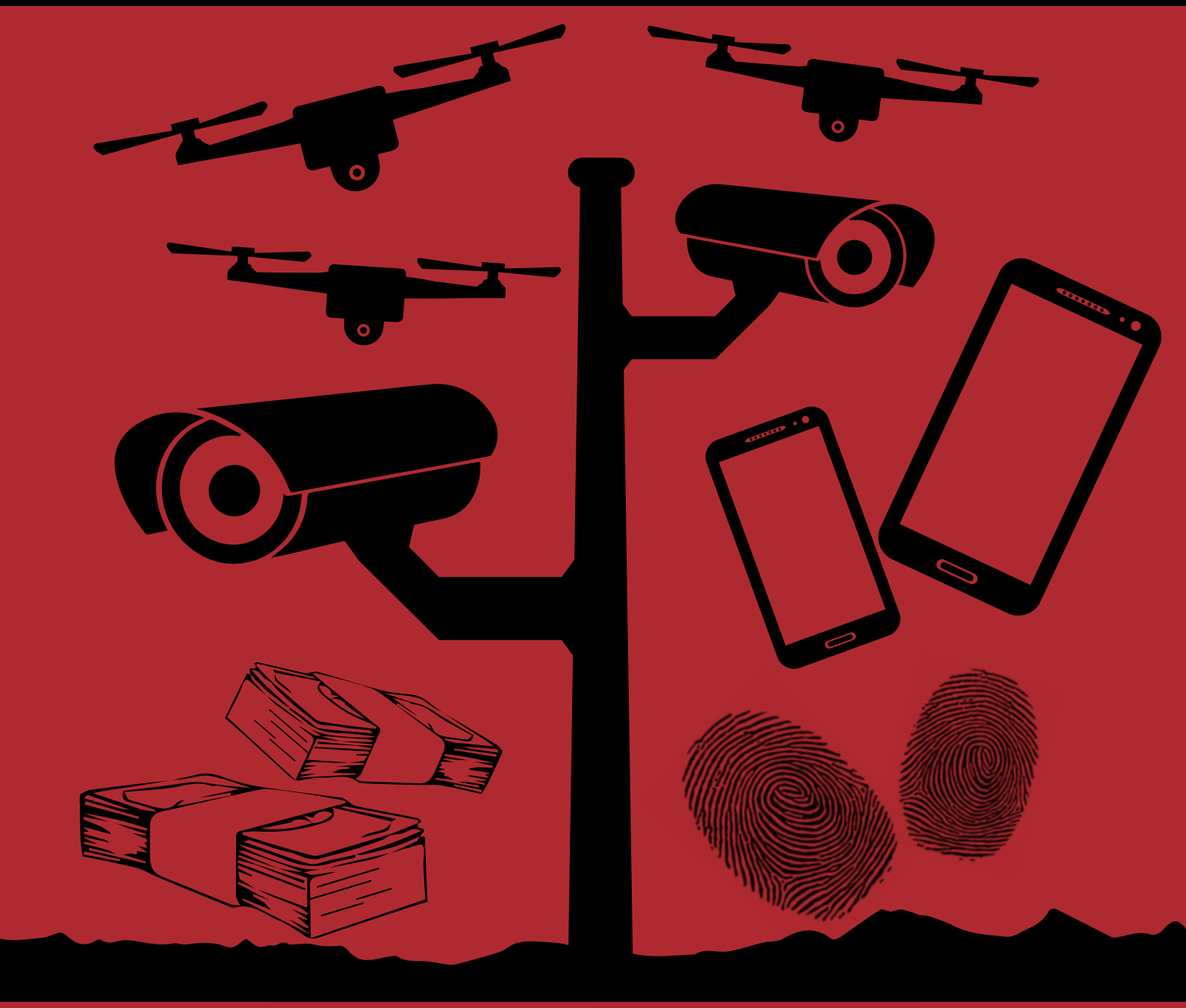
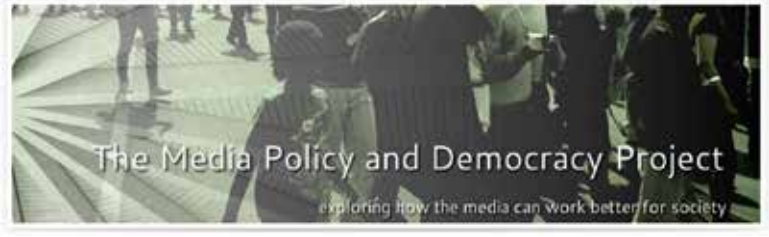
Produced as part of a collaborative research project between the Right2Know Campaign and the Media Policy & Democracy Project



# New Terrains of Privacy in South Africa

Dr. Dale T. McKinley




RIGHT2KNOW

# New Terrains of Privacy in South Africa: Biometrics/Smart Identification Systems, CCTV/ALPR, Drones, Mandatory SIM Card Registration and Fica[1]

**Dr. Dale T. McKinley**

**[December, 2016]**

**Produced as part of a collaborative research project between the Right2Know Campaign and the Media Policy & Democracy Project**

**Available from:**

**Media Policy and Democracy Project:** http://www.mediaanddemocracy.com/

**Right2Know Campaign:** http://www.r2k.org.za/

## Acknowledgements

*Many thanks to the IDRC for funding this research, to R2K for providing an institutional home and to the MPDP for being the initiator and catalyst; and a special thanks to Professor Jane Duncan whose political commitment and intellectual passion have gone a long way to ensure that surveillance/privacy issues remain a central part of the ongoing struggle for social justice in South Africa. May this contribution expand and strengthen that struggle.*

# Table of Contents

# Introduction

Privacy issues in South Africa have a particular historical significance. One of the central pillars of the apartheid system was the systemic violation of the privacy of the black majority alongside anyone who acted in opposition to that system. A significant part of the struggle to defeat apartheid and to reclaim the human dignity of the oppressed was the battle to regain both individual and collective privacy.

Understandably, South Africa's new democratic constitution unequivocally broke from that history by laying down a range of civil and political rights, including the right to privacy. As per the constitution, the right to privacy 'applies to all and "binds" all institutions and organs of the state, as well as a "natural" and "juristic" person, to the extent that it is applicable, taking into account the nature of the right and the nature of the duty imposed by the right' (Section 8(1)(2)). Further, the right to privacy is linked to and reinforces other rights, such as access to information and freedom of expression and association.

However, in the initial post-apartheid period, the issue of the right to privacy was treated, both legally and politically, as largely applicable to the realm of personal/individual 'dignity'. This is not that surprising.

The limited and generalised lack of attention paid to broader privacy issues by both the state and the citizenry in the early period of the democratic transition can be 'explained' in the context of: the country's 'identification heavy' past – namely, the apartheid system's mass use of biometrics[2]; the general push for the government to address other, more politically important socio-economic rights; and societal responses to rising concerns about crime and matters of safety and security/safety. This then provided fertile ground for the widespread and generally uncritical embracing of new and rapidly expanding communication technologies (for example, CCTV, cell phones and the internet) and state policy and private activities where the right to privacy took a back seat.

However, there are several pieces of legislation that have been passed and these explicitly deal with the right to privacy and seek to give practical, legal content to its realisation. The most central are: the Protection of Personal Information Act 4 of 2013 (POPI), which focuses on data protection; the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA), which deals with the interception of communications; and the Electronic Communications and Transactions Act 25 of 2002 (ECTA), particularly in relation to encryption.[3]

The most enduring problem, however, has been the consistent failure to match legislative intent with practical implementation and enforcement. One of the most popular laments in South Africa is that while it may have one of the most progressive constitutions in the world and some really good legislation, it also has a poor track record of translating these into positive, practical impact on the lives of its citizens.

While it is too early to assess how effectively POPI will be implemented – given that the Information Regulator (as the prime enabler of the law) is still in the process of being established – there is also a secondary problem with other, relevant legislation. In the case of the RICA, this relates to the generally lax approach to privacy concerns, especially in respect of SIM (Subscriber Identity Module, which allows cell phones to use the communications network and allows the network to identify the SIM and its installed information) card registration and metadata. In the case of the Financial Intelligence Centre Act (FICA)[4], it is the dominant focus on security, whether national or institutional/corporate, which has often relegated privacy concerns to the side lines.

In particular, there are privacy issues that should be of particular concern when it comes to the following areas:

- The ramped up rollout, integration and interoperability of biometric databases and smart identification systems/cards, with specific focus on the social security and population management/control systems;

- The massive increase in the presence and technological sophistication of CCTV/ALPR[5] hardware and software, alongside associated surveillance in both public and privately-owned (public) spaces;
- The rapid rise in the use of drones for private use and commercial application, coupled with the incipient nature of associated regulation and enforcement;
- The collection, storage, 'sharing' and commodification of ever-increasing amounts of personal information and associated metadata by both public and private sector entities, specifically in relation to SIM card registration and FICA.

All of these specific areas are under studied and researched, despite the fact that they 'touch' – in the most direct and increasingly widespread ways – the privacy of every citizen. This monograph, which is based on desktop research and interview material[6], will therefore survey the general lay of the land that frames these focus areas and then provide a closer look at each, highlighting procedural and practical realities, as well as privacy concerns and gaps. It is hoped that this initial effort will provide a good foundation for further research and advocacy.

# Framing: The Lay of the Land

Over the last decade in particular, issues of privacy have become more and more central to framing and understanding South Africa's political economy. One of the main reasons for this is that Jacob Zuma's occupation of the (highest) seat of power within both the state and the (governing) African National Congress (ANC) has been paralleled by the rise of a surveillance- and intelligence-driven state. Complementarily, there has also been the hugely expanded role of the private sector/corporate world in 'delivering' outsourced/privatised public goods and services, especially in the realm of telecommunications. This has occurred within a context of dominant, privacy-stripping global responses to 'terrorism', to citizen concerns around individual and residential safety and to rising levels of organised criminal activity – all of which have been fashioned and framed by the explosion in communications and surveillance technology.

This has produced a shifting of the foundations of power. Together with the coercive and disciplinary power of the state and the economic and social power of capital, we now have the combined political, economic and social power that comes from 'the vast amounts of permanently stored personal data about entire populations'.[7] It is this power that is now being used and abused by the South African state for political and factional surveillance and by the private sector for further financial gain.

