *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.*

The wording of the Constitution clearly shows that the right to privacy is extensively protected under the law. The law of South Africa proscribes interference with the private communications of individuals. A more comprehensive protection of the digital right to privacy is accorded in the yet to be fully implemented POPI Act that will be discussed below.

South Africa is also a party to several international human rights legal instruments which recognise and protect the right to privacy, namely, the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the Committee on the Rights of the Child (CRC), and the African Charter on the Rights and Welfare of the Child (ACRWC). South Africa is a dualist state and international instruments can only be directly applicable after domestication except in cases of self-executing treaties and customary international law.

S 39(1b) and S 233 of the Constitution provide that when interpreting the Bill of Rights, the courts must consider international law and 'prefer any reasonable interpretation of the legislation that is consistent with international law over any alternative interpretation that is inconsistent with international law.'[33]

Furthermore, in the case of the *Government of the Republic of South Africa and Others v Grootboom and Others,* the court held that, where the relevant principles of international law bind South Africa, such principles may be directly applicable.[34]

However, the right to privacy is not absolute. The protection awarded to the right to privacy has a limitation clause under Section 36 of the Constitution. This clause states that any restriction of a right must be limited only in terms of the law of general application and to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. Under international law, the proportionality test demands that all the statutes that affect human rights must be proportionate or reasonable. Any statutes must therefore be adequate, necessary and proportionate *stricto sensu*.

Crime control and maintenance of public order through the use of CCTV cameras can be considered a legitimate ground for limiting the right to privacy. However, an overall blanket breach of the right to privacy through CCTV surveillance measures and mass surveillance activities, without any clear legal guidance or limitations and not in accordance with the law, is clearly not proportionate and it is against the rule of law and the values that underline the South African Constitution.

CCTV surveillance and the POPI Act

While international law, common law and the South African Constitution set the standards relating to the right to privacy, the practical implementation of this right, particularly the protection of personal information, is set out in two pieces of legislation – the yet-to-be fully implemented POPI Act of 2013 and its related regulations of 2018.

The POPI Act recognises the right to privacy as enshrined in S 14 of the Constitution and it reflects the State's commitment to respect, protect and fulfil this right. In its preamble, the POPI Act broadens the definition of the right to privacy to include 'a right to protection against the unlawful collection, retention, dissemination and use of personal information.' The Act seeks to promote the protection of personal information processed by public and private bodies and to introduce conditions that constitute the minimum requirement for processing personal information.[35] The Act also establishes the office of the Information Regulator to administer the Act by, among other things, issuing codes of conduct, providing for the rights of persons regarding unsolicited electronic communications and automated decision-making, as well as regulating the flow of personal information across South African borders.[36]

This paper, however, focuses on CCTV surveillance and the right to privacy in view of the minimum conditions for lawful processing of personal information as outlined in Chapter 3 of the POPI Act. The subject matter raises several questions. To what extent is CCTV surveillance an issue in South Africa? Is CCTV surveillance a threat to privacy? Is it reasonable to expect privacy in public spaces? How about CCTV at workplaces, and in private spaces and homes? What would be the legal position regarding privacy where CCTV is used in private residences and workplaces? And as the POPI Act relates mainly to the protection of personal information, does CCTV surveillance violate or interfere with personal information and under what circumstances? A cross-cutting question: To what extent do these conditions meet the standards set in international law? In regulating CCTV systems, these are some of the questions the Information Regulator would need to deal with and give direction to responsible parties.

CCTV surveillance systems and the protection of personal information

The first question would be to address whether information captured and stored through CCTV systems constitutes personal information, the collection of which would constitute interference with the right to privacy. A CCTV camera surveillance system comprises cameras, links between the cameras and monitors, video equipment, a control room, a control-room monitoring system, an information storage system and an evidence control system. When surveillance is in a public space, the common law position in South Africa is that there is no reasonable expectation of privacy in public spaces. However, when such a CCTV camera surveillance system collects, processes and stores personal information, then it triggers the risk of exposing private personal information that could harm the reputation and image of the subjects of that information.

