COLLATERAL INTRUSION: SAFEGUARDING PRIVACY IN AN AGE OF SURVEILLANCE

GUIDELINES FOR SOUTH AFRICA'S INFORMATION REGULATOR

Melissa Cawthra

APCOF
RESEARCH PAPER
SERIES 29
SEPTEMBER 2020

APCOF **RESEARCH SERIES** 2020

COLLATERAL INTRUSION: SAFEGUARDING PRIVACY IN AN AGE OF SURVEILLANCE

GUIDELINES FOR SOUTH AFRICA'S INFORMATION REGULATOR

Melissa Cawthra

SEPTEMBER 2020

#29

APCOF **RESEARCH PAPER** 2020

This publication is No. 29 in the APCOF Research Series. For these and other publications, please visit www.apcof.org.za.

ISBN: 978-1-928332-64-0

African Policing Civilian Oversight Forum (APCOF)
Building 23B, Suite 16
The Waverley Business Park
Wyecroft Road
Mowbray, 7925
Cape Town, ZA

Tel: +27 21 447 2415
Fax: +27 21 447 1691
Email: info@apcof.org.za
Web: www.apcof.org.za

Designed, typeset and proofread by COMPRESS.dsl | www.compressdsl.com

Contents

INTRODUCTION

> *The spread of the internet and new communications methods has increased the intrusiveness of surveillance as well as its power. It's now technically possible to monitor entire groups and nations on a mass scale, systematically and relatively cheaply. This poses a fundamental threat to individuals [sic] security, civil society, human rights, as well as democracy itself […] Even in political systems with significant checks and balances, surveillance capabilities have regularly outstripped the ability of laws to effectively regulate them. In non-democratic and authoritarian countries, surveillance technology can be used for human rights abuses and undermine democratic development and privacy, a human right essential in allowing individuals control, dignity, and the realisation of other human rights such as freedom of expression.*[1]

The above excerpt, from an explainer on the global surveillance industry published by Privacy International, places surveillance at the intersection of security, privacy and human rights; and it is this nexus that this paper seeks to explore. The passage also illustrates the far-reaching threats and risks – to individuals and societies at large – of weak or ineffective regulation of State and non-State surveillance operators, and highlights the pressing need for legislation and accountability and oversight mechanisms to uphold the right to privacy and other fundamental human rights.

Surveillance systems in South Africa are increasingly affordable and widely used, and while they can be useful tools in preventing, detecting and investigating crimes, adequate oversight and safeguards must be in place to protect constitutional rights and ensure that surveillance operators remain accountable. At present, there are no laws specifically regulating the use of surveillance technologies, nor is there any coordination between the various pieces of legislation relating to privacy and surveillance. In addition, guidelines on the collection, processing and storage of personal information by surveillance operators are non-existent.

The anticipated coming into force of South Africa's Protection of Personal Information Act[2] (POPIA) is timely and topical, as this piece of legislation provides an opportunity to craft guidelines on the protection of personally identifiable or potentially sensitive information. POPIA was enacted in November 2013 and certain sections of the Act were signed into law by

the President on 1 July 2020.[3] Once it has been gazetted, organisations will have 12 months to comply with its provisions.

This paper sets out evidence-based advice for South Africa's Information Regulator to develop a code of conduct for public and private sector surveillance operators. The task ahead of the Information Regulator is not without precedent: equivalent mandate-holders in a number of countries have developed codes of practice, several of which have been analysed in this research, and which can serve as a useful benchmark for the Information Regulator when drafting its own domestic guidelines.

For the purposes of this paper, 'surveillance' will include communications surveillance, closed-circuit television (CCTV) cameras, drones, body-worn video, automatic number plate recognition, and social media surveillance and big data. The latter category will be treated as a separate sub-section, given its pervasiveness and the scale of the threat that this type of surveillance poses to privacy.

One of the consequences of the information age and the ubiquitous use of online platforms to store and process personal information is the unprecedented volume and richness of data that is stored online, and the potential for this data to be accessed unlawfully and misused. The latest technological advances, such as artificial intelligence (AI), behaviour analytics and machine learning, have multiplied these risks and added an additional layer of complexity to the cyber governance landscape. Given the massive increase in cybercrime and data breaches and leaks,[4] it is clear that data has become a valuable currency, and there is a need to balance the right of freedom of expression and access to information with the right to privacy and security.

At a global level, the Facebook-Cambridge Analytica scandal of 2016 is perhaps the most famous example of the unlawful interception and misappropriation of the personal data of individuals without their knowledge or consent, for the purpose of influencing voter behaviour in the context of the electoral process.[5] Examples such as these illustrate the manner and extent to which big data is fundamentally changing the political and social landscape, and highlight the crucial need for legislation and regulation in the digital space to protect individuals from excessive surveillance, cybercrime and the unauthorised collection, processing and storage of their personal data.

An earlier paper published by APCOF on CCTV surveillance and the right to digital privacy in South Africa noted:

> *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.*[6]

As a follow-up to APCOF's first research paper on this theme, surveillance and personal information will be the lens through which the current research is examined.

The first section sets out the key concepts dealt with in the paper and gives an overview of the legal framework governing surveillance, privacy and the protection of personal information. At the international and regional level, this legislation focuses on physical and digital privacy, and at national level, the focus is on surveillance and the protection of personal information. In this section, surveillance will be conceptualised from the perspective of human rights and accountability, with a discussion on the implications of surveillance for each of these areas.

The next section explores key factors to be taken into consideration by the Information Regulator in drafting a code of conduct for surveillance operators in South Africa. This section includes general and specific guidelines for the implementation of surveillance safeguards and compliance tools. The technologies covered in this section include CCTV cameras, body-worn video, drones, automatic number plate recognition (ANPR), communications surveillance, and social media surveillance and big data. The latter category includes a case study on the weaponisation of data in a well-known global data breach: the Facebook-Cambridge Analytica data scandal. The section ends with a discussion of cross-cutting issues and technologies including AI, behaviour analytics and machine learning; proposes oversight mechanisms and remedies based on the recommendations of the Special Rapporteur on the right to privacy; and outlines challenges relating to the implementation of a surveillance code of conduct.

The paper will then touch on the issue of digital security during the COVID-19 pandemic, which has significantly increased reliance on web-based platforms for communication, with specific reference to the measures announced by the South African government and the Information Regulator under the national state of disaster. It ends with an overview of emerging trends and new or nascent technologies that are gaining traction globally in response to the pandemic; pointing to the rapid rise of the so-called 'health surveillance state'.

CONCEPTUALISING SURVEILLANCE

International legal framework

International human rights law protects the right of all persons against arbitrary or unlawful interference with their privacy, notably in Article 12 of the Universal Declaration of Human Rights, and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Despite these clear legal statements on protection against such interference, there is no single, universally agreed definition of privacy, though attempts have been made to define it by several international legal instruments. According to the tenets of international law, while the right to privacy is not absolute, any instance of interference with privacy must be subject to 'a careful and critical assessment of its necessity, legitimacy and proportionality'.[7]

In December 2013, the United Nations General Assembly adopted Resolution 68/167, in which it expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights, and recalled that 'International human rights law provides the universal framework against which any interference in individual privacy rights must be assessed.'[8] The resolution reaffirmed the right to privacy as expressed in key international treaties and its application to both on- and offline environments, while recognising the symbiotic relationship between development and access to online information and communication technologies. The resolution made various demands on States, including, the extension of privacy rights to digital communications, ensuring consistency between international obligations and national law (including the review and necessary revision of existing laws, practices and procedures), and the establishment of independent oversight mechanisms to ensure transparency and accountability in relation to State communications surveillance and the collection of personal data.