The results are there for all to see and experience. Factionalism within the ANC and the state and the corresponding politicisation of state institutions and governance, both of which centrally involve 'state capture' by corporate capital, have led to more secrecy and less transparency. In turn, abuses of informational and locational privacy have become the 'new normal'. Examples abound, whether it be the seemingly never-ending controversies surrounding President Zuma and his inner circle regarding the abuse and manipulation of the privacy terrain for political gain and personal enrichment; the conscious abandonment of privacy-related regulatory responsibilities by various government departments and entities, such as the South African Social Security Agency (SASSA[8]); or the evisceration of informational privacy by taking advantage of the low thresholds of enforcement of privacy rights by the State Security Agency (SSA) and telecoms companies.

Yet, it is also the generalised lack of political and societal will to confront these increasing abuses and violations of the hard-won right to privacy that have added fuel to the proverbial fire.[9] For example:

- There has been little in the way of sustained pro-active engagement with and advocacy for the enforcement of relevant legislation (of RICA, the Promotion of Access to Information Act and the Consumer Protection Act, for example) from the collective citizenry, although there have been exceptions to this from some sections of civil society[10].

- Where legislation has been actively enforced – for example, regarding FICA – it has happened without due regard for the protection of personal informational privacy by both the public and private sectors.
- Broader citizen and civil society acknowledgement of privacy problems has been dangerously slow, leading to limited counter-mobilisation and resistance to give legal and political content to the 'right to privacy' imperative.

This has given rise to a double-edged and contradictory approach to privacy in South Africa, which the general public and civil society are only just beginning to realise. The reality is that in practice there is a range of increasingly broader and more conscious abuse and violation of the right to privacy that is proceeding in a vacuum of specific legislative control, oversight, enforcement and political will and accountability. This explains why the very first post-apartheid piece of legislation – POPI – that directly addresses the right to privacy in respect of personal information and data processing could, despite being passed by Parliament in 2013, lie dormant on the President's desk for almost three years.

The areas on which this research focuses are certainly not the only ones which constitute present-day threats to privacy in South Africa, but they most definitely should be of huge concern because, in many ways, they have been overshadowed by the bigger political and rights-based questions and problems of the day, as well as shaped by a skewed discourse/sales pitch when it comes to privacy rights.

That discourse/sales pitch relegates privacy to a secondary societal concern in the name of broader and more central security and safety-related rights, concerns and challenges. In a nutshell, the dominant trope is that what is being done (or not done) and pursued on the privacy front does not really constitute a threat to privacy, but is in the public interest, which is always conflated with 'national' interest. Thus, are egregious abuses and violations of privacy carried out and defended in the name of service delivery and prevention of fraud, as legitimate measures to respond to national security concerns, crime levels and to protect the public?

In tandem, those in the private sector that 'benefit from the death of the privacy attempt to frame' the ever-increasing erosion of privacy 'in terms of freedom' by claiming that people 'share data in return for valuable services'. That is akin 'to opting out of electricity or cooked foods; you are free to do it in theory, [but] in practice, it will upend your life'.[11] As the South African Law Reform Commission notes: 'The question is no longer whether information can be obtained, but rather whether it should be obtained and, where it has been obtained, how it should be used'.[12]

Privacy rights and concerns in general are not only being consciously manipulated, abused and violated for specific political, economic and social purposes, but more explicitly, the areas of focus in this research are in the vanguard.

# The Five Focus Areas

*'Privacy is dead, get over it'*
*(Sun Microsystem's Scott McNealy, 1999)*[13]

## *Biometric databases and smart ID cards*

Biometrics is the measurement and statistical analysis of people's 'unique and distinctive' physical and behavioural characteristics. The associated technology is mainly used to confirm the identity of individuals and for access and movement control. 'Biometric information is developed by processing extractable key features into an 'electronic digital template', which is then encrypted to regulate access to it, saved and stored in a database'.[14] Biometrics is hugely invasive of the right to privacy, precisely because there is nothing more private than an individual's biological 'property'. If a biometric identifier is stolen, corrupted or misused, there is no way to replace, retrieve or correct it. Once captured, biological characteristics constitute a

permanent record of an individual's most natural and irreplaceable identity, which then provides the basis for a wide range of potentially illegal, abusive, fraudulent and indiscriminatory uses.

It is no accident that a large part of the story of colonial and apartheid South Africa is a story of biometric control. 'Biometric identification has been an ubiquitous feature of South African life for a century. The earliest forms of computerised biometrics in South Africa were deployed in the effort to regulate the movement and work of labourers on the South African gold mines'.[15] Fast-forward to the twenty-first century and what do we find? Biometrics are no longer used to underpin an entire system of racialised oppression; their use has simply shifted into constructing an ever-expanding and centralised system of identification management and control as well as a colossal and, as yet, uncontrolled 'commercial data analysis sector'.[16]

Across the globe, the collection and use of biometric data is spreading rapidly. A recent research report by the Bank for International Settlements forecasts that 'the global biometric market will grow from US$10.08 billion in 2014 to US$25.31 billion in 2020'.[17] In most cases, biometrics are being used to construct national identification systems that are then linked to 'smart' identification (ID) cards that can be used for various purposes. In the public sector, examples of use include: population registers, national IDs, passports, immigration movement and border control[18], driving licenses, criminal justice databases and the delivery/payment of social services. For the private sector, biometric use is widely applied for security and information sharing – mostly marketing – purposes related to banks, credit transactions, a range of financial services[19], social media advertising[20] and access control to private business premises and residential estates.

When it comes to South Africa's private sector, there are huge biometric databases that have been assembled by the banking and financial services industry in South Africa. Standard Bank has already rolled out its biometric banking application and Capitec Bank has fingerprint details of all its 6.2 million customers and has linked its biometric database to the Department of Home Affairs (DHA) database for the stated purpose of enabling it to verify customer identity. In addition, First National Bank has announced that it is fast moving towards the rollout of biometric-enabled automated teller machines (ATMs), initially using fingerprints and later, possibly voice recognition and iris scans.[21]

In South Africa's public sector, one of the largest biometric databases that has been fully constructed to date is that of SASSA. Starting in 2012, SASSA entered into a contract with a private company, Net1/Cash Paymaster Services (CPS), for the payment of social grants through the introduction of an automated biometric-based payment system. The stated reason for this was to combat and ultimately prevent fraud and corruption.[22] Over the last several years, every single individual receiving a social grant (the latest count being close to 17 million[23]) has had their fingerprints and photographs captured, with some also having had their voices recorded for both verification and authentication purposes – all of which have been loaded onto a central database.

This has produced a whole range of problems; specifically with regard to the privacy of grant beneficiaries. CPS, owned by a larger company, Net1 (formerly Packard Bell) – which in turn has partnered with Grindrod Bank and Mastercard – has used the biometric database to create a massive hardware and software network to market a range of financial services to beneficiaries. In order for beneficiaries to access this network for the payment of their grants, they must register for a SASSA/CPS 'smart' card, for which the provision of cell phone numbers is mandatory. Once in this system, beneficiaries are inundated with 'offers' for anything, including other cards that can be used like a shop card/current account and which require the provision of SIM card numbers and the signing of contracts with little transparency and no recourse; funeral services; airtime; and small loans. Payments for any and/or all of these 'services' are deducted directly from the beneficiary's social grant which is available through the smart card system.[24]

In such a system, personal informational privacy is treated with contempt or simply ignored. The privacy concerns and questions are widespread:

- What are SASSA officials – who are in control of registration and the 'cleaning' of the system – doing with the information to which they have access?
- SASSA's biometric database is linked to a range of other public databases within the state, such as the population register in the Department of Home Affairs (DHA), the database of the South African Receiver of Revenue (SARS) and that of the Government Employees Pensions Fund.[25] Yet, there is no beneficiary or public knowledge of how the information is being shared across each system;
- What parts of the information database are being kept, shared and possibly sold on by all the private entities that collectively run and manage the smart card system?
- Because the system does not operate in 'real time' and 'live', fully integrated and secure databases have yet to be constructed and multiple spaces are opened up on the 'information highway' for violations of personal information privacy, fraudulent access of personal information and tracking.[26]

As stated by Elroy Paulus of Black Sash[27] –which has been engaged in an ongoing battle with SASSA over the payment system – it is a classic example of 'pure extortion, pure theft of personal information'[28]. What makes this all the more outrageous is that this biometric system is being used to take advantage of those who are amongst the most poor and vulnerable in society, most of whom do not know their privacy rights.

Besides SASSA, the DHA is in the process of assembling an even larger biometric database that is being used to construct a range of subsidiary databases for various purposes. These are[29]:

- The Home Affairs National Identification System (HANIS) which has become the main centralised repository of fingerprints for all citizens and permanent residents in the country and the foundational basis of the biometric system. All ten fingerprints and a photograph are being gathered and this is being greatly aided by the ongoing 'dumping' of the South African Revenue Service (SARS) fingerprint database into the HANIS system. New 'smart' national IDs are being rolled out as the system is populated.
- The National Population Register – now biometrically-enabled – which has a long-term goal to have one-stop centres where all personal and locational information will be recorded at birth (live capture) and multiple biometric identifiers such as fingerprints, blood type, facial recognition (and eventually DNA) are captured.
- The Enhanced Movement Control System (EMCS) which at present remains a largely textual information database for identifying and monitoring 'travellers' in and out of the country. A pilot project is presently underway at the three main urban, international airports to capture biometric data (fingerprints, scanning of travel documents and photographs). It will soon be extended to all airports and border posts and aims to add facial recognition technology to the database.[30]
- The National Immigration Information System which, although officially still a pilot project, has been capturing and storing biometric information from refugees, asylum seekers and other temporary residents and workers in the country.