The definition of personal information under the impending POPI Act makes video footage that has been recorded, processed and stored via CCTV camera surveillance systems personal data. The POPI Act defines personal information as 'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.'[37] The Act provides a list of identifiers, such as information relating to race, gender, sex, pregnancy, marital status, national/ethnic/social origin, colour, sexual orientation and age. This is in line with the Data Protection Act in the United Kingdom and Ireland and the European Union's General Data Protection Regulation (GDPR), which view storing recorded security footage the same as storing personal data.[38] What this means is that every owner of a CCTV system in South Africa that collects and stores information that has these elements is considered a responsible party.[39] That comes with responsibilities under the POPI Act and these are encapsulated in the eight conditions in Chapter 3 of the Act.

Legality: POPI Act introduces lawful interference to privacy rights

Legality constitutes the first condition for the lawful processing of personal information under the POPI Act. In the South African context, this will be done retrospectively and prospectively. With respect to retrospective compliance, the POPI Act states that 'All processing of personal information must within one year after the commencement of this section be made to conform to this Act.'[40] Any new responsible parties would be obliged to ensure that the conditions for lawful processing of

personal information set out in Chapter 3 of the Act 'are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.'[41]

The POPI Act also places the data subject[42] at the centre of information processing. First, the Act carries a consent clause which, among other things, stipulates that personal information may only be processed with the consent of the data subject, or where the data subject is a minor, the consent of a competent person.[43] Further, in Section 11(2) (a) of the Act, 'The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection (1) (a).' There is nothing in the POPI Act or its regulations to indicate the minimum requirement of proof that a CCTV surveillance system has met the consensual requirement for processing personal information. There is also no specific policy defining the code of practice for CCTV camera surveillance in South Africa. In addition, considering that CCTV surveillance is a method of mass surveillance, it is not clear what the minimum threshold is for the Information Regulator to determine that the required data subject's consent has been granted. The Information Regulator will need to come up with the minimum acceptable standard of acceptable proof.

In the absence of such policy guidelines, companies such as Vumacam, a private company installing CCTV surveillance cameras in the northern suburbs of Johannesburg, have developed their own interpretation of consent. When asked about the need for consent, Vumacam Managing Director Ashleigh Perry was quoted as saying, 'It's not necessarily about consent, it's about abiding by the regulations.'[44] From a legal point of view, this can be problematic. It is imperative that if the CCTV surveillance systems are installed to protect the public, then the public should be duly consulted, their prior consent should be obtained and they should have a say in the developments that affect their rights.

Necessity and proportionality vis-à-vis CCTV surveillance in South Africa

Section 36 of the South African Constitution stipulates that the rights contained in the Bill of Rights must be limited only in terms of the law of general application and to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. The purpose specification condition in Chapter 13 of the POPI Act seems to apply in relation to CCTV surveillance.

The POPI Act stipulates that 'Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.'[45] In the case of CCTV surveillance, such surveillance should not be conducted in an indiscriminate manner. It must be legitimate, lawful and necessary and must also pass the limitation test like any other ground of limitation of fundamental rights in a democratic state.[46] There are two elements that the Information Regulator will have to determine in this respect.

The first relates to the requirement that the purpose of processing personal information must be related to a function or activity of the responsible party. Consider, for example, Vumacam. The company is a subsidiary of a fibre company that has decided to venture into installing CCTV cameras, mostly in wealthy suburbs, in order to sell footage to security companies who in turn pass the costs to consumers. Vumacam is not registered as a security company under PSIRA. One could argue therefore that the collection of personal information is not related to a function or activity of the company. Does this, therefore, disqualify Vumacam from collecting and storing personal information? The Information Regulator will need to give clear policy direction in such instances.