Through the adoption of Resolution 68/167, the General Assembly requested that the High Commissioner for Human Rights prepare a report on the right to privacy in the digital age. The General Assembly, noting with interest the Office for the High Commissioner for Human Rights' (OHCHR) report, called upon all States to respect and protect the right to privacy, and

encouraged the Human Rights Council to consider the possibility of establishing a special procedure to further this aim.

In July 2015, the Human Rights Council appointed a Special Rapporteur on the right to privacy for a period of three years. The Special Rapporteur is an independent expert appointed by the Council to examine and report back on a country situation or a specific human rights theme. The Special Rapporteur is mandated to report on alleged violations of the right to privacy, including in connection with the challenges arising from new technologies. States were called upon to cooperate fully and assist the Special Rapporteur.[9]

Regional legal framework

At regional level, the Declaration of Principles of Freedom of Expression and Access to Information in Africa (the Declaration) was adopted by the African Commission on Human and Peoples' Rights (ACHPR) at its 65th Ordinary Session in Banjul, in November 2019. The Declaration contains 43 principles aimed at providing an authoritative interpretation of Article 9 of the African Charter on Human and Peoples' Rights on access to information and freedom of expression.

A revised declaration was published in April 2020, in the midst of the COVID-19 pandemic.[10] Principles 37 to 43 cover freedom of expression and access to information on the internet: Principle 40 contains provisions on privacy and the protection of personal information; Principle 41 relates to privacy and communications surveillance; and Principle 42 sets out the legal framework for the protection of personal information.

There are also specific provisions with respect to the criminalisation of false news, which has a chilling effect on freedom of expression, and the protection of journalists reporting on the pandemic.[11] Principle 22 of the Declaration calls upon States to repeal laws that criminalise sedition, insult and the publication of false news, and Principle 20 urges States to guarantee the safety, physical and mental well-being of journalists, who should be regarded as essential service workers for the vital role that they play in the COVID-19 crisis.

National legal framework

Surveillance

In South Africa, the covert surveillance activities of public authorities are governed by the Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA)[12] and the Criminal Procedure Act (CPA), and strictly speaking, do not fall within the jurisdiction of POPIA, whose scope is discussed in more detail in the sub-section on personal information, below.

However, there is a growing body of evidence to suggest that the processing of personal data by law enforcement and intelligence agencies under RICA and the CPA is excessive and does not pass the so-called necessity and proportionality test contained in POPIA; meaning, it is not necessary for, or proportionate to, a legitimate aim which it seeks to achieve. For this reason, the question of mass surveillance of cell phone metadata is discussed here. Concerns have also been raised about the unlawful processing of data, the extent of processing, the blanket retention of metadata captured by mass surveillance operations, and the excessive duration of data retention.[13]

A distinction should be made between mass surveillance and targeted surveillance. Targeted surveillance is authorised in the context of criminal investigations, which are technically exempt from the requirements of POPIA. As it stands, police officers are empowered to seize

an individual's communications records from network providers by means of an order or subpoena from the lower courts, through a legal loophole in RICA which allows them to invoke Section 205 of the CPA; thereby circumventing the need to seek permission from a high court or constitutional court judge to access a suspect's call records.[14] Section 205, therefore,

> *serves as a parallel route to access people's communications metadata which bypasses nearly every safeguard or oversight measure built into the RICA Act […] Section 205 of the Criminal Procedure Act allows that a police official of any seniority can request access to a person's communications data, as long as the request is authorised by one of a wide category of prosecutors and even the most junior magistrates.*[15]

The current regulatory framework protects the content of data but not metadata. Metadata is information *about* data, and includes such details as call records, IP addresses, location data and cell phone contact lists. South African cell phone providers are required by RICA to retain the metadata of all subscribers for a minimum of three years for law enforcement purposes; surpassing international norms (averaging one year) by a wide margin.[16] The argument in favour of metadata being less sensitive than data content is questionable, as a large number of metadata points gathered about a data subject – particularly over this period of time – can reveal surprisingly sensitive information and paint a very comprehensive picture of an individual's personal life. There is also a risk that this data can be sold or misused if adequate safeguards are not in place.

Section 205 subpoenas are not restricted to communications data: investigators can invoke this piece of legislation to seek 'bank records, CCTV footage, and all manner of information' held by a third party.[17] This is problematic for several reasons; most notably as the processing of tower records (metadata captured by cell phone towers in dragnet operations) are in violation of the processing limitation principle of POPIA (explained in the sub-section on personal information below), and with respect to the lack of user notification or consent inherent in this mass surveillance practice.

In a landmark ruling in *amaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*, the Gauteng High Court found that the provisions in RICA which allow for the bulk interception activities of the intelligence agencies, and the failure of the police and intelligence services to notify subjects that they had been under surveillance long after an investigation had been completed, are unlawful and unconstitutional. The matter is currently on appeal before the Constitutional Court.

Personal information

The Protection of Personal Information Act (POPIA)

Data privacy is a major concern in South Africa, which ranks third in the world for cybercrime victims.[18] The right to privacy is protected by common law and enshrined in Section 14 of the Constitution, and there is established case law on the privacy of communications, bodily privacy and territorial privacy.[19] POPIA gives effect to this right by putting in place mandatory mechanisms and procedures for the handling and processing of personal information. The purpose of the Act is to 'ensure all South Africans conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise personal information in any way'.[20]

POPIA is in line with international best practice and privacy laws. It is roughly based on the European Union's General Data Protection Regulation (GDPR), which acknowledges that data

protection is a fundamental human right,[21] and the Organisation for Economic Co-operation and Development (OECD) Privacy Principles, and further inspired by models of data privacy from the United States, Canada, Australia and the United Kingdom.

However, South Africa's failure to fully promulgate POPIA and delays in operationalising it have raised concerns both domestically and internationally. In a submission on privacy legislation in South Africa, made in 2017, Privacy International, in association with the Right2Know Campaign, noted its concern 'in light of the requirement under RICA for mandatory SIM card registration, and the introduction in recent years of government backed schemes to collect personal data of individuals, such as using of biometrics for passports and banking.'[22] Similarly, the UN Special Rapporteur on the right to privacy expressed concern at the state of legal protection of the right to privacy in the country, given the failure by the Government to fully operationalise POPIA.[23] During a March 2020 roundtable discussion on the state of privacy in South Africa, he lamented the slow pace of adoption and operationalisation of the legislation, noting that the country is 30 years behind its global counterparts and faces significant challenges with capacity and resourcing of the Office of the Information Regulator; the custodian of POPIA. He urged the Government to promulgate the Act without further delay, and requested an official country visit to South Africa.

Once it finally comes into operation, POPIA will set out the protections and their exemptions, provide for the implementation and enforcement of its provisions, and establish consequences for non-compliance. Each element of the Act is discussed in more detail below.

Protections

The protections under POPIA extend to juristic persons (e.g. companies and trusts) as well as natural persons, which is broader than protections offered in Europe through the GDPR, which only offers protection to natural persons.[24] Under the Act, 'personal information' means information relating to an identifiable natural or juristic person that includes but is not limited to:

> *(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person'.*[25]

This definition is important in the context of surveillance, which involves the collection, processing and storage of data which is designated as sensitive by privacy legislation. Due to its sensitive nature, strict safeguards and protocols need to be in place to guard against its misuse; both in national privacy legislation and in the code of conduct developed to regulate compliance with the legislation by public and private sector surveillance operators.