Like the dominant global rationale for promoting and defending the use of most other intrusive technologies, the main reasons given for the rollout of biometrics/smart IDs in South Africa are fairly predictable. There are the ever-present arguments that they will enhance and protect 'national security' and boost the fight against terrorism and organised crime. Other justifications are that they will stop people using multiple identities/fraudulent documents and will greatly assist to 'simply keep track of who is receiving what'.[31]

Much of this rings hollow, given the 'significant number of falsified biometric identification documents' that have already surfaced. In the Netherlands, 'the database storage of digital

fingerprinting for travel documents was halted following questions over the reliability of the biometric technology', with the Mayor of one Dutch city reporting that '21 percent of fingerprints collected … could not be used to identify any individuals'.[32] In the case of South Africa, there is ample evidence to strongly suggest that the quality and accuracy of the biometric databases that the DHA is compiling are being negatively affected by the poor state and mismanagement of existing records that are being digitalised, thus creating the likelihood of a significant amount of false and/or incomplete information.[33]

On the privacy front, the American Civil Liberties Union has pointed out that biometric data accumulation and sharing can 'perpetuate racial and ethnic profiling, social stigma, and inaccuracies throughout all systems and can allow for government tracking and surveillance on a level not before possible'.[34] This is possible because of imperfect capturing and thus matching of biometric information, which can result in false confirmation and/or negatives of identification verification. In turn, this can lead to exclusionary and discriminatory targeting; for example, manual labourers whose fingerprints are worn/damaged and individuals with darker skin when it comes to facial recognition systems.[35]

When it comes to tracking and surveillance, the case of American lawyer, Brandon Mayfield, is salutary. Falsely linked to the 2004 Madrid train bombings through a false fingerprint confirmation by the Federal Bureau of Investigation (FBI), Mayfield was kept under surveillance for weeks, his phone was 'wire tapped' and his house and office were broken into more than once. The FBI further justified their actions by reference to Mayfield as a convert to Islam and the (illegal) discovery of online searches for travel packs to Spain on his home computer. Mayfield's subsequent arrest and two-week incarceration only came to an end when the Spanish authorities conclusively proved that the fingerprints were not Mayfield's.[36]

Such concerns are all the more real in South Africa in light of: the increased powers and reach of the intelligence agencies; the growing rate of organised crime; the very obvious problems with the integrity of inter-operability between all the various databases; and the DHA's general treatment and almost auto-responsive criminalisation of African refugees and asylum seekers, where biometrics are likely being used to 'lock people out' of the system.[37]

Further, there are serious question marks around the security of both government and private sector databases, especially related to illegal access and the subsequent misuse of biometric information. This is especially the case when it comes to the commercialisation of both personal information and transaction data that follows 'from the widespread use of "smart ID" cards for identification and payment. The threats to privacy from "cross-referenced data gathering" are the principal … reason that most European democracies have chosen not to implement a biometric system'.[38]

And yet, in South Africa, a private SA-Japanese company (Marpless) is the sole 'vendor' for the single, largest biometric database in the country – the DHA's HANIS – raising another range of privacy concerns related to who owns and controls the database. There is no law or regulation that speaks directly to this 'vendor locking' and whether there should be open systems or proprietary ones. And then, of course, there is the issue of the business and personal connections between such vendors and senior government bureaucrats and politicians that raise concerns over conflicts of interest.[39]

In sum, the present privacy protections are extremely weak with regard to biometric databases. There is, for the most part, a dominant reliance on the application of in-house self-regulation and the general law of privacy, which are unsuited to the biometric world of data collection, processing and storage. POPI does legally cover many of the present concerns around privacy related to biometric databases, but given the rapid inter-operability and expansion of such databases (both in the public and private spheres), it is going to be a mammoth task to try and ensure a significant degree of compliance and enforcement.

### *CCTV/ALPR/Video Surveillance Systems*[40]

Over the last twenty-odd years in particular, the use of CCTV video cameras for surveillance purposes have spread like wild fire across the globe. While places like the United Kingdom, Europe and the USA have long been at the forefront in both the public and private use of CCTV, there has been a massive uptake in the last decade or so in the developing world. South Africa has been no exception.

Universally, the stated aims for the public/state use of CCTV systems centre predominately on combatting and preventing crime. In some cases, including in South Africa, this has been expanded to include general 'urban management' (mostly in large cities and at certain key sites such as airports). For example, Johannesburg's CCTV system has been promoted as an integral part of the city's 'urban and business renewal plans'. When it was being rolled out in the late 1990s, a senior provincial community safety official stated that the use of CCTV would 'assist in the prevention and detection of crime, help maintain public order, enhance the sense of security of the public and reduce vandalism'.[41]

Further CCTV/ALPR systems are being used for traffic control, enforcement and management' including road tolling systems and border control. Private sector use is also centred mainly on crime prevention and includes tracking/monitoring movement and access control to business premises (for example, mines and shops), as well as private residential estates and gated communities. More recently, private debt collectors and repossession agents are making use of CCTV/ALPR systems.[42]

CCTV systems have also become much more technologically sophisticated. No longer does it entail just stationary CCTV cameras with basic video capacity; many have now been fitted with a range of expanded capacities such as facial recognition, infrared and ALPR technology[43], as well as direct connection to radio frequency identification tags on vehicles[44] and the ability to calculate average speed over distance[45]. Those used for electronic road tolling purposes also operate via cellular networks (3G) and Wi-Fi system/data-links[46].

Mobile CCTV camera surveillance units have also been developed and deployed in recent years. Besides those that are fitted onto law enforcement vehicles and handheld versions, specially constructed mobile CCTV vehicles have now been purchased by at least two main metropolitan authorities in South Africa (Nelson Mandela Bay and eThekwini). These come with additional capabilities that include: super-high resolution 360 degree cameras with a range of up to 7 km; thermal imaging cameras that form an image using infrared radiation to detect and see areas of heat, such as human bodies; laser range-finders which are devices that use a laser beam in order to determine, with great accuracy, the distance to an object; and ALPR technology[47].

Almost all public/state CCTV cameras deployed in South Africa are part of much larger, extensive and integrated systems which are inter-networked and then connected to central control rooms. Here, constant monitoring and evaluation of the video feeds takes place and the control rooms are also linked directly into the communications systems of local law enforcement for response/action; all footage is stored on digital servers.[48] Almost every CCTV camera surveillance system across South Africa is supplied (with hardware and software), operated and managed through public-private partnerships. For example, in Johannesburg, a private company, Omega, 'installs and maintains all of the CCTV cameras in the Central Business District and also provides staff for monitoring of the cameras on a 24-hour basis, seven days a week'.[49]

CCTV camera surveillance systems are ubiquitous in public spaces all over South Africa; it is hard to miss them. Local authorities in all of the major metropolitan areas – Johannesburg, Tshwane, Ekurhuleni, Cape Town, eThekwini and Nelson Mandela Bay – have rolled out extensive systems and there are smaller systems present in other regional towns. Most of these are stationary cameras, covering public streets, government buildings, key tourism sites, sports stadiums, city bus routes/stations, train stations and whatever national key points are located in these areas. The

latest numbers available show that in Johannesburg there are now over 400 cameras in the CBD and adjacent areas,[50] and in the Cape Town CBD and environs 440[51] and in Nelson Mandela Bay the count is 350[52]. However, in all probability, the numbers are substantially higher given the paucity of formal number audits and the under-counting of privately deployed CCTV cameras that are hooked into the public/state network;[53] This is made more difficult because of the complete lack of signage informing/warning people that they are being watched.

As noted earlier, both eThekwini and Nelson Mandela Bay have deployed mobile units, although there might well be others out there. We simply do not know, but we should definitely try and find out. All metropolitan and provincial traffic authorities are making use of CCTV/ALPR systems on the country's main roads and the South African National Roads Agency Limited (SANRAL)[54] has deployed hundreds at all stationary tolling plazas as well as at electronic tolls in the Gauteng province. Further, the systems are present at all major airports, at all border posts as well as in and around most national, provincial and local government buildings. In terms of wholly privately owned and operated systems, there are also many instances where these cover public spaces, for example at boom gates in residential (gated) neighbourhoods and in front of and around businesses which encompass public streets and spaces.[55]

Most of the surveillance cameras now possess ALPR technology[56]. Examples include: electronic tolling cameras in Gauteng and at tolling gantries on most main public highways across the country; stationary cameras in most metro CBDs and surrounding areas; stationary cameras used by traffic authorities to calculate vehicle average speed over distance, as well as cameras used by police (whether stationary or mobile) in 'normal' traffic control operations; and cameras used to monitor rapid transit bus systems in Cape Town and Johannesburg. While it is hard to find up-to-date evidence of facial recognition[57] and infrared technology – integral parts of these systems – there is every reason to believe that many cameras possess this technology. Confirmed cases are cameras that are part of mobile vehicular units and those set up for access control to public buildings.[58] Also, there is every indication that many of the systems used by the private sector possess ALPR and facial recognition capabilities, particularly in relation to access control to residential areas.[59]

Before turning to privacy issues related to CCTV camera surveillance, it is crucial to note that the prime rationale and motivation that has been and continues to be proffered for these systems – namely, combatting and preventing crime – is a chimera. A 2009 study conducted by the Scottish government conclusively found that, 'there is minimal evidence to suggest that CCTV effectively deters crime, and in cases where crime does appear to be deterred, this effect is generally short-lived'.[60] An ACLU survey of CCTV surveillance systems in the UK (the country which has made use of such systems more than any other) found that in the case of 'the two main meta-analyses conducted for the British Home Office … video surveillance has no impact on crime whatsoever'.[61] Among the main reasons why CCTV has minimal impact on the very problem it claims to address is simply that criminals generally do not perceive their presence as an effective deterrent.[62]

Existing privacy protections are woefully inadequate on a number of fronts. Crucially, they are minimal in respect of the internal operational systems and associated checks and balances directly related to the security of the data processing and information cycle, including storage and retention. In most cases, there are simply stated and/or pledged protections such as those in ECTA which, rely on a self-regulation regime. For example, if there has been a breach in the system, then the relevant public entity or private company should inform its clients. However, there is no indication that this is being carried out in any serious or sustained way, as was shown when the eNATIS system (which is the national electronic register that stores, records and manages all information related to vehicle registration and licensing[63]) was hacked several times between 2007 and 2012; yet

most vehicle owners and drivers were completely unaware of this.[64]

While the newly passed POPI has a range of general protections related to all aspects of informational privacy, these are not yet being practically enforced. But even the POPI protections have several gaps in specific relation to visual (personal) data captured and processed by CCTV/ALPR systems, as well related to who is doing the capturing/processing and where it is taking place.[65] Such gaps are widened due to the exceptions that POPI provides for law enforcement and intelligence authorities; related to 'lawful purpose' capturing and processing and also providing a broad legitimating umbrella of 'national security'.