The second aspect is related to the long-standing legal principles of necessity and proportionality. The concept in the South African Constitution and in international law that the limitation of a right contained in the Bill of Rights, such as the right to privacy, must be 'necessary in a democratic society' means that the State must not only demonstrate that the limitation meets a 'pressing social need' but also, is proportionate to the legitimate aim pursued.[47] In South Africa, as in other

jurisdictions, the general objective of installing CCTV is public safety and security. But in South Africa, more emphasis is placed on CCTV surveillance for crime prevention and personal/communal security. Considering the high levels of crime in South Africa, one could say crime reduction is a pressing social need. There is a strong but untested belief among policymakers, private security companies and marketers of CCTV camera technologies that CCTV can detect, deter and even prevent crime which is seen as creating a multiplier effect on policing resources.[48]

However, while it may be necessary, the use of CCTV surveillance must be proportionate to the legitimate aim pursued. The proportionality test means that there must be a logical link between the measure (CCTV surveillance) and the intended objective (crime prevention and safety) invoked for limiting the right to privacy.[49] It stands to reason therefore that a proportionality test would mean that a measure that is ineffective in achieving the objective cannot be said to be necessary and proportionate. When it comes to CCTV, the often-stated objectives of using it are not directly linked to its efficacy. According to Minnaar, the impact and effectiveness of CCTV in preventing crime, public buy-in and operational and policing imperatives are largely under-researched[50] and do not appear to be a key consideration in the process of rolling out CCTV.[51]

Empirical research worldwide, including in South Africa, presents reservations on the logical links between CCTV and crime prevention. For example, a systematic and meta-analysis of CCTV's efficacy in crime prevention in the United Kingdom and the United States found that CCTV caused a modest 16% decrease in crime largely driven by its effectiveness in car parks.[52] This research only found one attempt at an empirical assessment of CCTV effectiveness in South Africa. This was undertaken in Benoni by the Civilian Secretariat for Police[53] in 1995–1996. Although there were challenges with the methodology, the evaluation found that priority crimes had decreased by 8.8% in the CBD where the CCTV camera system had been installed but that crime elsewhere in Benoni increased significantly by 46%, illustrating displacement of crime.[54] Crimes such as break-ins into private homes, and business and car theft went down. This points to the fact that CCTV is not a silver bullet. It works in some contexts and on some categories of crime, and not others.

One could also add the cost-effectiveness to the proportionality test. The operationalisation and maintenance of CCTV cameras comes at great cost to public authorities and the taxpayer. Municipalities are setting aside significant budgets for the installation of CCTV. For example, of the R524 million allocated to the Tshwane Metropolitan Police Department (TMPD) in 2019, R18.4 million was allocated to the expansion of the coverage and range of CCTV cameras around the city.[55] Similarly, in the City of Cape Town, a capital budget of R7.561 million was allocated in 2019–2020 for XXXXXX.[56]

Public-private partnerships and the commercialisation of CCTV surveillance

The Information Regulator will need to closely monitor the role of the private sector in CCTV camera surveillance which includes the use of drones and body-worn cameras. As observed above, CCTV expansion in South Africa is driven by the private sector through public-private partnerships, particularly by private security companies and insurance companies. While crime prevention and public safety are touted as the principal motives for the expansion, the often-muted profit motive can be a significant ethical issue that will require scrutiny in order to avoid excessive and unwarranted surveillance of individuals.

Advertisements for CCTV surveillance lure clients by pitching an argument that CCTV surveillance's security and deterrence effect reduces the risk of theft and reduces business insurance costs. This is based on the mantra that the fewer insurance claims made by businesses and individuals, the more profit the insurers will make. This motive must be factored into impact assessments to ensure that CCTV surveillance does not open up a scramble for profit while unnecessarily interfering with fundamental human rights, such as the right to privacy.

The CCTV surveillance for profit argument must however be balanced with the fact that the funding and expansion of CCTV surveillance is part of what Minnaar calls 'outsourcing by default' which has been beneficial to the SAPS. Additional resources for crime-fighting have been provided to the SAPS without the financial burden of running and installing them.[57] The expansion of this service in an increasingly competitive market will provide challenges in the implementation of the POPI Act. Clear guidelines will have to be provided on how to balance crime detection and deterrence with the protection of citizens' privacy rights. Profits will need to be measured in terms of the general social good coming out of such surveillance systems.

Accountability and the right to a remedy

As the old Roman legal maxim states, where there is a right, there is a remedy.[58] Accountability of the private sector engaged in surveillance practices is currently a major concern. This is because most surveillance practices, including CCTV camera surveillance, are conducted by the private sector. Yet, international human rights instruments do not hold private corporations legally liable to protect, promote and respect the recognised and protected rights of individuals, including the digital right to privacy.