POPIA presents a set of conditions and principles that prescribe the way in which personal information may be processed. It makes a distinction between *data subjects* and *responsible*

parties. A data subject is the person to whom the personal information relates, and 'whose personal data is being collected, held or processed. Everyone becomes a data subject at some point; for example, when applying for a job, using a credit card or simply by browsing the Internet, individuals necessarily disclose some personal information'.[26] A responsible party refers to 'a public or private body or any other person which, alone or in conjunction with others, determines the purpose and means of processing personal information'.[27]

Broadly speaking, the Act is based on the following eight principles,[28] with which the responsible party is required to comply:

1. accountability;
2. processing limitation;
3. purpose specification;
4. further processing limitation;
5. information quality;
6. openness;
7. security safeguards; and
8. data subject participation.[29]

Exemptions

The Act sets out specific instances where responsible parties may be granted an exemption to process personal information. These exemptions must be published by the Information Regulator, by notice in the *Government Gazette*. In these instances, the public interest is deemed to outweigh, 'to a substantial degree,'[30] the right to privacy. This includes processing for 'journalistic, literary or artistic purposes'[31] and processing by 'bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law'[32] for activities relating to national security (such as criminal investigations, or terrorist and related activities). The current national state of disaster, discussed in the following section, is another example of a situation in which exemptions may apply.

Implementation and enforcement

An Information Regulator is appointed to monitor and enforce compliance by public and private bodies with the provisions of POPIA. Data subjects will be able to complain to the Information Regulator, who is empowered to take action on their behalf. The Information Regulator is granted extensive powers to investigate and fine responsible parties. The Regulator reports to Parliament.

Consequences of non-compliance

In the event of data loss or breach, it is incumbent upon the responsible party to first inform the Information Regulator, and then inform every data subject who may have been affected. In addition to the risk of reputational damage, non-compliance with the Act will incur penalties, ranging from civil claims to fines of up to R10 million or 10 years in jail per incident.[33]

Implications of surveillance for human rights and accountability

Any discussion of the implications of surveillance on human rights and accountability should necessarily focus on the bigger picture. On this matter, cyber-policy expert Paul Bernal notes:

> *The nature and depth of internet surveillance has been revealed to be very different from what had previously been publically acknowledged or politically debated. There are critical ways in which the current debate is miscast, misleading and confused. Privacy is portrayed as an individual right, in opposition to a collective need for security. Data gathering and surveillance are portrayed as having an impact only on this individual right to privacy, rather than on a broad spectrum of rights, including freedom of expression, of assembly and association, the prohibition of discrimination and more […] The impact of data gathering and surveillance is often portrayed as happening only at [sic] when data are examined by humans rather than when gathered, or when examined algorithmically. Commercial and governmental data gathering and surveillance are treated as separate and different, rather than intrinsically and inextricably linked. This miscasting has critical implications. When the debate is recast taking into account these misunderstandings, the bar for the justification of surveillance is raised and a new balance needs to be found, in political debate, in law, and in decision-making on the ground.*[34]

Human rights

Surveillance, while infringing upon the individual right to privacy, can be seen as a form a social control in that it encourages self-censorship and threatens to undermine fundamental human rights such as freedom of expression, assembly and association. This applies to online (digital) as well as physical or locational surveillance. Examples of self-censorship include individuals restricting and controlling what they share online for fear of interception or reprisal; or deciding against attending political, social or religious gatherings for fear that their activities may tracked or monitored via social networks, cell phone surveillance, cell phone location monitoring, or CCTV cameras installed in public spaces. Surveillance also poses a potential threat to the human right to freedom from discrimination, through facial recognition technology and predictive policing software, whose algorithms have the potential to enforce and perpetuate existing biases.

Accountability

With respect to accountability, surveillance raises important concerns around necessity and proportionality. This is particularly relevant in the context of indiscriminate mass surveillance conducted by governments – even in democratic regimes.

To determine whether the use of a surveillance system or activity is justified, it must be necessary and proportionate to the purpose that it seeks to achieve. A distinction should be made here between targeted surveillance of individuals (for instance, in the context of preventing, detecting and investigating crime) and indiscriminate mass surveillance of large sections of the civilian population, which is discussed in greater detail in the following section of this paper.

The discussion around surveillance has typically focused on surveillance for control purposes in the case of misconduct, in order to establish 'whether control mechanisms cause a disproportionate damage to individual freedom as compared with the need for preventing and controlling crime'.[35] However, the scope of analysis should be expanded to include

surveillance for prevention purposes, or where 'the extent to which surveillance causes a breach of privacy, one should evaluate the effects resulting from the widespread use of surveillance as regards citizens' freedom of movement and behaviour'.[36] This ties in with the human rights concerns mentioned above regarding self-censorship and social control, and raises key questions for accountability, with respect to the extent to which surveillance is justified, necessary and proportionate. On this point, Buttarelli notes, 'the public as a whole should not suffer excessive limitations on account of the need to prevent the misbehaviour of a minority.'[37]

Surveillance also raises questions regarding knowledge and consent as, in many cases, user notifications informing individuals that they are being monitored or recorded are lacking, or privacy policies are absent or so vaguely or technically worded as to render them meaningless to the general population.

Another accountability concern is the issue of data processing and storage – where the extent of processing and the storage retention period frequently exceed the initial intended purpose, or retention periods are simply not specified or codified. Lastly, there is the pressing matter of legal accountability. As mentioned previously, there are no laws specifically regulating the use of surveillance technologies by State and non-State actors in South Africa, and grey areas exist as far as oversight and regulation of the private security industry are concerned. Another major challenge is that the pace of technological innovation frequently outstrips the pace of the law. These two broad areas of concern – human rights and accountability – are the focal points of the recommendations to the Information Regulator, which are outlined below.

CONSIDERATIONS FOR THE INFORMATION REGULATOR

Section 40(1)(f)(ii) and Section 65 of POPIA require that the Regulator develop guidelines to assist affected persons and stakeholders to develop or to apply for the approval of codes of conduct.[38]

In its guidelines on POPIA compliance for South African law firms, the Law Society of South Africa notes that the overall responsibility of the Information Regulator is multi-faceted, and the protection of personal information is novel jurisprudence. In light of this, and given the pervasiveness of information and the rapidly changing landscape with regard to the processing of personal information, the Regulator will need to adopt a flexible approach, while still establishing legal certainty wherever possible.[39]

This section sets out some of the key issues to be considered by the Information Regulator in developing a code of conduct for surveillance operators in the public and private sectors. The surveillance technologies covered here include CCTV cameras, body-worn video (BWV), automatic number plate recognition (ANPR), unmanned aerial systems (drones), and other systems that capture data of identifiable individuals, or data relating to individuals.

Developing a surveillance systems code of conduct

There are currently no clear regulations for CCTV and related surveillance technologies in South Africa; nor is there any coordination between the laws that regulate surveillance. The Information Regulator will need to address this gap by enforcing a set of norms and standards for surveillance operators; offering guidance on how to balance the advantages of this technology as a crime-fighting tool with fundamental privacy rights. Central to this process will be the development of a code of conduct for surveillance systems: a set of legally binding rules with instructions on the installation and conditions of use of specific technologies to ensure compliance with the provisions of the Act and bring South Africa in line with international privacy standards. The Regulator will also need to clarify the interaction between POPIA and existing international and domestic surveillance and privacy legislation.

In the UK, the Information Commissioner's Office (ICO) has developed and published a set of codes on its website.[40] Similar codes have been issued by Information Commissioners in

Australia and Canada. These portals are user-friendly and a rich source of information for anyone planning to use surveillance software. They provide a benchmark for international best practice and could be a useful template for the development of a code of conduct for South African surveillance operators.