There are a multitude of specific privacy concerns:

- The security of the data processing cycle and related information is arguably the most central. Taking the e-tolling system as a prime example, the sheer volume of the personal information collected and captured (such as addresses, phone numbers, banking details and physical location) raises a range of serious concerns around the accessibility of this information, the consequent ability to track an individual's movements using the information and the physical and electronic security of the storage servers. In 2015, SANRAL admitted, after the fact, to their systems having been hacked;[66] these systems rely on radio frequency and 3G technology and are linked into the ENATIS system;
- Criminal intent and abuse of the system, such as stolen identification and subsequent misuse for personal, institutional or criminal purposes, including for tracking people's movements[67], as well as illegal access and use as evidence in prosecutorial activities;
- The lack of informational consent for and knowledge of the scale of deployment and locational use of cameras with facial recognition and infrared technology, which are much more intrusive;
- 'Mission creep' in the use of information collected. For example, the use of information for discriminatory targeting of specific individuals on the basis of political/ideological activism, race, age, class and sexual preference. Also, the slippery slope between targeted and mass surveillance, between specific and 'dragnet' capturing of information;
- The inter-operability of systems and the compilation and sharing of information – especially in respect of state/public systems that are linked to private operators, processers and storers of that information – for purposes that are not clear or known and that involve the private sector. A good example once again is the situation with e-tolling where Kaptsch (the private e-toll vendor contracted by SANRAL) gives information to ITC Business Administrators (a debt collection agency). Also, what access does the private company ORACLE (which makes/provides the proprietary software) have to the captured/stored information?[68]

As things stand, 'there has been an almost total absence of any public debate' around the extensive privacy issues involved in 'the implementation of both public and private CCTV surveillance in an integrated security system'.[69] Without proper and committed public knowledge, participation and engagement, South Africans are literally allowing the watchers and surveillers to remain in the shadows.

### *Drones (Remotely Piloted Aircraft Systems)*

The drones are coming. No, this is not about some new B-grade sci-fi movie; it is a true reality show playing out right in front of us. For many years now, the world has watched as large weaponised and surveillance drones (mostly deployed by US military and intelligence forces) have wreaked untold fear, misery and death on those deemed, for whatever reason, to be enemies of the most powerful country on earth. As has been the case with a range of initially secretive technologies developed originally for specific military and intelligence use, drone technology has now developed so rapidly

that is has quickly morphed 'into commercial uses never before contemplated'[70]. As a result, civil aviation authorities and regulators across the globe, including in South Africa, are scrambling to keep up while the general populace is only just now trying to understand what is going on and what it all means for ordinary people; particularly for their privacy.

In South Africa, the Civil Aviation Authority (CAA) became one of only a handful of such authorities to come up with regulations for drones when they were put into operation in May 2015 as an amendment ('Part 101') to the CAA Act of 2009. Prior to these regulations, the operation of drones was completely unregulated; the few drones previously in use for recreational and hobby purposes were, and remain, under a self-regulation regime. There is ample evidence to show that prior to the onset of the regulations, drones were already being used by farmers, mines, wildlife officials and some media/film companies[71].

As was and still is the case globally, there was a rush to develop regulations, given the explosion of the technology and pressure from commercial outfits wanting to use drones legally. In the CAA's case, a draft policy developed by US authorities and the Australian regulatory model constituted the core reference points for the formulation of the regulations. Further, key referencing standards were taken from the International Civil Aviation Organisation, many of which do not apply to drones and do not address privacy issues.[72] All of these were, and remain, predominantly framed by and oriented to the needs and interests of the commercial/business sector. Indeed, it was this sector that represented virtually the only domestic 'stakeholders' that were consulted by the CAA in drafting the regulations.[73]

Below is a summary listing of key aspects of the regulations[74]:

**General terms:**

- The regulations apply to owners, operators, observers, pilots and the performance of maintenance.
- The regulations cover commercial, corporate, non-profit (for example, SAPS, fire and rescue and state intelligence) and private operations.
- The CAA Director may issue directives as she/he sees fit for the 'safe and secure operation' of drones.
- No registration or licence is required for recreational users/hobbyists and distance thresholds are 150 feet above the surface and from any public road.
- All drone operations are limited to a lateral distance of 50 metres from any person, group of people, structure or public road, unless otherwise granted an exception by the CAA Director.
- Anyone over the age of 18 is allowed to purchase a drone, with or without a licence.
- No drone can 'release, dispense, drop or deliver or deploy any object or substance' nor carry any dangerous goods or cargo unless approved by the CAA Director.
- No drone can be operated in controlled airspace without an exception or permission granted by the CAA Director.
- All accidents involving injury/death, damage to property, destruction of the drone or loss of control must be reported to the CAA.
- No drone can be flown in formation and/or a swarm.
- No drone can operate over 400 feet above ground or within 10 km of an airport and cannot be flown over/above or adjacent to a police station, a court, a nuclear station, a national key point, prison, crime scene or strategic installation.
- No drone can be operated at night unless under 'Restricted-Visual Line of Sight' (R-VLOS – which applies to private drones) operation or as approved by the CAA Director.

**For private ownership/use:**

- The use of the drone must have no commercial interest or purpose.
- Drones must be operated on property owned by the operator or on property on which the operator has the necessary permission to fly.

- Distance thresholds are 500 m from the pilot and never higher than any obstacle within 300 m from the pilot.
- There is no obligation to have the drone approved and registered, nor is there a licensing requirement.

**For commercial ownership/use:**

- The drone must be registered with the CAA and each drone must be issued with an Air Services Licence (from the Department of Transport).
- Each drone must have a 'Letter of Approval' from the CAA Director.
- The drone pilot must have a license (valid for 12 months and then renewable – subject to revalidation – for 24 months).
- The drone pilot must have a Remote Operator Certificate which is accompanied by an approved operations manual with type and scope of operations. The operations manual along with a proper record of activities generated must be keep for at least 5 years.
- The drone pilot must keep a flight manual.
- Each drone must have registration marks, an ID plate, strobe lights and a transponder, amongst other secondary requirements.
- Each drone must have a maintenance programme and manual (generated by the operator/manufacturer).
- Each drone must have a security manual that covers storage, background and criminal record checks, security training and regular inspection.
- Each drone must have approval for all radio frequency equipment through the Independent Communications Authority of South Africa (ICASA).
- Any registered drone company must be at least 75% South African owned and have a Broad Based Black Economic Empowerment (BBBEE) certificate.
- Each drone must have liability insurance cover.

Although the regulations have been out for only just over a year, the CAA has been flooded with applications for commercial operators and pilot registrations/licences. According to one drone industry operator, as at July 2016, '130 people had remote pilot licenses (RPLs), but only seven operating licences had been issued to drone companies', with a large backlog for operating licences.[75] Not surprisingly, the major users of commercial drones are concentrated in farming, mining, film and entertainment, and media/journalism.

There are also what the CAA has categorised as 'non-profit' users, which include state/public entities such as the police, intelligence services, search & rescue outfits and wildlife/parks management.[76] In respect of these 'non-profit' drone users, it is virtually impossible, as yet, to get any verifiable and specific information on who is actually operating drones and for what specific purposes. For example, the City of Cape Town – in conjunction with the SAPS – widely publicised making use of a drone in June 2015 (which they claimed was a 'pilot project') as part of an 'anti-crime' operation in the Cape Flats.[77] However, there has been no further indication or information as to whether this 'pilot project' has been extended or of the use of drones by police forces elsewhere in the country. The CAA says that they are unaware of any drone usage by SAPS or the state's intelligence agencies.[78] When it comes to private users of drones, we simply have no idea how many there are or for what purposes they are used.

There is complete silence with regard to privacy protection of drone regulations. Incredibly, there is not a single mention of privacy or of relevant legislation such as RICA or POPI. The approach, confirmed by the CAA and one of the few lawyers in the country who has done any legal work on drones, is to deal with any privacy concern and/or issue on a case-by-case basis, informed by the principle of 'reasonable expectation'. Within the ambit of the privacy clause in Section 14 of the Constitution, this means, for example, that a camera-fitted drone hovering outside the open window of an individual's bedroom would be a direct violation of that individual's 'reasonable expectation' not to have their 'person or home searched'. Even then,

the responsibility for processing and acting on any privacy-related complaint rests with the Department of Transportation in conjunction with SAPS.[79] As such, surveillance is not addressed either, noting that the issue of consent is almost impossible, given the operational distances of drones as set out by the regulations. There is no process set out in terms of redress/recourse for those who believe their privacy has been violated and there are no privacy-related measures in place for flight log books and manuals and the storage and processing/use of images that might be captured by camera-fitted drones.

Further, the regulations contain no distinction between state and private ownership and use; and there is no mention of 'public order' drones use by police, security and intelligence services – or of weaponised drones. While there is a general prohibition on carrying dangerous goods and releasing/dispersing objects, there is a range of exemptions that can be given at the discretion of the CAA Director. Specifically, the CAA Director can provide exemptions for[80]: releasing of objects/substances and carrying of dangerous goods [Sections 101.05.04 and 101.05.05]; the of allowable height of operation as well as operating within and over/above restricted areas/buildings [Section 101.05.10(3)]; drone flights operated Below-Visual Line of Sight (B-VLOS) [Section 101.05.11(1)]; night flights [Section 101.05.12(1)]; flights that are closer than a lateral distance of 50 m from person/group of people [Section 101.05.13] and/or closer than 50 m lateral distance from a structure/building [Section 101.05.14(1)(a)]; and flights that are in the vicinity of public roads [Section 101.05.15]. The added problem here is one of enforcement: Who enforces any kind of oversight and control in respect of the users and use of the drones that have been so exempted?