The State is the primary duty bearer under international law and it is the sole responsibility of the individual State to ensure that the rule of law is upheld within their terrain. States Parties to the ICCPR, for instance, are expected to formulate adequate laws to regulate and control the activities of private corporations. They have the obligation to ensure that private corporations abide by the law and are held accountable for their breaches of fundamental rights under domestic law.

The UN's guiding principles on business and human rights implement the UN framework of 'protect, respect and remedy'. They recognise that private corporations have a responsibility to respect human rights, the state has a duty to protect them, and the individual must have access to a remedy if their rights have been infringed upon.[59] However, these are merely guidelines that States may refer to for guidance and they are not legally bound by them.

In South Africa Section 8(2) of the Constitution states that private corporations can be held liable for breach of human rights principles. However, according to Meyersfield and Nyembe, in practice this provision is underutilised.[60] The constitutional court in the case of *Governing Body of the Juma Masjid Primary School and Others v Essay N.O. and Others*[61] confirmed that private parties have a negative obligation in relation to human rights, that is, the obligation not to interfere with or obstruct the realisation of human rights. In addition, the Companies Act under Section 7(a)[62] stresses that the purpose of the Act is to promote compliance with the Bill of Rights enshrined in the Constitution of South Africa. Based on the above, in general, the law legally makes it possible for private corporations to be held accountable for their human rights breaches.

In the context of digital privacy, under Section 8 of the POPI Act, the public and private corporations dealing with personal data are held accountable. The Act uses the consent of the data owners as the primary tool and prescribes that collection, transfer as well as storage of data only be conducted in accordance with the prescribed eight conditions in Chapter 3 of the Act. Failure to adhere to the law will result in the company facing severe penalties. The Act has put adequate safeguards in place to ensure the protection of information privacy by both public and private corporations. Section 18 of the Act, which can be referred to as the notification clause, plays a critical role in securing the right to a remedy as stipulated in S 34 of the South African Constitution and under Article 2(3) of the ICCPR. The notification clause requires that when processing personal information, the responsible party must 'take reasonably practicable steps' to ensure that the data subject is aware of the information being collected. In addition, the data subject must know the source of the data, the name and contact details of the responsible party, the purpose for which it is being collected, the particular law that authorises or requires the collection of such information and whether the responsible party intends to transfer the information to a third country or international organisation and the level of protection of that information.[63]

This is an important requirement for the protection of personal information because if an individual does not know who is collecting their personal information, they may not have the wherewithal to have inaccuracies corrected or request the deletion of that information as stipulated in Section 24 of the POPI Act. In accordance with the above, it is the responsibility of the Information Regulator to ensure that public and private bodies engaged in CCTV surveillance practices are compliant with the POPI Act and that proper checks must be conducted in such companies as soon as the Act comes into effect.

Lessons from the United Kingdom CCTV camera surveillance legal framework

In jurisdictions such as the EU and the UK (with arguably the highest per capita surveillance apparatus in the world), there are clear rules and regulations regarding when, how, where and for what purpose it is justifiable to use CCTV surveillance to maintain national security.

In the UK, CCTV camera surveillance regulation is a collaborative process managed through three pieces of legislation: the Data Protection Act of 1998, the Regulation of Investigatory Powers Act of 2000 and the Protection of Freedoms Act of 2012. The Regulation of Investigatory Powers Act (RIPA) covers covert surveillance and is not comparable with the POPI Act in respect of transparency and accountability requirements. The Protection of Freedoms Act of 2012 created the office of the Surveillance Camera Commissioner whose role is to encourage voluntary compliance with the Surveillance Camera Code of Practice (SCOOP) of 2013.

The mandate of SCOOP is to balance CCTV needs with society's right to privacy. It was developed to address concerns of potential abuse or misuse of surveillance by the State in public spaces. Failure to comply with SCOOP does not make the responsible party liable to criminal or civil proceedings but the code is admissible as evidence in criminal proceedings and a court or tribunal may take into consideration the failure by a relevant authority to take regard of the code in determining liability in such proceedings.