In 2013, the UK's Home Office created a Surveillance Camera Commissioner (SCC).[41] The SCC issued a code of practice setting out guiding principles for all surveillance camera systems in public places; operated by local authorities, the police, and the private sector. The code is published on the SCC's website and contains information on the development and usage of surveillance camera systems, the processing of data obtained by these systems, and the powers and functions of the SCC. A key difference between the Information Regulator and the SCC is that the latter has no enforcement or inspection powers. The SCC also provides clarity on the intersection – and interaction – between the code and other pieces of legislation, and which law prevails in defined situations.

In South Africa, the Information Regulator's mandate covers the dual roles of the ICO and the SCC. The code established by the Regulator could draw on the following 12 guiding principles[42] for system operators, outlined in the guidance provided by the SCC. These principles provide a framework to ensure that surveillance systems are transparent, legitimate, proportionate and effective. The code will need to be updated frequently to keep up with the rapidly changing privacy landscape. It should be published on the website of the Regulator and be open for public consultation.

1. *Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.*
2. *The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.*
3. *There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.*
4. *There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.*
5. *Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.*
6. *No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.*
7. *Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.*
8. *Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.*
9. *Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.*

10. *There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.*

11. *When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.*

12. *Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.*[43]

Safeguards and compliance tools

Ideally, all surveillance systems technologies would be included under the banner of a surveillance code of conduct, with specific guidelines issued by the Regulator for each surveillance system. These guidelines will need to be updated regularly as new software emerges or comes into use. This sub-section contains general guidelines for all types and systems of surveillance. The following sub-section proposes guidelines for specific surveillance technologies.

General guidelines

Surveillance systems can be privacy intrusive, and surveillance operators should be encouraged to objectively assess whether their use is justified, necessary and proportionate, and to consider less intrusive alternatives wherever possible. In the UK, the ICO published a complementary code of practice to assist operators in conducting privacy impact assessments prior to installing surveillance technologies. The Information Regulator could potentially draw on this code as a benchmark.

The ICO identified the following best practice guidelines; applicable to all surveillance technologies discussed here:

- In addition to conducting privacy impact assessments, operators should implement privacy management systems and adopt strict necessity and proportionality protocols where it is established the installation of a surveillance system is legitimate.
- Privacy management programmes should include the establishment of appropriate internal mechanisms and the development of incident response plans, which must be regularly reviewed and updated. Operators should be prepared to demonstrate their privacy management programmes to the Regulator or the authorities if need be.[44]
- Operators should be encouraged to purchase technology that incorporates 'privacy by design', whereby 'technologies, processes and practices to protect privacy are built into system architectures, rather than added on later as an afterthought'.[45]
- Clear signage to inform data subjects that they are being recorded, and the use of privacy notices, are important to ensure fair processing, especially in places with a high expectation of privacy. The information contained in the privacy notice should be conveyed concisely and written in plain language, with 'a person of average reading age in mind'.[46]

- All operators must have clearly documented procedures for handling data, and keep a record (audit trail) in the event the footage needs to be handed over to law enforcement, or submitted as evidence in a court case.
- The privacy of live feeds and recorded images must be safeguarded by limiting monitoring or viewing to authorised personnel, in restricted areas.
- Every effort must be made to ensure that individuals are not identifiable in sensitive settings, and systems should be equipped with the ability to obscure identifiable individuals if necessary.
- Clear storage and retention policies must be implemented and data sharing agreements established with third parties where recorded information is to be shared with them.
- Data must be stored for the shortest possible time period and deleted when it is no longer needed.
- Adequate safeguards should be in place to ensure that the disclosure of information is appropriate.
- Robust physical and technical security measures, such as encryption and cloud computing storage, should be in place to protect potentially sensitive data.
- There should be some degree of human interaction to complement automated technology for all surveillance systems.
- Where information matching takes place, operators must ensure that databases are up-to-date and accurate.
- Data subjects have the right to request their personal data, and operators may be required to provide the data subject with a copy of all the information caught by the request that constitutes their personal data, unless an exemption applies.

Specific guidelines

Specific guidance relating to different types and systems of surveillance is included below.

Communications surveillance

In order to be compliant with human rights, surveillance tools must meet a number of criteria: they must be targeted, based on reasonable suspicion, meet a legitimate aim (such as investigating a crime), subject to judicial and parliamentary oversight, proportionate to the legitimate aim, and non-discriminatory. When considered through the lens of legitimacy, necessity and proportionality, mass surveillance is not justifiable.[47] Clear guidance from the Information Regulator is needed on the issue of communications mass surveillance, and the extent to which this is subject to the provisions of POPIA.

At the international level, the 13 Necessary and Proportionate Principles were drafted by a global coalition of civil society organisations and privacy experts as a framework for modern communications surveillance laws and practices to align with human rights protections.[48] The principles were launched at the 24th session of the United Nations Human Rights Council (UNHCR) in September 2013, and have subsequently been signed by over 400 organisations worldwide. This document is now being used as a model for reform of surveillance law and policy around the world, and to provide a benchmark for measuring whether a State's surveillance practices comply with international human rights law.[49]

The Regulator could look to such international frameworks to inform the development of its guidance on this issue. The guidance issued by the Regulator will also need to include the extent to which cell phone metadata surveillance is covered by POPIA, and the interaction between the different pieces of legislation.

CCTV cameras

Specific guidelines on CCTV cameras could include best practice in terms of locational privacy, protection from abuse by private and public entities, and technical and operational guidelines relating to acceptable standards for CCTV installation.

Private security companies in South Africa are regulated by the Public Security Industry Regulatory Authority (PSIRA). Where a surveillance camera covers a public space, the system operator should be aware of the statutory licensing requirement of the PSIRA. Clarity is needed from the Regulator on the interaction between POPIA and the PSIRA Act.

The use of CCTV cameras for limited household use is exempt from the requirements of POPIA; however, in line with international best practice and jurisprudence,[50] where a fixed surveillance camera faces outwards from an individual's private domestic property and captures images of individuals beyond the boundaries of their property – particularly where it monitors a public space – the recording cannot be considered as being for a purely personal or household purpose. In the same vein, any camera that covers a public space, such as a pavement or a street – even partially – may not be exempt from the requirements of the Act. It would be useful for the code of conduct to include complementary guidance for the public on how to ensure that the use of a surveillance camera on a private domestic property is legitimate and complies with POPIA.

Where it is established that the use of CCTV surveillance is justified, operators should be encouraged to adopt safeguards to prevent excessive processing, such as setting up the system to only record events that are likely to cause concern – for instance, movement into a defined area. A CCTV system that allows recording to be switched on and off easily, rather than recording continuously, will help mitigate the potential risk of recording excessive volumes of information. In places with a high expectation of privacy (such as changing rooms), cameras should only be installed in exceptional circumstances, with strict limitations on viewing and disclosure of footage, and making every effort to inform data subjects that they are being recorded.

Unmanned aerial systems (drones)

Drones have massive potential to violate physical and informational privacy because they lower the cost of aerial surveillance. They also have 'unprecedented capacity for undetected, pervasive mass surveillance of people – including of actions that may not usually be discernible to the naked eye' and can 'contribute to a routinisation of surveillance in public life, which can alter people's behaviour in undesirable ways.'[51]

The code of conduct should distinguish between drones for private domestic use and drones used for professional or commercial purposes. Non-domestic use operators will need to comply with the provisions of POPIA. Drones have a high potential for collateral intrusion given the heights they can reach and the unique vantage point they afford. Even where individuals are not immediately identifiable, they can be identified through the context in which they are recorded, and by using the equipment's zoom function. Recording should be able to be switched on and off when appropriate, given the capacity of drones to capture large numbers of subjects in their footage.

Data should be stored securely using encryption, and disposed of appropriately and in a time-bound manner. Operators are encouraged to incorporate privacy by design methods,

such as purchasing a drone with restricted vision functionality. This should be incorporated in privacy impact assessments and procurement processes. Data subject consent and fair processing are especially important given the high potential for collateral intrusion.