The regulations do not cover the use of larger drones – namely, fixed wing drones, usually used by military/police – although the CAA indicates that these will be included soon.[81] Then there is also the issue of recreational drone use being completely self-regulated and the virtually non-existent regulatory threshold for private users. These present serious privacy concerns in a context where there is rapid technological advancement in drone design and capacity; for example, silence and payload. Such 'recreational' and 'private' drones could well be used for personal spying and/or 'public order' surveillance (examples of function creep); however, such use is presently unregulated and there is no way of knowing who is flying them and for what purpose.[82]

Given the dominance of the commercial sector in the regulatory drafting process alongside the clear absence of privacy-related content in the regulations, a strong case can be made that when it comes to the brave new world of drones in South Africa there has been 'commercial capture'.[83] However, it should be acknowledged that this area is a work-in-progress and that most countries do not yet have formal regulations in place. Also, there is no common law jurisprudence on drone usage, no legal cases have yet been brought and therefore there are no guiding legal principles and precedents in relation to drones and privacy at present.[84]

There is a dire need for general education on/about drones and, more specifically, the CAA regulations – both for citizens, users and those state/public entities (such as SAPS) who are the 'enforcers' of the regulations. There is also a need for the active participation of citizens and civil society organisations in the ongoing process of additions to and expansion of the regulations. In this respect, South Africa would do well to look to the privacy principles proposed by both the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU).[85] Further, because of the almost complete lack of any enforcement mechanisms related to privacy, it will be crucial 'once the information regulator is set up' for the CAA to 'collaborate with this body on reviewing its privacy baseline standards and ensure that all drone operators are familiar with the requirements of POPI and that all data gathered from drones should be handled in terms of the Act'.[86]

### *SIM Cards (RICA)*

South Africa implemented mandatory SIM card registration in 2002 with the passage of RICA.[87] It is illegal for any telecoms service providers to activate a SIM card until the relevant person (either natural or juristic; either citizen or foreign national) has provided certain personal or juristic information and until the telecoms provider has verified that information. That information consists of: a cell phone number; full names/surnames; ID or passport number; a certified copy of ID document or passport; and proof of residence which has to include person's name and residential address (such as a bank statement, rates bill or retail account – none of which many be older than 3 months). For a juristic person, the same information is required, relevant to the business/institution, and if a person lives in an informal settlement they must provide an official/stamped letter or affidavit from a school, church or retail store where their post is received.[88]

RICA (Section 40) stipulates that when someone sells or passes on a SIM card, the same information must be provided by the person now in possession of that SIM card to the telecoms provider who must then verify the information. In respect of all of the above personal information, as well as in respect of every MSIDSN (Mobile Subscriber Integrated Service Digital Network) number of each SIM card and every IMEI (International Mobile Equipment Identity) number of each cell phone, the telecoms provider must record and store that information securely on its premises and keep it for a period of 5 years after the cancellation and/or termination of the subscription

Only persons specifically designated by the telecoms provider and who are in the employ of those companies are legally allowed by RICA to have direct access to this stored information. These individuals – usually no more than a handful – need to be vetted and cleared by the SSA.[89] Further, RICA (Section 40) allows for designated representatives of selected 'applicants' (who comprise the SSA, SAPS, the National Prosecuting Authority, the South African National Defence Force and the Independent Police Investigative Directorate) to make an application to access SIM-card related information. Such an application must be brought in front of and approved by a high court judge, a regional court magistrate or a magistrate and made in terms of Section 205 of the Criminal Procedures Act of 1977. 'To obtain the information, law enforcement agencies must have opened a case docket and must show that obtaining the information [is] absolutely necessary to build the [relevant] criminal case'. In other words, such applications should be 'used as the last resort'.[90]

Once such an application has been approved and the state authority has made the request to the telecoms provider, RICA (Section 40) requires that the personal information must be provided immediately. If the MSIDSN and IMEI numbers are requested they must be provided within 12 hours. Also, if either a cell phone or a SIM card is lost, stolen or destroyed, the responsible person must report this to the SAPS who is required to keep all such reports on record (Section 41)

RICA further prescribes that all telecoms companies must provide a telecommunications service that has the capability to be intercepted, encompassing real time and archived information (Section 30). Interception centres and coordinating offices for Interception Centres (OIC), have been established for such purposes [Sections 32 and 33). This all falls under the Minister of State Security who can bring in designated members of the SAPS, the South African National Defence Force (SANDF) and any other designated officers of state departments so authorised to work on and assist with the interceptions. Thus, there is a situation in which access to parts of SIM card related databases – through either request or interception – are potentially open to a fairly wide range of state officials under the overall control and direction of the intelligence services.

In respect of the use of the databases, RICA provides that they are only allowed to be used for law enforcement purposes. The prime motivation – as evidenced in RICA's explicit inclusion of the Prevention of Organised Crime Act – is to target organised crime and, more generally, to combat

and prevent criminal activity related to cell phone communications (which also links to FICA). However, all evidence clearly shows that this is not working and that the intended impact on levels of related crime is extremely minimal. There are a number of reasons for this that also raise huge privacy concerns.

The person capturing information during the SIM card registration process, commonly referred to as a RICA agent, does not require a police clearance certificate when applying to be an agent. There is also no requirement for the agent to be security vetted and no criminal (especially financial fraud) background checks are done. 'Agents have access to a RICA registration screen where they fill in the data, which then is transferred to the service provider database. There are no security measures in place ensuring that the agent does not, for example, sell the information to someone who may use it for identity theft. The result is that anyone who has committed fraud or any other type of crime can be a RICA agent, and client privacy depends entirely on the honesty of the agent.'[91]

Last year, investigations by journalists from The Times newspaper revealed that 'thousands of cell phone SIM cards are registered fraudulently in terms of RICA'. Journalists were able to purchase RICA-registered SIM cards for all the major service providers at many shops and street stalls in both Johannesburg and Pretoria. They found that such pre-registered SIM cards were being made available, either through insiders at telecoms companies or through fraudulent access to a RICA machine.[92] As a result, it is highly likely that a sizeable portion of the personal information that is being captured, especially for pre-paid SIM cards which the majority of South Africans use, is incorrect or fraudulent. When investigative journalist, Heidi Swart, recently interviewed a manager in the law enforcement division of a major telecoms company, the manager stated that: 'In about one in ten cases, the RICA information is accurate and useful in law enforcement cases.[93]

Further, beyond the RICA requirement concerning designated internal access by telecoms providers to stored information, there is little in the way of knowing and thus preventing illegal access to the information databases that are internal to the telecoms service providers. Given that there is no common law on negligent personal information sharing and data collection,[94] at present there is also little to prevent the sharing of user information within and among state entities/departments, the checking of that information against other databases or private sector network sharing and selling of information. All of this enables the creation of comprehensive personal and life/work profiles of users that violate the right to privacy.

Because the 'backdoor' interception requirement in RICA does not specify what kind of 'capability' is required, this facilitates unknown and unregulated equipment to be built into networks/systems, leaving users completely in the dark and compromising the integrity of the entire system. In turn, this introduces vulnerabilities into the network that can potentially be exploited by a range of actors, including hackers. What makes the present situation that much worse is that there is no information in the public domain about how these security holes have been abused or what, if anything, has been or is being done about it.

There is another seriously concerning reason why mandatory SIM card registration is not an effective tool against criminal activity and instead opens up further space for illegal access to and abuse of personal information. It is the widespread corruption, criminal activity and lack of professionalism within the SAPS as well as other related state entities (for example, SSA and the NPA) that are the main 'enforcers' of RICA in the state fight against crime. This is largely due to the fact that over the last decade in particular, these state entities have become highly politicised and factionalised. Paralleling the same in the ruling ANC under the leadership of President Zuma, the state's security and intelligence services have become political fiefdoms where politically deployed individuals are protected from on high and where there is pervasive fear and distrust. This has allowed a culture of impunity from the law and democratic sanction to embed itself.

According to one of South Africa's foremost experts on law enforcement agencies, the reality is that the most widely used practice of SAPS is to make use of after-the-fact collection of data from confiscated phones: 'The police usually bug your phone first and then find something so that they can then apply procedurally for an interception order' [to access SIM-card related personal information and metadata]. There is of course, no legal authority for this kind of retrospective interception.[95]

Given that much of the personal information is likely to be false, it is to the metadata that the police and intelligence agencies turn. Metadata is the information generated or processed as a consequence of a communication's transmission, such as location data, user data and the subscriber data of the device/service being used; it is storable, accessible and searchable. Such metadata 'gives them all the information they need to track movements and establish where the person of interest lives, for instance'.[96] This is all the more worrying on the privacy front, because RICA does not deal adequately with the interception, collection and use of communications metadata and does not allow citizens to enquire as to whether their communications have been intercepted. However, the unstated and constantly denied 'uses' of databases are clear: the targeting of individuals, based on political, ideological and personal reasons by those with (unregulated) access in the intelligence and security services as well as mass surveillance by scooping up metadata. With the recent 'discovery' of at least two International Mobile Subscriber Identity (IMSI) 'catchers' (mobile devices that allow for the mass tracking and surveillance of cell phones) in South Africa, the possibility now exists that, at the 'touch of a button', thousands of cell phone users' names and addresses can be accessed by either state or private entities.[97]

As many other studies and investigative reports have found, there is more than enough evidence to confirm that the OIC and the National Communications Centre (NCC – run by the domestic branch of the SSA) have the technology to bypass the official channels (namely, the installed technology at the telecoms companies) for interception. As a result, they possess the capability to engage in parallel, untargeted, secretive and unregulated collection and use of SIM card related metadata. Here are three prime examples: the state's mass surveillance capacity was misused to spy on perceived opponents of the then contender for the presidency, Jacob Zuma; leading figures in the crime-corruption busting outfit – the 'Scorpions' – had their phone calls listened to while they were finalising corruption charges against Jacob Zuma during his ascendency to the presidency[98]; and a former military intelligence operative told investigative reporter, Heidi Swart, that the NCC had intercepted conversations of members of the Scorpions successors – the 'Hawks' – as well as bank and government officials.[99]

Taking into consideration the lengthy period of between 3 and 5 years required for data retention, an enabling environment has been created for widespread privacy violations. There is no protection against the reality that mandatory SIM card registration eliminates, to a large extent, the ability of citizens to communicate anonymously. This is a direct and unambiguous violation of the right to privacy.