On the other hand, the Data Protection Act created the office of the Information Commissioner whose duty is to uphold information rights by all sectors in the public interest. This entails upholding the lawful processing and protection of personal information collected through technology, such as automated number plate recognition (ANPR), body-worn video (BWV), drones or unmanned aerial systems (UAS) and other systems that capture information of identifiable individuals or information relating to individuals.[64] The Information Commissioner has the power to investigate complaints by individuals about interference with their information rights, as well as the power of enforcement. This includes issuing penalties for failing to comply or breaching a code of practice set out in the CCTV Code of Practice. The Code is titled *In the picture: A data protection code of practice for surveillance cameras and personal information*. Thus, the two commissioners manage two overlapping aspects of CCTV surveillance.

In the South African context, the Information Regulator under the POPI Act occupies both roles (Surveillance Camera Commissioner and Information Regulator). Unlike SCOOP, compliance with the POPI Act will be mandatory; but the Information Regulator's mandate will be similar to that of the Information Commissioner under the Data Protection Act.

The Data Protection Act grants the individual liberty to access, see and consent to the information held about them, including images captured by the CCTV or images which give away information about them, such as their car number plate. It also provides guidelines or a set of rules which CCTV operators must follow when they gather, store and release CCTV images of individuals. The Information Commissioner can enforce these rules. The guidelines on the installation of CCTV prescribe that the public be notified that they are under surveillance. The rollout should be conducted after a privacy impact assessment has been conducted and published. The recordings must also not be kept longer than necessary which is not more than 31 days. The Freedom of

Information Act (FIA) allows the public to request official information by writing to the public authority, who must respond within 20 working days.

The above discussion highlights what is absent in the South African context. There is no coordination between the laws that regulate surveillance; there is no mention of a CCTV code of practice even in the POPI Act; there are no legal provisions ensuring a balance is maintained between the need for CCTV camera surveillance and the right to privacy; CCTV cameras in South Africa continue to be installed without privacy assessments being done beforehand; neither public opinion nor participation is allowed in the rollout of CCTV measures, yet the purpose is to protect the public.

6. LOOKING AHEAD: OPTIONS ANALYSIS

In view of the preceding discussion and analysis, the impending full implementation of the POPI Act will require a well-calculated phase-in period to address potential grey areas in ensuring that existing CCTV surveillance systems are legalised to effectively serve a legitimate and necessary purpose in South Africa.

The POPI Act sets out the conditions for lawful processing of information and the powers and functions of the Information Regulator in enforcing this law. It also provides regulations that detail the administrative processes for the enforcement of the Act. However, there remain grey areas such as policies, guidelines or codes of practice to standardise practice with respect to the processing of personal information through specific technologies, such as overt CCTV surveillance. Without such guidance, stakeholders will be left to implement the law in the way that they understand it, resulting in several, perhaps contradictory, practices. This requires the Information Regulator to take practical steps to ensure that directives are standardised and ready for when the POPI Act is fully implemented.

In respect of CCTV surveillance, the Information Regulator must ensure that there is a standard code of practice that every public and private body using the technology must adhere to. The United Kingdom model is a good example to follow in terms of the aspects it covers. The first aspect deals with best practices in terms of installing CCTV systems in public spaces using standards that recognise the need for reasonable expectation of privacy, comparable to locational privacy, to allow people to go about their business without feeling watched at all times. The second aspect covers the protection of personal information from potential abuse by private and public authorities that harvest, store and process it.

The POPI Act provides a strong protection of information element but it is not clear whether the Information Regulator will develop and enforce specific standards for deploying surveillance cameras in public spaces. In order to ensure compliance with the POPI Act when it is finally fully implemented, the Information Regulator will need to take a broad approach to issue standards and guidelines. Some of the areas of focus should include, but are not limited to the following:

- Guidelines regarding acceptable standards for installing surveillance camera systems in public spaces, workplaces and private homes. Such guidelines should not be to prohibit CCTV surveillance usage, but to set acceptable standards for deploying the technology in order to balance privacy rights and public safety and security imperatives.
- Codes of practice for lawful processing of personal information collected and stored through CCTV camera surveillance. The codes of practice must be broad and include best practices for use of other surveillance technologies, such as police body-worn cameras, drones (unmanned aerial systems) and any other camera surveillance systems. These codes of practice must be continually reviewed and updated as new technology emerges.