Body-worn video (BWV)

BWVs involve the use of cameras worn by a person – usually attached to clothing or uniforms – which have the ability to record both audio and video information. In the South African context, law enforcement officers under the 'smart policing' initiative attach BWVs to the dashboard of their vehicle. Due to their cost effectiveness, BWVs are also used by civilians. This technology is likely to be more intrusive than CCTV cameras because of its mobility.[52] When conducting privacy impact assessments, operators should establish whether the collection of both audio and visual data is necessary and proportionate. According to the ICO, 'continuous recording will require strong justification as it is likely to be excessive and cause a great deal of collateral intrusion'.[53]

Users should be encouraged to adopt the most privacy-friendly approach and to favour privacy by design; such as purchasing a system where video and audio recording can be controlled and turned on and off independently of each other, and processed as separate data streams. The degree of potential privacy intrusiveness is amplified by the presence of audio, and the code should require operators to provide further justification for the use of BWVs in sensitive areas such as schools, private dwellings and care homes.

Automatic number plate recognition (ANPR)

ANPR systems require particular attention in the development of a code of conduct as they are increasingly used by private and public bodies, are relatively affordable, have the ability to process large volumes of data, and can be easily linked to other databases for matching purposes. Initial privacy impact assessments should identify the type and volume of information that the system will collect, and whether this is justifiable (for instance, recording of vehicles and occupants versus number plates).

When cross-referencing the data with other databases, operators must ensure that databases are up-to-date and accurate. Data sharing agreements should be in place for operators who share the information they process with third parties. Data must be stored for the minimum period necessary and deleted when it is no longer needed, and data retention periods should be specified at the outset. Data subjects should be informed that ANPR recording is taking place, and the best way to achieve this is through the use of signage.

Social media surveillance and big data

When big data technologies were initially developed, their primary application was in the sphere of marketing, where their use was relatively lucrative and low-risk. As the technology began to be used in more high-stakes decisions, such as loan approvals, hiring decisions, medical diagnosis and crime prevention, more social and ethical implications arose.[54]

Recent technological advancements, including AI, behaviour analytics and machine learning, have exacerbated the risks posed by big data and further complexified the cyber governance landscape. The proliferation of cybercrime, as well as of data leaks and breaches has highlighted the importance of preserving online privacy and security. The Facebook-Cambridge Analytica scandal, explained in the textbox below, is arguably the most well-known example of the unlawful processing and mining of the personal information of data subjects, without their knowledge or consent, for political ends. This case study demonstrates how big data is substantially altering the social and political landscape, and underscores the pressing need for regulation and legislation in the digital age.

One notable feature of POPIA is its absence of provisions relating to online privacy.[55] The surveillance code of conduct should include guidance on the regulation of online privacy in respect of big data analytics, AI and machine learning, in order to bring South Africa in line with the current privacy landscape and international best practice.[56] Regulation in this area is especially pertinent given the increasing incidence of data mining on social media platforms. In this guidance, a distinction should be made between big data analytics and more conventional forms of data processing, and the implications of big data for privacy and data protection. In its 2018 report on big data analytics, the ICO identifies several distinctive features of big data analytics, namely: the use of algorithms and the potentially intrusive nature of automated profiling; the opacity of the processing; the tendency to collect 'all the data'; the repurposing of data; and the use of new types of data.[57] The report provides compelling reasons to draft a set of codes governing this particular category of personal data, and warns against the 'high risk of collateral intrusion'; noting:

> *It is possible for data collected by a range of surveillance systems to be integrated into 'big data' processing systems operated by organisations. This has implications in terms of processing, what can be learnt about individuals and how decisions are made about them.*[58]

Case study: the Facebook-Cambridge Analytica data scandal: how 'likes' were turned into votes

Targeted advertising is the basis of Facebook's business model in general, but the Cambridge Analytica breach was particularly nefarious as users' information was processed, without their knowledge or consent, for political profiling and micro-targeting, most notably in the context of Brexit and the 2016 US presidential election.

In the wake of the scandal, it emerged that the political data analytics firm had been employed by a number of governments to stir up unrest through the use of inflammatory content (videos, speeches, bot/fake Twitter accounts, dedicated Facebook pages and events) disseminated on social media platforms in recent years. Another prominent example included swaying the vote in the Trinidad and Tobago presidential elections. The company achieved this by a strategy of increasing apathy among the youth ahead of the ballots. The extent of electoral manipulation in the Global South, where privacy and cybersecurity laws tend to be less advanced, has been seriously under-reported in the media.

Many of the social unrest movements that swept across the US in 2016/2017 have been traced back to targeted disinformation campaigns – or at least, while they likely had their roots in peaceful protest, the movements gained momentum through targeted political and campaign messaging generated by political data consultancies, with specific protest events and campaign pages forming part of the media package they provided to clients. The involvement of political consulting, data analytics and PR firms in political messaging via Facebook has not been limited to domestic campaigns – it is alleged that Cambridge Analytica was employed by the Russian government to inflame existing tensions in the US, in much the same way that the UK-based PR firm Bell Pottinger was contracted by the Guptas in 2016 to spearhead its 'white monopoly capital' campaign in South Africa – the stated intent of which was to inflame racial divisions, which the contracting party then used to further its personal or political agenda: https://www.nytimes.com/2018/02/04/business/bell-pottinger-guptas-zuma-south-africa.html. Interestingly, the public outrage caused by Bell Pottinger's campaign in South Africa spelled the end of the PR firm's 30 years in operation.

In addition to harvesting Facebook users' personal data for political research and data gathering, Cambridge Analytica actively targeted the same users with targeted political ads and content as a means of behaviour modification to influence electoral outcomes. Facebook's liability in this was not only giving political parties and data analytics firms access to sensitive user data for profiling purposes, but allowing the spread of misinformation and disinformation on its platform, which deliberately misled Facebook users and exacerbated existing tensions.

One whistleblower described a category of Facebook users which the firm referred to as 'the persuadables': a group of people identified through profiling to be on the fence politically and/or likely to be easily persuaded, which Cambridge Analytica then actively targeted through disinformation campaigns on the platform, in order to encourage them to vote in a certain way. The campaigns included invitations to political rallies and events, and emotive and inflammatory content covering a range of media, which was micro-targeted to individual users based on comprehensive data points built up about them from Facebook and through psychological profiling.

The specific mechanism that was used to harvest user data was a detailed personality test administered on an external site, which required survey respondents to log onto Facebook after completing the survey in order to be paid for their participation. At this final stage of the administration of the survey, the information collected in the 120-point questionnaire (the Five Factors, or 'OCEAN' model, designed by a Cambridge psychology professor) was then matched with a comprehensive set of data points stored about the individual on Facebook – including personally identifiable information – to match users to the electoral record, using Facebook 'likes'. The app then replicated the process for all Facebook friends of each survey respondent, and used predictive analytics algorithms to generate a dataset containing 253 predictions per profiled record. The responses generated by the survey were then used by the firm to build up in-depth profiles on respondents, who unwittingly became guinea pigs in the electoral targeting campaigns. We know that the user data of nearly 60 000 South African Facebook users was compromised in the Cambridge Analytica breach (this is even mentioned on the website of the Information Regulator), but we do not have any further detail on what the stolen data was used for here.

The following is from a report by the UK's Information Commissioner: 'the Facebook platform… allowed an app that ended up harvesting 87 million profiles of users around the world that was then used by Cambridge Analytica in the 2016 US presidential campaign and in the referendum.' So, in this sense, a type of targeted advertising was happening, but it took the form of political campaigning, and the data was used for the purposes of electoral messaging as opposed to commercial advertising.