The effectiveness of mandatory SIM card registration in achieving its stated purpose of combatting and preventing crime would appear to be just as weak at a global level. A 2012 survey of the Organisation for Economic Co-operation and Development (OECD) member countries found tenuous connections between registration and positive impacts on criminal activities. Additionally, widespread privacy concerns have seen mandatory registration torpedoed in many countries. In Canada, the privacy commissioner 'repudiated the idea after investigation, and it was rejected after consultations in the Czech Republic, Greece, Ireland, the Netherlands, and Poland'.[100] There is currently 'little empirical evidence [globally] that mandatory registration leads to a reduction of crime'.[101] Coming back to South Africa, there is a plethora of evidence to show that it actually 'fuels the growth of identity-related crime and black markets for those wishing to remain anonymous'.[102]

And then there is the 'use' for private material gain. For example, by using registration details to market new products and services, and also to sell data about personally identifiable customers. Such violations of privacy could also possibly be used to 'redline' people (namely, to 'serve the finance industry's need to define, measure, and differentiate the population in terms of its financial capacities') when registration information is sold on to financial services.[103] Above all – and in light of the clear evidence that the main, crime-centred, motivation and rationale is secondary – SIM card databases are clearly being used in general terms as a growing base for state surveillance and monitoring and control of communications infrastructure. If there is a need for further confirmation, then the revelation by the University of Toronto researchers (in 2013) that 'offensive digital intrusion software called FinSpy' is present in South Africa, should leave little doubt.[104]

While POPI regulates the information databases derived from SIM card registration, there is a lack of clarity over whether such information can and/or will be used and processed beyond that which is presently required by RICA. Besides a clear need to repeal the RICA provision for mandatory SIM card registration, the telecoms companies urgently require different sets of legislation and guidelines; more especially, because they cut across varying jurisdictions. This will only come with the activation of the Information Regulator and the application of POPI, which will most likely take at least 3-5 years before it is clear whether things are working on this front.[105]

## *Financial Intelligence Centre Act (FICA)*

It is concerning but also not totally surprising that little work/research has been done in respect of privacy issues and financial intelligence in South Africa – certainly not by progressive civil society organisations. It would appear, as is the case with the state's intelligence agencies, that the 'world' of financial intelligence is marked by excessive secrecy. Further, there is very little knowledge, or for that matter much concern, among the general citizenry when it comes to privacy, financial services and personal and/or institutional information. Combined with the fact that FICA has been amended several times, with the latest 2015 Amendment Bill still to be signed into law by President Zuma, the 'lay of the land' in this area can best be covered by setting out the relevant basics of FICA in respect of its core purpose, informational architecture, provisions for who can access information and its privacy protections.[106]

FICA was passed into law in late 2001; one of a number of post-9/11 laws enacted as part of South Africa's contribution to fighting the 'war against terror'. Its centrepiece is the establishment of a Financial Intelligence Centre (FIC) with 'the principal objective of the Centre [being] to assist in the identification of the proceeds of unlawful activities and the combatting of money laundering activities and the financing of terrorist and related activities'. Added to this are two secondary objectives: to make the information it collects available to 'investigating authorities, the intelligence services and the South African Revenue Service'; and also, 'to exchange information with similar bodies in other countries'. The 'investigating authorities' include SAPS and the NPA and the 2016 amendment adds the Public Protector, IPID, the Intelligence division of the SANDF and any investigative division of an organ of state to those bodies with whom the FIC must 'inform, advise and cooperate'.

The main actionable requirement of FICA is that 'no accountable institution[107] may knowingly establish or maintain a business relationship or conduct a single transaction with a client who is entering into that business relationship or single transaction under a false name'. The 2015 amendment replaces 'under a false name' with … 'anonymous clients and clients acting under false or fictitious names'. A recently released 'Notice [of] Amendment of the Schedules' to FICA also proposes to add a wide range of individuals, businesses and institutions to the list of 'accountable institutions' contained in the original Act.[108]

FICA requires an 'accountable institution' to obtain a range of information from both citizen and

foreign national 'natural persons', as well as from companies, closed corporations, partnerships and trusts (whether domestic or foreign). This includes: full names, dates of birth, identity or passport numbers, income tax registration numbers and residential/business addresses. All this information must be verified and this includes reference to a photograph. All recorded and stored information must be kept for a period of five years.

The 2015 amendment adds a new section related to the 'obligation to keep transaction records'. This requires that an 'accountable institution must keep a record of every transaction … that are reasonably necessary to enable that transaction to be readily reconstructed'. More specifically, it requires that a record be kept of all parties to the transaction, all business correspondence and 'the identifying particulars of all accounts and the account files at the accountable institution that are related to the transaction'.

In relation to access to information held by an 'accountable institution', a designated representative of the FIC, upon the granting of a warrant by a judge, can access records 'in respect of reports required to be submitted to Centre'. The 2015 amendment adds that any information relevant to the identification of the proceeds of unlawful activities or the combatting of money laundering or financing of terrorist and related activities held by the FIC can be accessed by: the NPA, the IPID, an intelligence service, the Intelligence Division of the National Defence Force, a Special Investigating Unit, an investigative division in an organ of state, the Public Protector, SARS and foreign entities performing similar functions to those of the Centre. Such information can be withheld if the FIC reasonably believes it would prejudice the rights of any person. Further, the FIC must make information it holds available to the appropriate intelligence structure if it reasonably believes that such information relates to any potential threat or threat to the national security.

In respect of FICA's privacy protections, the original Act makes provision for the protection of confidential information, in that no person may disclose such information held by or obtained from the FIC other than: 'within the legislative scope of that person's powers and duties; with the permission of the Centre; for the purpose of legal proceedings; or in terms of an order of court'. The 2015 amendment adds an entirely new section related to the 'protection of personal information'. The FIC must ensure that 'appropriate measures' for 'personal information in its possession or under its control are taken to prevent: loss of, damage to or unauthorised destruction of the information'; and, 'unlawful access to or processing of personal information, other than in accordance with this Act' and POPI.

Further, the FIC must 'take reasonable measures' to: 'identify all reasonable and foreseeable internal and external risks to personal information in its possession or under its control; establish and maintain appropriate safeguards against the risks identified; regularly verify that the safeguards are effectively implemented; and ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards'.

Crucially however, the 2015 amendment allows for the Minister of Finance to exempt 'any person, accountable institution or category of persons or accountable institutions' from compliance with 'any of the provisions' of the Act. Such an exemption must be tabled in Parliament before being published in the Government Gazette. Further, before the Minister issues, withdraws or amends an exemption he/she must give notice where a draft of the exemption or withdrawal notice of an exemption will be available, invite and then consider submissions received. Exactly why such powers of exemption have been given to the Minister of Finance and how these might be used in the future in specific relation to the collection and processing of personal information that falls outside the scope of POPI is a serious cause for concern.

The primary basis for such a concern relates to that fact that POPI does not apply to the processing of personal information by a public body like the FIC which involves national security or that includes

activities aimed at assisting in the identification of the financing of terrorist and related activities. POPI also does not apply to activities whose purposes are 'the prevention, detection, assistance in identification of the proceeds of unlawful activities and the combatting of money laundering activities' (Section 6 of POPI). The net effect is that unless other existing laws provide sufficient safeguards for privacy, the privacy 'regime' for FICA-related information relies on FICA itself.

Given the biometric databases that banks and financial institutions already possess and are rapidly expanding, this could become particularly pertinent and of concern. For example, the Payments Association of South Africa has recently struck up a partnership with Visa and Mastercard to implement a standardised specification to facilitate biometric authentication on payment cards supported by multiple 'vendors'; an inter-operable system that is the first of its kind in South Africa.[109]

When it comes to the effectiveness of FICA in achieving its core purpose of combatting and preventing financial crimes, the record is less than salutary. Over the past several years, financial crimes in South Africa have skyrocketed; especially money laundering.[110] A 2016 report by PricewaterhouseCoopers entitled, 'Economic Crime: A South African pandemic', reveals that despite one-third of financial institutions being subject to enforcement actions by a regulatory authority, only 50% of money laundering and terrorist financing incidents were detected.[111] The Davis Tax Committee, set up by the Minister of Finance to review South Africa's tax policies, has indicated that from 2008 to 2014, over R200 billion was 'lost' to illicit financial activities and transactions.[112]

# Conclusion

The recent passage of POPI is a major step forward in privacy protection. For the first time in post-apartheid South Africa, there is now a law that contains a comprehensive definition of what constitutes 'personal information', which includes biometric information and applies to both natural and (where applicable) juristic persons. POPI's definition of 'information processing' is also broad enough to include most main areas of import and concern. Importantly, in relation to the right of access to personal information (Section 23), there is now the explicit right to 'request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject'.

Further, there is now an expanded set of data subject rights (Section 5), which include the right:

- to be notified that personal information about him, her or it is being collected;
- to be notified that his, her or its personal information has been accessed or acquired by an unauthorised person;
- to request access to his, her or its personal information;
- to request, where necessary, the correction, destruction or deletion of his, her or its personal information;
- to object, on reasonable grounds relating to his, her or its particular situation, to the processing of his, her or its personal information;
- to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator;
- to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

However, there is a crucial exclusion (Section 6) where the Act does not apply: 'The processing of personal information, by or on behalf of a public body which involves national security' or that includes core information processing that falls under FICA. POPI also does not apply to the processing of personal information 'by the Cabinet and its committees or the Executive Council of a province'. Other exemptions – under the rubric of 'in the interests of national security' – are also applied

on several other fronts, such as further processing (Section 15) and notification (Section 18). Further, POPI only covers the informational dimension of privacy, leaving physical privacy to remain in the legislative wilderness.

Despite the fact that POPI represents a huge improvement in the legal protection of privacy, there remains a dual macro-challenge going forward: to ensure a viable, professional, independent and internally strong Information Regulator's Office and to see whether the regulator's double-barrelled information access and privacy mandates will work effectively together. Meeting these challenges will go a long way in seeing that POPI is successfully rolled out (with accompanying codes of conduct and popular education), that the Regulator is accessible and that the application and enforcement of the legislative mandates are carried out in a complementary way and without fear or favour.