- With the convergence of technologies, the Information Regulator should issue separate guidelines for the use of software that can be installed on the cameras, such as facial recognition software (FRS), license plate recognition (LPR) software and any other software that further interferes with individual privacy. Such guidelines must precisely stipulate the circumstances under which the use of such technologies is lawful.

The cross-cutting issue with all the codes of practice and guidelines would be the need for them to be congruent with the Constitution, international law and the principles of personal protection under the POPI Act. To ensure transparency and accountability, the development of these guidelines and codes of practice must have a strong component of meaningful public awareness and participation in their formulation and in the rollout of such measures. Privacy assessment impacts should be published or made available to the public for transparency purposes. These codes of practice must be in place from the onset of the full enactment of the POPI Act to ensure that in the first year, public and private authorities have sufficient guidelines to achieve full compliance.

ENDNOTES

1 J Duncan (2019) UJ's Prof. Duncan explores how CCTV surveillance poses threat to privacy in South Africa. Available at: https://www.uj.ac.za/newandevents/Pages/uj-prof-jane-duncan-explores-how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa.aspx [accessed on 16 July 2018]; B Whitfield (25 February 2019) Vumacam MD insists private CCTV video feed across are in line with the law. Available at: http://www.702.co.za/articles/339123/vumacam-md-insists-private-cctv-video-feeds-across-jozi-are-in-line-with-the-law.

2 A Minnaar (2012) Private security companies, neighbourhood watches and the use of CCTV surveillance in residential neighbourhoods: the case of Pretoria East, *Acta Criminologica: Southern African Journal of Criminology,* Special Edition 1, 2012, 104.

3 Ibid., 103.

4 With increasing robberies in shopping centres and malls in 2008, the Consumer Goods Council of South Africa encouraged shopping centre managements to install CCTV camera surveillance systems throughout their hallways and adjacent car parks as part of an integrated security measures at shopping centres.

5 PSIRA (2019) *PSIRA security equipment satisfactory survey report*, p. 22. Available at: https://www.psira.co.za/psira/dmdocuments/research/PSIRA%20Integrated%20Security%20Equipment%20Report_March%202019.pdf [accessed on 26 August 2019].

6 L van Jaarsveld & A Minnaar (2012) Managing safety and security in schools – a case study from Tshwane, South Africa, in *Acta Criminologica: Southern African Journal of Criminology*, Special Edition 2, 2012, 129.

7 SANRAL (2018) Integrated report Volume 1, p. 37. Available at: https://www.nra.co.za/content/SANRAL_Integrated%20Report%202018_Volume-1-29-August-2018.pdf.

8 L Engelbrecht (2008) SANRAL camera project winds up. Available at: https://www.itweb.co.za/content/wbrpO7gzVA9vDLZn.

9 A Gorpi (2018) 'Big Brother' watching: cameras monitor highways. Available at: https://www.iol.co.za/ios/news/big-brother-watching-cameras-monitor-highways-14939633 [accessed on 8 June 2018].

10 SANRAL (2017) SANRAL cameras monitor road safety in severe winter storm. Available at: https://stop-over.co.za/sanral-cameras-monitor-road-safety-severe-winter-storm/ [accessed on 17 July 2019].

11 City of Cape Town (2010) Integrated Rapid Transport Pack. Available at: http://www.cityenergy.org.za/uploads/resource_202.pdf [accessed on 14 July 2019].

12 H Swart, (2018) Controlling Cape Town: the real costs of CCTV cameras and what you need to know. Available at: https://www.dailymaverick.co.za/article/2018-10-05-controlling-cape-town-the-real-costs-of-cctv-cameras-and-what-you-need-to-know/ [accessed on 14 July 2018]. This number excludes CCTV camera systems installed by other operators, like private security companies, Business Against Crime South Africa, individuals and any other players.