For a comprehensive breakdown of how this happened, see https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

While it is clear that big data analytics, if used responsibly, can have enormous social benefit in key sectors such as public health, policing, transport planning and education; considering the volume and variety of big data and the complexity of the analytics, there is a need for regulatory guidance.

In the area of big data policing, also known as 'predictive policing', critics have pointed to the high likelihood that algorithms will perpetuate existing biases (biased inputs lead to biased outputs) and re-criminalise past offenders.[59] The extract below illustrates the way in which big data is used in modelling techniques for policing:

> *Surveillance in big data furthermore contributes to preventive policing. Rather than starting with a suspect and then monitoring him or her, the goal is to start from generalised surveillance and then generate suspects. This form of monitoring is not just for purposes of determent (for instance the placement of a surveillance camera in a notorious crime spot) but constitutes an actual strategy for intervention in the future through the use of modelling techniques.*[60]

Accordingly, the code of conduct should establish appropriate security measures to protect personal data against information security risks. The Information Regulator could issue the following guidance to operators with respect to data protection, in accordance with international best practice, as outlined by the UK's ICO:

- *Use appropriate techniques to anonymise the personal data (data anonymisation);*
- *Be transparent in the processing of personal data (transparency of processing);*
- *Embed a privacy impact assessment framework into big data processing activities;*
- *Adopt a 'privacy by design' approach;*
- *Develop ethical principles (organisations should be encouraged to set up Councils of Ethics that stress the values of fairness and transparency and foster trust of data subjects);*
- *Develop auditable machine learning algorithms.*[61]

Public perceptions of personal data collection are increasingly negative, and suspicions regarding the sharing of personal data with third parties are on the rise. Support by the Information Regulator on the establishment of an ethical framework built into the code of conduct would go some way towards improving fairness and transparency in the processing of personal data and mitigating unlawful processing and public distrust. So too would a public information sharing campaign by the Information Regulator on these issues.

Cross-cutting issues and emerging technologies

Surveillance technologies are increasingly sophisticated and interconnected, in the sense that data collected across different platforms or systems can be linked or matched together; posing further concerns with respect to the personal information of data subjects.[62] Appropriate safeguards should be put in place for operators intending to match data together from different sources, to ensure the information they collect is accurate and not excessive; in line with the conditions of purpose specification, data minimisation and further processing limitation laid out in POPIA and international privacy guidelines.

POPIA contains provisions for limitations on information matching in Section 44 (e)(i), and according to point (d) of the same section, the Information Regulator is instructed to 'consider any developing general international guidelines relevant to the better protection of individual privacy'.

Oversight and the right to an effective remedy

The report of the Special Rapporteur on digital privacy proposes steps that can be taken by States to provide oversight and ensure effective remedies for violations of privacy through digital surveillance. The report notes that effective remedies can come in a variety of legislative, judicial or administrative forms, but that they typically share the following characteristics:

- *First, the remedies must be known and accessible to anyone with an arguable claim that their rights have been violated […]*
- *Second, effective remedies involve prompt, thorough and impartial investigation of alleged violations. This may be provided through the provision of an independent oversight body […] governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society.*'[63]
- *Third, for remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation.*[64] *Such remedial bodies must have 'full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders'.*[65]
- *Fourth, where human rights violations rise to the level of gross violations, non-judicial remedies will not be adequate, as criminal prosecution will be required.*[66]

Challenges with the implementation of a surveillance code of conduct

The Special Rapporteur recently expressed concern at the sizeable challenges faced by the office of the Information Regulator with regard to funding and staffing; noting that the Regulator currently employs fewer than 20 personnel, whereas Colombia's privacy watchdog, by comparison, employs 200 dedicated staff. The Special Rapporteur also found it regrettable that POPIA, which was drafted in 2013, has only been partially operationalised by the State; noting that South Africa is 30 years behind its international counterparts insofar as the adoption of national privacy legislation is concerned. The Regulator therefore faces a significant backlog, which is further hampered by delays with the Presidency signing the Act into law. These challenges need to be acknowledged in the context of the development of a code of conduct.

As mentioned, the Regulator will also need to provide clarity on the relationship between the various pieces of domestic legislation relating to privacy and surveillance in developing a surveillance code of conduct.

Another challenge relating to the development of a code is that international human rights instruments do not hold private corporations legally liable for violations of human rights, including the digital right to privacy – this is the domain of the State – nor are UN guiding principles legally binding on States. To mitigate the risk of non-compliance by companies, APCOF's earlier paper on surveillance notes: 'It is the responsibility of the Information Regulator to ensure that public and private bodies engaged in CCTV surveillance practices are compliant with POPIA and that proper checks must be conducted in such companies as soon as the Act comes into effect'.[67]

The challenges relating to accountability and oversight of the private security industry also need to be acknowledged. In 2010, APCOF published a policy brief on the regulatory challenges relating to the private security industry, in which it noted:

> *As the private security industry seeks to capture more market share positioning itself for greater public roles, forms partnerships with government in the form of municipal and city improvement districts that are common across South Africa and lobbies for state funding, the line between private and public becomes less clear.*[68]

Lastly, it needs to be acknowledged that legal instruments typically struggle to keep apace with technological advances. The surveillance code of conduct will need to be updated regularly and this will require adequate personnel and financial resources within the office of the Information Regulator. As the UN Human Rights Committee has also noted, it is important for the State not only to provide paper safeguards, but to actually carry out ongoing checks to see whether these safeguards work in practice. Regular audits will need to be conducted by the Information Regulator once a code has been developed.

CONSIDERATIONS IN THE CONTEXT OF THE CURRENT PUBLIC HEALTH CRISIS: THE RAPID RISE OF 'HEALTH SURVEILLANCE'

In the context of the ongoing global COVID-19 pandemic, the issue of surveillance is particularly relevant as government scrambles to adopt emergency legislation to curb the spread of the virus. These measures confer extraordinary powers on the executive. One potential consequence of this is a lack of judicial and legislative review and a sidestepping of due process. The task of ensuring the right to digital privacy in the face of a public health crisis is increasingly complex, and the role of the Information Regulator is accordingly crucial in this time.

Following the declaration of a national state of disaster, the Minister of Cooperative Governance and Traditional Affairs (COGTA) issued a policy directive, whereby cell phone providers were required to hand over the cell phone records of all South Africans to the Minister of Communications to aid the government's COVID-19 tracking and tracing initiative. The surveillance of cell phone data under the new emergency regulations, preceded by similar developments in other countries, has raised alarms about the encroachment on freedoms and individual digital privacy rights that this kind of widespread, normalised mass surveillance engenders, and prompted concerns that the authorities – granted extraordinary powers under the temporary disaster regulations – may be reluctant to relinquish once the outbreak is over.

The Regulator responded swiftly to the disaster regulations. It issued a press statement within days of the President's proclamation, calling on government and the private sector to continue to uphold and respect data privacy. One week following the policy directive issued by COGTA, the Regulator published a guidance note on its website; detailing and clarifying the conditions of processing of user data under the emergency regulations.

By and large, the guidance note passes the necessity and proportionality test. It contains so-called 'sunset clauses', in the form of provisions on the extent and duration of data retention, and makes it mandatory for data subjects to be notified within six weeks of the end of the state of disaster. Sunset clauses are key components in mitigating against excessive

processing of personal data. In fact, according to information activist Murray Hunter, the provisions outlined in the Regulator's guidance note provide greater privacy protections than the existing privacy legislation.[69]

One area which should be monitored is the provision in the guidance note for the potential for the data to be reused at a later stage for research or statistical purposes. This is in contravention of the purpose limitation principle enshrined in POPIA and in international law. It is also worth noting that, while the note provides assurances with respect to the anonymisation and de-identification of personal data collected during the pandemic; in reality, it is very difficult to anonymise and de-identify location data.