Two more immediate challenges will be: to ensure that the Regulator is up and running as soon as possible – noting that POPI provides for a one year period (which can be extended) for compliance and implementation by all those who hold personal information/data; and that the Regulator is adequately resourced – on both the human and financial fronts – to carry out its extensive responsibilities to monitor, enforce, receive and process complaints, and also engage in legal action if necessary.

The question of resourcing is absolutely crucial, given that the Regulator will, according to the Department of Justice (DOJ), consist of a Chairperson and four ordinary members. It is 'envisaged that 12 administrative support staff will be appointed in 2016/17'.[113] When added to the almost herculean mandate that the Regulator will be expected to adhere to, there are serious questions as to whether the DOJ's allocated budget for the next three years will be even close to adequate. According to the DOJ, R10 million has been allocated for 2016/17; R25.9 million for 2017/18; and R27.3 million for 2018/19.[114]

All of this is of critical importance precisely because there is widespread ignorance among the citizenry when it comes to informational privacy; more specifically, regarding the various information systems themselves (deployment, use, place and capabilities) and entitled rights, especially in relation to the recently enacted POPI, and how to go about enforcing those rights (namely, the role and mandate of the Information Regulator). And, as noted in the introduction, there remains a widespread and generally uncritical embracing of privacy-invading technologies among the South African public.

By and large, POPI has integrated the 'Fair Information Practice Principles' (FIPPS).[115] Moreover, close attention has been paid to relevant international instruments such as the Council of Europe's 1981 'Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data' (COE Convention) and the 1981 Organisation for Economic Cooperation and Development's (OECD) 'Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data'. Comparatively speaking, as a distinct piece of national informational privacy law, it is arguably among the most comprehensive around.

Nonetheless, there is an argument to be made that the kind of approach to informational privacy that is now fully set out in a piece of legislation like POPI is too 'narrow and legalistic' (namely, reduced to principles such as 'notice, choice, access, security and enforcement'). According to this argument, this 'reflects a procedural approach to maximising individual control over data rather than individual or societal welfare' and further, that the approach 'is not working', with 'the available evidence [suggesting] that privacy is not better protected'. Rather, the argument goes, 'the approach should be one of reclaiming the original broader concept of the FIPPS by adhering to Consumer Privacy Protection Principles that include substantive restrictions on data processing designed to prevent specific harms'.[116] Therefore, with regard to POPI, there is already an expressed concern that it is insufficient when it comes to the security of the data processing cycle and information collected (whether

visual or otherwise), especially considering the exemptions given to law enforcement authorities and intelligence agencies. There is the specific need for criminal justice legislation that speaks directly to the use of powers when it comes to processing information/data.[117]

There most certainly should be ongoing debate about the need to continuously re-evaluate and strengthen existing legislation and also to enact new legislation when it comes to the entire terrain of informational/data privacy. In addition, the numerous recommendations that have been put forward by several civil society organisations[118] lay solid foundations for shifting that terrain in favour of a democratic, transparent and accountable privacy regime.

However, the reality is that with the passage of POPI the biggest problem is not so much about the adequacy of legislation and integration of international instruments and principles, but about the enforcement of that legislation alongside more widespread active participation and political/societal pressure from the general citizenry and civil society to continuously push the privacy envelope. Alongside the question of how the criminal justice and national security exemptions are going to work in reality, this has been the permanent lacuna in relation to South Africa's surveillance, access to information and informational/data privacy terrain. Unless the enforcement and participatory sides of South Africa's democracy is expanded and intensified on all fronts, the same problems will continue to surface.

Doing so will catalyse the struggle 'to exercise democratic control' over those that systematically violate individual and collective privacy rights, but it will be a tough ask. As one honest techie states: 'Even if you trust everyone spying on you right now, the data they're collecting will eventually be stolen or bought by people … we have no ability to secure large data collections over time'. What that then requires, is a parallel struggle whose goal should not be to make 'the apparatus of surveillance politically accountable (though that is a great goal) but to dismantle it'.[119]

# Endnotes

1 CCTV (Closed Circuit Television); ALPR (Automated License Plate Recognition); SIM (Subscriber Identity Module – for cell phones); FICA (Financial Information Centre Act of 2001 as amended).

2 Keith Breckenridge (2005), 'The Biometric State: The Promise and Peril of Digital Government in the New South Africa', Journal of Southern African Studies, Vol. 31, Number 2, June: 267-282.

3 Right2Know and Privacy International, 2016; The Right to Privacy in South Africa Stakeholder Report; Universal Periodic Review, 27th Session – South Africa, September.

4 Passed in 2001, FICA established the Financial Intelligence Centre (FIC) whose principal objective is 'to assist in the identification of the proceeds of unlawful activities and the combatting of money laundering activities and the financing of terrorist and related activities'.

5 CCTV is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes. CCTV relies on strategic placement of cameras, and observation of the camera's input on monitors. ALPR consists of high-speed cameras designed to capture a photograph of every passing licence plate; it is combined with software that analyses those photographs to identify the licence plate number.

6 Despite repeated requests, I was not able to secure interviews with the Director or any senior official at the Financial Intelligence Centre, with either the Deputy Director-General or Deputy Director of the Civic Services section of the Department of Home Affairs and with the Executive Head: Group Media Relations at Vodacom.

7 Maciej Cegłowski, 2016, 'The Moral Economy of Tech', Text version of remarks given on June 26, 2016, at a panel on the Moral Economy of Tech at the SASE conference in Berkeley, California. Available at: http://idlewords.com/talks/sase_panel.htm.

8 SASSA is a national agency of the South African government which was created in April 2005. SASSA's mandate is to administer the application, approval and payment of social grants.

9 See Jane Duncan, 2014, 'Big Brother erodes our right to privacy', Mail & Guardian, 28 November. Available at: http://mg.co.za/article/2014-11-27-big-brother-erodes-our-right-to-privacy.

10 Most notably from civil society organisations such as the Right2Know Campaign, the Open Democracy Advice Centre, the Media Policy & Democracy Project, the Freedom of Expression Institute and the amaBhungane Centre for Investigative Journalism.

11 Maciej Cegłowski, 2016, 'The Moral Economy of Tech'.

12 South African Law Reform Commission, 2005, 'Privacy and Data Protection', Discussion Paper 109, October. Available at: http://www.justice.gov.za/salrc/dpapers/dp109.pdf.

13 As quoted in Breckenridge, 2005: 269.

14 Privacy International, 2013, 'Biometrics: Friend or Foe of Privacy'. Available at: https://www.privacyinternational.org/sites/default/files/Biometrics_Friend_or_foe.pdf ; Also see, http://searchsecurity.techtarget.com/definition/biometrics.

15 Breckenridge, 2005: 270-272.

16 Ibid: 269.

17 'Is biometrics the answer to secure and easy online payment?', 30 August 2015. Available at: http://www.fin24.com/Tech/News/Is-biometrics-the-answer-to-secure-and-easy-online-payment-20150827.

18 Katitza Rodriguez, 19 June 2012, 'Biometric National IDs and Passports: A False Sense of Security'. Available at: https://www.eff.org/deeplinks/2012/06/biometrics-national-id-passports-false-sense-security.

19 Lameez Omarjee, 2016, 'Fingerprint authentication coming to SA bank cards', 26 July. Available at: http://www.fin24.com/Tech/Companies/fingerprint-authentication-coming-to-sa-bank-cards-20160726.

20 For example, Facebook is already mining biometric information from user photographs to then sell users' viewing histories for advertising. See, Joel Rosenblatt, 2016, 'Facebook says you can't stop it from using your biometric data', 27 October. Available at: http://www.fin24.com/Tech/News/facebook-says-you-cant-stop-it-from-using-your-biometric-data-20161027.

21 'Is biometrics the answer to secure and easy online payment?, 30 August 2015.

22 Statement by the Minister of Social Development, Ms Bathabile Dlamini on the introduction of the new biometric-based payment solutions for social grants, Pretoria, Friday, 17 February 2012. Available at: http://www.sassa.gov.za/index.php/newsroom/speeches?download=115:statement-by-the-minister-of-social-development-ms-bathabile-dlamini-on-the-introduction-of-the-new-biometric-based-payment--solutions-for-social-grants-pretoria-17-feb-2012.

23 South African Social Security Agency, 2016, 'Fact sheet: Issue no 2 of 2016 – 29 February 2016 – A statistical summary of social grants in South Africa'. Available at: http://www.sassa.gov.za/index.php/knowledge-centre/statistical-reports.

24 Interview with Elroy Paulus from Black Sash, 23 September 2016.

25 As confirmed by the Social Development Minister during the unveiling of the new biometric system in 2012 (Statement, 17 February).

26 Most of these questions/points come from my interview on 30 September 2016 with Natasha Vally who has just finished her PhD. at Wits University, which is entitled, 'South African Social Assistance and the 2012 Privatised National Payment System'.

27 Black Sash was started in 1955 by liberal, white women as a campaign to oppose and mobilise against the human rights violations of the apartheid system. After 1994, the organisation became a human rights NGO which advocates for social justice through education, training, rights-based information, advocacy and community monitoring.

28 Interview with Natasha Vally, 30 September 2016.

29 The majority of the information that follows is taken from my interview on 8 August 2016 with Florencia Belvedere, former Head of the DHA Crown Mines Refugee Reception Centre and subsequently a Director in Civic & Immigration Services at the DHA Head Office in Pretoria.

30 'Statement by Home Affairs Minister Malusi Gigaba during the inspection of the pilot project on biometric capturing at ports of entry', OR Tambo International Airport, 15 December 2015. Available at: http://www.home-affairs.gov.za:8087/index.php/statements-speeches/721-statement-by-home-affairs-minister-malusi-gigaba-during-the-inspection-of-the-pilot-project-on-biometric-capturing-at-ports-of-entry-or-tambo-international-airport; Also, 'Home Affairs to make border posts biometric', 2014. Available at: https://www.immigrationsouthafrica.org/ blog/home-affairs-to-make-border-posts-biometric/

31 Evie Brown, 2014, 'Social protection Management Information Systems (MIS)', GSCRD Applied Knowledge Services research report (December). Available at: www.gsdrc.org.

32 Katitza Rodriguez, 19 June 2012.

33 'Missing documents at the Department of Home Affairs'. Available at: http://www.archivalplatform.org/blog/entry/missing_documents_at_the_department_of_home_affairs/.