13 R Moatshe (4 October 2018) Tshwane's CCTV system 'still operational'. Available at: https://www.iol.co.za/pretoria-news/tshwanes-cctv-system-is-still-operational-17347303 [accessed on 4 October 2018].

14 L Ngobeni (May 27 2019) Half a billion to fight crime in Tshwane. Available at: https://rekordeast.co.za/207849/half-a-billion-to-fight-crime/.

15 Businesstech (23 July 2018) Joburg is getting new CCTV surveillance cameras. Available at: https://businesstech.co.za/news/business/260151/joburg-is-getting-new-cctv-surveillance-cameras/.

16 A Minnaar (2012) (n 2 above) p. 107.

17 Ibid.

18 J Duncan (2018) Stopping the spies: constructing and resisting the surveillance state in South Africa. Available at: https://theconversation.com/how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa-97418 [accessed on 26 July 2019].

19 A Lukács (2016) What is privacy? The history and definition of privacy, Available at: http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf [accessed on 19 March 2019] p. 258; see also South African Law Reform Commission (2005) Privacy and data protection, *SALRC discussion paper*, 109, p. 12. Available at: http://www.justice.gov.za/salrc/dpapers/dp109.pdf [accessed on 13 August 2019].

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

21 Article 17, International Covenant on Civil and Political Rights.

22 Human Rights Committee, General Comment No. 16, 1988. Also refer to Global Partners Digital (2018) *Travel guide to the digital world: data protection for human rights defenders.* London: Global Partners Digital, p. 39. Available at: https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf.

23 S Warren & L Brandeis (1890) The right to privacy, *Harvard Law Review*, 4:5, 195.

24 Ibid.

25 D Solove (2006) A brief history of information privacy law, GWU Law School Public Law Research Paper, 215, 6. Available at: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

26 A Lukács, (2016) (n 19 above), pp. 259–260.

27 C van der Bank (2012) The right to privacy: South African and comparative perspectives, *European Journal of Business* Sciences, 1:6, 77.

28 Y Burns (2001) *Communications law*, Durban: Butterworths, p. 3.

29 T Balule & B Otlhogile (2015) Balancing the right to privacy and the public interest: surveillance by the State of private communications for law enforcement in Botswana, *Statute Law Review*, 37:1, 19–32.

30 Ibid., 20.

31 Ibid.

32 J Duncan (2019) UJ's Prof Duncan explores how CCTV surveillance poses threat to privacy in South Africa, p. 142. Available at: https://www.uj.ac.za/newandevents/Pages/uj-prof-jane-duncan-explores-how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa.aspx [accessed on 16 July 2018].

33 Constitution of the Republic of South Africa (1996) Section 233.

34 *Government of South Africa v Grootboom* [2000] 11 BCLR 1169 (CC), 26.

35 The *Conditions for lawful Processing of Personal Information* are outlined in Chapter 3 of the Protection of Personal Information Act 4 of 2013.

36 Protection of Personal Information Act 4 of 2013.

37 Protection of Personal Information Act 4 of 2013, Definitions.

38 Data Protection Act, 1998.

39 The POPI Act defines a responsible party as 'a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information'.

40 POPI Act, Section 114(1).

41 POPI Act, Section 8.

42 The POPI Act defines the data subject as the person to whom personal information relates.

43 POPI Act, Section 11(1)(a).

44 B Whitfield (25 February 2019) Vumacam MD insists private CCTV video feed across are in line with the law. Available at: http://www.702.co.za/articles/339123/vumacam-md-insists-private-cctv-video-feeds-across-jozi-are-in-line-with-the-law.

45 POPI Act, Section 13(1).

46 *Digital Rights Ireland v Seitlingerv.* Minister for communications, marine and natural resources C-293/12 and C594/12 CURIA (2014).

47 Electronic Frontier Foundation & Article 19 (2014) Necessary and proportionate: international principles on the application of human rights law to communications surveillance, p. 44. Available at: https://www.article19.org/data/files/medialibrary/37564/N&P-analysis-2-final.pdf [accessed on 1 October 2019].