The key question is, therefore, does – or rather, should – a public health crisis justify the suspension of civil liberties, and are these restrictions likely to be reversed once the crisis is eased, or resolved? Historical experience suggests this is seldom the case.

It is too early to tell to what extent privacy rights are being complied with in South Africa in the context of the COVID-19 crisis response, with recent media articles reporting that the government's cell phone location tracking initiative is not yet operational despite the policy directive being issued several months ago.[70] Internationally, the accuracy of location data in contact tracing has also been questioned, with Bluetooth being shown to be much more accurate than location tracking. In the absence of a fully operationalised Act, the Information Regulator will need to continue to keep the public informed of any developments likely to affect the provisions of the legislation in the context of the pandemic, by publishing frequent and updated guidance on its website as the situation evolves.

LOOKING AHEAD: PANDEMIC RESPONSE AND THE PANOPTICON

The normalisation of health surveillance poses some interesting questions in relation to emerging technologies. One is the use of thermal scanners, which have been widely adopted in a range of public spaces in many countries. In South Africa, the use of this technology was initially limited to airports, but it was touted in the Department of Health's guidelines to employees for the mandatory screening of staff upon their return to work post-lockdown, and has subsequently been expanded to the workplace and the retail sector. It is possible that guidance and clarity on the regulation of this software will be sought from the Information Regulator in the near future.

In the context of the work-from-home measures imposed by governments, civil rights defenders have raised concerns about privacy protection for employees who are monitored by surveillance software installed by their employers.

Another factor to consider in the context of the COVID-19 pandemic is the increased use in public spaces of facial recognition software, whose algorithms have the potential to reinforce and perpetuate existing biases. It would also be useful to consider the implication of the mandated wearing of face masks in public spaces for facial recognition software, whose algorithms may need to be adapted or risk providing inaccurate information if they are not equipped with occlusion detection capabilities.[71]

Lastly, the increased prevalence of the processing of biometric data for the purposes of health screening, particularly for international travel, is a distinct possibility; and the Information Regulator may need to formulate guidelines on the collection, processing and storage of DNA data in extraordinary circumstances under the disaster regulations.

To avoid sidestepping of judicial and legislative due process, all measures and technologies introduced or employed in the context of the pandemic response should include the following safeguards to be compliant with fundamental human rights: testing for necessity and proportionality; instituting independent oversight; ensuring openness and transparency; sunsetting; and limiting data collection, access and use.[72]

In the interests of transparency and accountability, it will be important to guard against the erosion of civil liberties through the excessive processing of personal data under the auspices of public health – the so-called 'architecture of oppression' described by Edward Snowden.[73] The role of the Information Regulator in striking this balance will be crucial.

ENDNOTES

1 See https://privacyinternational.org/explainer/1632/global-surveillance-industry.

2 Protection of Personal Information Act 4 of 2013, Government Gazette. Available at: https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

3 It was anticipated that POPIA would be signed into law on 1 April 2020 but this has been delayed, ostensibly due to the outbreak of the COVID-19 pandemic and the South African government's declaration of a national state of disaster on 15 March 2020. The state of disaster has since been extended several times and remains in place at the time of writing (August 2020).

4 The number and magnitude of data breaches is staggering. See article on data breaches in 2019 and 2020: https://selfkey.org/data-breaches-in-2019/.

5 See C Cadwallar, The Guardian (20 July 2019), The Great Hack: the film that goes behind the scenes of the Facebook-Cambridge Analytica data scandal. Available at: https://www.theguardian.com/uk-news/2019/jul/20/the-great-hack-cambridge-analytica-scandal-facebook-netflix. See also The Great Hack, award-winning documentary on the Facebook-Cambridge Analytica data scandal. Available on Netflix South Africa at: https://www.netflix.com/watch/80117542?trackId=13752289&tctx=0%2C0%2C948b6118fc95cef75485f814bec4a26f1992ae88%3Abc300df8c767263d27ee814b1e25c71cc00c613f%2C%2C. See also media statement issued by the Information Regulator, announcing that the data beach concerned 59 777 South Africans. Available at: https://www.justice.gov.za/inforeg/docs/ms-20180410-facebook.pdf.

6 Dorcas Basimanyane and Dumisani Gandhi (2020) APCOF Research Paper 27: Striking a balance between CCTV surveillance and the digital right to privacy in South Africa, December 2019, p. 10. Available at: http://apcof.org/wp-content/uploads/027-cctvsurveillanceanddigital-dorcasbasimanyanedumisanigandhi.pdf.

7 See OHCHR ,'The Right to Privacy in the Digital Age'. Available at: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx.

8 See Resolution 68/167 adopted by the General Assembly on 18 December 2013 [on the report of the Third Committee (A/68/456/Add.2)]. The right to privacy in the digital age. Available at: https://undocs.org/en/A/RES/68/167.

9 OHCHR 'The Right to Privacy in the Digital Age'. Available at: https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx.

10 Centre for Human Rights, University of Pretoria (2020) 'African Commission publishes revised Declaration of Principles of Freedom of Expression and Access to Information in Africa amid COVID-19 crisis', 23 April 2020. Available at: https://www.chr.up.ac.za/expression-information-and-digital-rights-news/2056-african-commission-publishes-revised-declaration-of-principles-of-freedom-of-expression-and-access-to-information-in-africa-amid-covid-19-crisis.

11 Ibid.

12 Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (RICA).

13 Privacy International report (2019) State of Privacy South Africa. Available at: https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa#commssurveillance.

14 Ibid.

15 Murray Hunter (2020) 'Cops and Call Records: Perspectives on privacy, policing and metadata in South Africa', p. 14. Available at: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/cops_and_call_records_web_masterset_26_march.pdf. See pp. 13–17 for a detailed description of the Section 205 procedures as they relate to the seizure of call records.

16 Ibid.

17 Ibid.

18 J Botha, M M Grobler, J Hahn and M M Eloff (2017) A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws. Available at: https://www.researchgate.net/publication/311495321_A_High-Level_Comparison_between_the_South_African_Protection_of_Personal_Information_Act_and_International_Data_Protection_Laws.

19 Data privacy or data protection in South Africa. Available at: https://www.michalsons.com/blog/data-privacy-in-south-africa/150.

20 J Geldenhuys, POPI and Social Media (2019). Popi and social media, February 2019. Available at: https://www.moonstone.co.za/popi-and-social-media/.

21 H van der Westhuizen (2019) New Bill offers robust game plan against cybercrime in South Africa, 12 June 2019. South African Institute of Foreign Affairs (SAIIA). Available at: https://saiia.org.za/research/new-bill-offers-robust-game-plan-against-cybercrime-in-south-africa/.

22 Privacy International (2017) The Right to Privacy in South Africa. Available at: https://privacyinternational.org/sites/default/files/2017-12/PI%20submission%20South%20Africa%20FINAL.pdf.

23 Lester Kiewit (2020) *Mail & Guardian* South Africa must implement privacy laws to protect citizens, says UN expert. Available at: https://mg.co.za/article/2020-03-12-south-africa-must-implement-privacy-laws-to-protect-citizens-says-un-expert/.

24 See https://www.businessinsider.co.za/bombarded-with-marketing-calls-and-messages-offenders-could-face-jailtime-or-fines-soon-2020-1.

25 Protection of Personal Information Act 4 of 2013, Government Gazette, Chapter 1, p. 15. Available at: https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

26 See glossary of terms. Available at: https://www.moonstone.co.za/upmedia/uploads/library/Moonstone%20Library/MS%20Industry%20News/The%20POPI%20Act%20glossary%20of%20term1.pdf. See also: https://www.mediaupdate.co.za/marketing/146322/understanding-the-popi-act-10-faqs-answered.