48 R Moatshe (2018) (n 13 above).

49 Electronic Frontier Foundation & Article 19 (2014) (n 47 above) p. 23.

50 The Civilian Secretariat for Police undertook a study to evaluate CCTV as a means of crime control. See L Ganz et al. (2008) An assessment of closed circuit television surveillance with reference to the Benoni project. Available at: http://www.policesecretariat.gov.za/downloads/reports/cctv.pdf [accessed on 16 July 2019].

51 A Minnaar (2012) (n 2 above) p. 103.

52 B Welsh & D Farrington (2009) Public area CCTV and crime prevention: an updated systematic review and meta-analysis, *Justice Quarterly*, 26:4, 716.

53 The Civilian Secretariat for Police is a South African constitutional body which performs advisory functions to the Minister of Police on various matters including but not limited to, departmental policy and strategy, legislation, police performance through conducting audits, communication, community mobilisation on crime prevention, the Integrated Justice System and international obligations and liaison. Refer to: www.policesecretariat.gov.za.

54 L Ganz et al. (2008) (n 50 above), p. 3.

55 L Ngobeni (May 27, 2019) (n 14 above).

56 Insert endnote

57 A Minnaar (2004) Crime prevention, partnership policing and the growth of private security: the South African experience. In G Mesko, M Pagon & B Dobovsek (eds) *Policing in central and eastern Europe*, Maribor: University of Maribor, p. 13. Available at: https://www.ncjrs.gov/pdffiles1/

nij/Mesko/207977.pdf [accessed on 3 July 2019].

58 See https://www.oxfordreference.com/view/10.1093/oi/authority.20110803110448446.

59 UNHRC (2008) Protect, respect and remedy: a framework for business and human rights A/HRC/8/5, p 3.

60 B Meyersfeld & N Nyembe (2016) Submission on the legal framework for corporate accountability, In the Marikana Commission of Inquiry, Pretoria. Johannesburg: Centre for Applied Legal Studies, p. 11.

61 *Governing Body of the Juma Masjid Primary School and Others v Essay N.O. and Others* [2011] (CCT 29/10) ZACC 13.

62 Companies Act 71 of 2008.

63 POPI Act, Section 18(b)-(g).

64 Information Commissioner (2008) In the picture: a data protection code of practice for surveillance cameras and personal information. Available at: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf.

65. This includes the Judicial Inspectorate for Correctional Services (JICS) and the Independent Correctional Centre Visitors (Melanie Lue Dugmore, Independent monitoring of police detention facilities in South Africa, APCOF Research Paper 20, January 2018, 12–13).

66. Lue Dugmore (note 2).

67. SAHRC, Media alert: SAHRC to host a breakfast seminar on the National Preventive Mechanism (NPM), 24 April 2019, https://www.sahrc.org.za/index.php/sahrc-media/news-2/item/1868-media-alert-sahrc-to-host-a-breakfast-seminar-on-the-national-preventive-mechanism-npm.

68. Ibid.; African New Agency, SAHRC welcomes ratification of UN torture agreement, *The Citizen*, 4 March 2019, https://citizen.co.za/news/south-africa/government/2095273/sahrc-welcomes-ratification-of-un-torture-agreement/.

69. SAPS, Annual Report 2015–16, 108; SAPS, Annual Report 2017–18, 102.

70. SAPS, Annual Report 2015–16, 117; SAPS, Annual Report 2017–18, 89 and 112.

NOTES

ABOUT THE AUTHORS

Dorcas Basimanyane

XXXX

Dumisani Gandhi

XXXX

ABOUT APCOF

The African Policing Civilian Oversight Forum
Building 23B, Unit 16
The Waverley Business Park
Wyecroft Road, Mowbray 7925
South Africa

Tel: +27 21 447 2415
Fax: +27 21 447 1691
Email: info@apcof.org.za
Web: www.apcof.org.za
Twitter: @APCOF
Facebook: African Policing Civilian Oversight Forum

This publication is No. 27 in the APCOF Research Series, each of which comprises a Research Paper, a Policy Brief and a Press Release. For these and other publications, please visit ***www.apcof.org.za****.*

Produced by COMPRESS.dsl | www.compressdsl.com

www.apcof.org.za