27 Protection of Personal Information Act 4 of 2013, Government Gazette, Chapter 1, p. 17. Available at: https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

28 See https://www.naveg.co.za/popi-principles/.

29 Ibid.

30 Protection of Personal Information Act 4 of 2013, Government Gazette, Section 37(1). Available at: https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf

31 Protection of Personal Information Act 4 of 2013, Government Gazette, Section 7. Available at: https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

32 Protection of Personal Information Act 4 of 2013, Government Gazette, Section 33(1). Available at: https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

33 See https://www.naveg.co.za/popi-principles/.

34 Paul Bernal (2016) Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy* 1:2, 243-264. Available at: https://doi.org/10.1080/23738871.2016.1228990.

35 See 'Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance', Giovanni Buttarelli, Secretary General of the Data Protection Supervisory Authority of Italy, p. 6. Available at: https://rm.coe.int/16806845ae.

36 Ibid.

37 Ibid.

38 See https://www.justice.gov.za/inforeg/docs/InfoRegSA-Guidelines-Invite-20191205.pdf.

39 LSSA Guidelines: Protection of Personal Information for South African Law Firms, p. 28. Available at: https://www.lssa.org.za/wp-content/uploads/2019/12/Protection-of-Personal-Information-for-South-African-Law-Firms-LSSA-Guidelines-2018.pdf.

40 See https://ico.org.uk/for-organisations/guide-to-data-protection/.

41 See https://ico.org.uk/for-organisations/guide-to-data-protection/.

42 Surveillance Camera Code of Practice, UK Home Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

43 UK Home Office (2013). 'Surveillance Camera Code of Practice', p. 10–11, , June 2013. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

44 See OECD (2013) 'Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' p. 24. Available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

45 Ibid.

46 ICO. 'Big data, artificial intelligence, machine learning and data protection'. Available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

47 Amnesty International online course, Digital Security and Human Rights. Available at: https://www.edx.org/course/digital-security-and-human-rights.

48 'Covid-19 and digital tracking – assessing the state's approach to privacy protections in South Africa'. Online Zoom discussion with the University of Johannesburg's Department of Journalism, Film and Television, presented by Murray Hunter and Prof. Jane Duncan, 15 April 2020. Available at: https://www.youtube.com/watch?v=AZHUTdz-3QA

49 See https://www.eff.org/document/13-international-principles-application-human-rights-communication-surveillance.

50 Ryneš vs. Czech Republic Office for Personal Data Protection, European Court of Justice ruling, 2014. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=17282.

51 Jane Duncan (2018) Daily Maverick Op-Ed. What Ramaphosa needs to do to fix state spying. Part 6 – drones, 7 March 2018. Available at: https://www.dailymaverick.co.za/article/2018-03-07-op-ed-what-ramaphosa-needs-to-do-to-fix-state-spying-part-6-drones/.

52 ICO. UK CCTV Code of Practice, 'In the picture: A data protection code of practice for surveillance cameras and personal information' p. 27. Available at: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf.

53 Ibid, p. 28.

54 Data & Issues & Opportunities: Trust, Surveillance and Free Will, Bird & Bird LLP. Available at: https://www.lexology.com/library/detail.aspx?g=a66523c5-8056-44b5-819d-c80987478587.

55 J Botha, M M Grobler, J Hahn and M M Eloff (2017) A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws, p. 7. Available at: https://www.researchgate.net/publication/311495321_A_High-Level_Comparison_between_the_South_African_Protection_of_Personal_Information_Act_and_International_Data_Protection_Laws.

56 See the set of guidelines published by the ICO on this topic: 'Big data, artificial intelligence, machine learning and data protection'. Available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

57 Ibid.

58 Ibid, p. 26.

59 Brian Barrett (2020) The Pentagon's Hand-Me-Downs Helped Militarize Police. Here's How, WIRED. Available at: https://www.wired.com/story/pentagon-hand-me-downs-militarize-police-1033-program/.

60 Big Data & Issues & Opportunities: Trust, Surveillance and Free Will. Bird & Bird LLP. Available at: https://www.lexology.com/library/detail.aspx?g=a66523c5-8056-44b5-819d-c80987478587.

61 ICO. 'Big data, artificial intelligence, machine learning and data protection'. Available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

62 ICO. 'In the picture: A data protection code of practice for surveillance cameras and personal information'. p. 26. Available at: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf.

63 'Joint declaration on surveillance programs and their impact on freedom of expression', issued by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, June 2013 (available from www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1), para. 9.

64 See for example European Court of Human Rights, *Segersted-Wiber and others v. Sweden*, application No. 62332/00, 6 June 2006. See also CCPR/C/21/Rev.1/Add. 13, paras. 15–17.

65 A/HRC/14/46.

66 Organization of American States (OAS) 'The right to privacy in the digital age'. Report of the Office of the United Nations High Commissioner for Human Rights, p. 13–14. Available at: https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

67 Dorcas Basimanyane and Dumisani Gandhi (2020) APCOF Research Paper 27: Striking a balance between CCTV surveillance and the digital right to privacy in South Africa, December 2019, p. 10. Available at: http://apcof.org/wp-content/uploads/027-cctvsurveillanceanddigital-dorcasbasimanyanedumisanigandhi.pdf.

68 See http://apcof.org/wp-content/uploads/2016/05/No-3-Regulating-Private-Security-in-South-Africa_-Context-challenges-and-recommendations-Julie-Berg-and-Vavariro-Gabi.pdf.

69 'Covid-19 and digital tracking – assessing the state's approach to privacy protections in South Africa'. Online Zoom discussion with the University of Johannesburg's Department of Journalism, Film and Television, presented by Murray Hunter and Prof. Jane Duncan, 15 April 2020. Available at: https://www.youtube.com/watch?v=AZHUTdz-3QA

70 Business Tech (2020). 'Big problems with South Africa's coronavirus phone tracking system: report, 26 April 2020. Available at: https://businesstech.co.za/news/technology/392867/big-problems-with-south-africas-coronavirus-phone-tracking-system-report/.

71 Eric Hess (2020). 'Straight Talk about Face Masks and Face Recognition' 14 April 2020. Available at: https://www.securitymagazine.com/articles/92140-straight-talk-about-face-masks-and-face-recognition.

72 Allie Funk (2020). 'Fighting Covid-19 shouldn't mean abandoning human rights' WIRED. Available at: https://www.wired.com/story/opinion-fighting-covid-19-shouldnt-mean-abandoning-human-rights.

73 Trone Dowd (2020). Snowden warns governments are using coronavirus to build the 'architecture of oppression'. VICE. 10 April 2020. Available at: https://www.vice.com/en_us/article/bvge5q/snowden-warns-governments-are-using-coronavirus-to-build-the-architecture-of-oppression.

ABOUT THE AUTHOR

Melissa Cawthra

Melissa is a Project and Research Officer at APCOF. She holds a Master of International Affairs, specialising in International Security, from the Paris School of International Affairs (Sciences Po). Her past experience includes work on anti-corruption, transnational organised crime and political-economic affairs at Global Integrity, the United Nations Office on Drugs and Crime (UNODC) and the Consulates of France and Belgium. Her research interests include international security, geopolitics and digital rights.

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. 29 in the APCOF Research Series.
For these and other publications, please visit ***www.apcof.org.za****.*

This publication was made possible through the support of the Sigrid Rausing Trust.

SIGRID RAUSING TRUST

APCOF
African Policing Civilian Oversight Forum

www.apcof.org.za