34 American Civil Liberties Union (and others), 2014, 'Letter to the US Attorney-General on the FBI Next Generation identification System (NGI), 24 June. Available at: https://www.aclu.org/letter/aclu-letter-attorney-general-holder.

35 Privacy International, 2013, 'Biometrics: Friend or Foe of Privacy'.

36 Matthew Harwood, 2014, 'The terrifying surveillance case of Brandon Mayfield', 8 February. Available at: http://america.aljazeera.com/opinions/2014/2/the-terrifying-surveillancecaseofbrandonmayfield.html

37 Interview with Keith Breckenridge, 16 September 2016.

38 Breckenridge, 2005: 280-281.

39 Interview with Keith Breckenridge, 16 September 2016.

40 Other names used to describe ALPR are Automatic or Intelligent Number Plate Recognition – ANPR/INPR)). A further name used to describe a combination of CCTV and ALPR, when combined with, for example, electronic road tolling, is Intelligent Transport Systems (INS).

41 Anthony Minnaar, 2007, 'The implementation and impact of crime prevention/crime control open street Closed-Circuit Television surveillance in South African Central Business Districts', Surveillance & Society, Special Issue on 'Surveillance and Criminal Justice' Part 1, 4(3): 174-207. Available at: http:// http://www.surveillance-and-society.org.

42 'Beware 'camera cowboys', Security, 27 May 2013. Available at: http://www.security.co.za/news/24653.

43 African News Agency, 2016, 'R14m for automatic number plate recognition', Cape Times, 13 March. Available at: http://www.iol.co.za/capetimes/r14m-for-automatic-number-plate-recognition-1997288

44 E. Hommes and M. Holmner, 2013, 'Intelligent Transport Systems: privacy, security and societal considerations within the Gauteng case study', Innovation No.46, June.

45 'The nuts and bolts of Licence Plate Recognition technology', Alberton Record, 27 March 2014. Available at: http://albertonrecord.co.za/27621/nuts-bolts-licence-plate-recognition-technology/.

46 Interview with Erin Klazer, 20 September 2016. Klazer works as a researcher with the Opposition to Unjust Tax Alliance (OUTA), formerly called the 'Opposition to Urban Tolling Alliance'.

47 Slindo Mbuyisa & Leon Engelbrecht, 2010, 'Mandela Bay purchases mobile surveillance vehicle worth R6 million', Defence Web, 16 July. Available at: http://www.defenceweb.co.za/index.php?option=com_content&view =article&id=8935 ; Simphiwe Dlamini and Smangele Radebe, 2012, 'eThekwini's Mobile CCTV a First', 25 January. Available at: http://www.durban.gov.za/Resource_Centre/new2/Pages/eThekwini%E2%80%99s-Mobile-CCTV-a-First.aspx.

48 Minnaar, 2007; Business Against Crime South Africa, 2013, Media Statement, 'Response to the article on the front page of the Star Newspaper, 27 May 2013, "Beware Camera Cowboys"', 28 May, available at, http://www.bac.org.za/Art/Media/Beware%20Camera%20Cowboys.pdf.

49 'Multi-million rand CCTV system hits crime hard in Jo'burg CBD', 14 August 2015. Available at: http://www.news24.com/SouthAfrica/News/Multi-million-rand-CCTV-system-hits-crime-hard-in-Joburg-CBD-20150814.

50 Ibid.

51 Thulani Gqirana, 2016, 'Cape Town set to spend R12m on more CCTV cameras', 23 June. Available at: http://www.news24.com/SouthAfrica/News/cape-town-set-to-spend-r12m-on-more-cctv-cameras-20160623

52 Mbuyisa and Engelbrecht, 2010. Since this was six years ago, the numbers of CCTV cameras have most likely increased substantially. Numbers could not be found for the other metros.

53 For a good example of this, see plans by the City of Cape Town to '"ensure inter-operability and create a city-wide database of suspicious vehicles and wanted vehicles that could be tracked by the private and City-owned cameras' in Africa News Agency, 2016, 'R14m for automatic number plate recognition'.

54 SANRAL is the parastatal responsible for the management, maintenance and development of the national road network.

55 Anthony Minnaar, 2008, 'Balancing Public Safety and Security Demands with Civil Liberties in a new Constitutional Democracy: The case of Post-1994 South Africa and the growth of Residential Security & Surveillance Measures', Paper presented to the International Workshop: Surveillance and Democracy, Department of Sociology, University of Crete, Rethymno, Crete. 2-3 June.

56 For a good summary list of the capabilities of ALPR, see ACLU, 2013, 'You are being tracked: How License Plate Readers Are Being Used To Record Americans' Movements', July. Available at: https://www.aclu.org/feature/you-are-being-tracked.

57 Facial recognition is a type of biometric software application that can identify a specific individual in a digital image by analysing and comparing patterns [See, whatis.techtarget.com/definition/facial-recognition].

58 Africa News Agency, 2016; E. Hommes and M. Holmner, 2013; Mbuyisa and Engelbrecht, 2010.

59 Minnaar, 2008.

60 'The Effectiveness of Public Space CCTV: A review of recent published evidence regarding the impact of CCTV on crime', Justice Analytical Services, Police and Community Safety Directorate Scottish Government, December 2009. Available at: http://www.gov.scot/resource/doc/294462/0090979.pdf.

61 ACLU, 2008, 'Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found', Noam Biale, Advocacy Coordinator, ACLU Technology and Liberty Program. Aavailable at: https://www.aclu.org/sites/all/libraries/pdf.js/web/viewer.html?file=https%3A%2F%2Fwww.aclu.org%2Fsites%2Fdefault%2Ffiles%2Ffield_document%2Fasset_upload_file708_35775.pdf.

62 'The Effectiveness of Public Space CCTV: A review of recent published evidence regarding the impact of CCTV on crime', Justice Analytical Services, Police and Community Safety Directorate Scottish Government, December 2009.

63 See, 'What is NATIS?'. Available at: https://arrivealive.co.za/National-Traffic-Information-System.

64 Interview with Erin Klazer, 20 September 2016.

65 Interview with Nora Li-Loideain, 3 October 2016. Ni-Loideain is an Irish academic who is presently conducting research into the City Of Cape Town's CCTV/remote camera projects.

66 Interview with Erin Klazer, 20 September 2016.

67 ACLU, 'What's Wrong With Public Video Surveillance?' Available at: https://www.aclu.org/whats-wrong-public-video-surveillance.

68 Interview with Erin Klazer, 20 September 2016.

69 Minnaar, 2008.

70 Andy Pasztor and Robert Wall, 2016, 'Drone regulators try to keep up with rapidly growing technology', 11 July. Available at: http://www.bdlive.co.za/life/gadgets/2016/07/11/drone-regulators-try-to-keep-up-with-rapidly-growing-technology.

71 Interview with Albert Msithini (project Leader for Remotely Piloted Aircraft System – RPAS – Integration at the CAA) and project team member Zia Meer, 12 October 2016; Also, interview with Mikaeel Adam (aviation lawyer at the South Africa-international law firm Hogan Lovells, 15 September 2016.

72 Interview with Mikaeel Adam, 15 September 2016.

73 Interview with Albert Msithini and Zia Meer, 12 October 2016.

74 These summary points are taken from: Government Gazette, 27 May 2015, Civil Aviation Act, 2009, Eight Amendment of the Civil Aviation Regulations, 2015. Available at: http://www.gov.za/sites/www.gov.za/files/ 38830_rg10437__gon444.pdf ; 'Legal Requirements for Operating Drones in South Africa'. Available at: http://www.safedrone.co.za/legal-requirements; 'Here is why South Africa's new drone regulations are ridiculous', 30 June 2015. Available at: http://businesstech.co.za/news/general/92072/here-is-why-south-africas-drone-regulations-are-ridiculous/.

75 Alistair Fairweather, 2016, 'Drones open up a new frontier for journalism', 11 July. Available at: http://mg.co.za/article/2016-07-11-00-drones-a-new-frontier-for-journalism?utm_source=Mail+%26+Guardian&utm_medium=email&utm_campaign=Daily+newsletter&utm_term=http%3A%2F%2Fmg.co.za%2Farticle%2F2016-07-11-00-drones-a-new-frontier-for-journalism.

76 Interview with Albert Msithini and Zia Meer, 12 October 2016.

77 'Drones used to fight crime in South Africa', 23 June 2015. Available at: http://www.mediaclubsouthafrica.com/tech/4272-drones-used-to-fight-crime-in-south-africa.

78 Interview with Albert Msithini and Zia Meer, 12 October 2016.

79 Ibid; Interview with Mikaeel Adam, 15 September 2016.

80 All taken from the Regulations.

81 Interview with Albert Msithini and Zia Meer, 12 October 2016.

82 Interview with Mikaeel Adam, 15 September 2016; Interview with Jane Duncan, 26 September 2016.

83 Interview with Jane Duncan, 26 September 2016.

84 Interview with Mikaeel Adam, 15 September 2016.

85 Electronic Frontier Foundation, 'Privacy principles with regards to drone surveillance'. Available at: https://www.eff.org/document/effs-comments-faa; ACLU, 2011, 'Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft', December. Available at: https://www.aclu.org /files/assets/protectingprivacyfromaerialsurveillance.pdf.

86 Right2Know Campaign, 2015, ' Concerns relating to proposed amendments to CAA legislation: Unmanned Aerial Vehicles. Available at: www.r2k.org.za/wp-content/uploads/Comments-on-the-CAAs-drone-regulations.docx.

87 Republic of South Africa, 2002, 'Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002' Available at: http://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information-8.

88 RICA-section 39; Vodacom, 'Information required when registering a SIM card'. Available at: http://help.vodacom. co.za/personal/faq/2026/What-details-do-I-need-to-register/1154/1165

89 Email interview with Heidi Swart, 1 November 2016. Swart is a well-known and accomplished South African investigative journalist who has written and researched extensively on surveillance issues.

90 Heidi Swart, 'Missed call: Rica "useless" for crime prevention purposes', The Daily Maverick, 10 November 2016. Available at: http://www.dailymaverick.co.za/article/2016-11-10-missed-call-rica-registration-useless-for-crime-prevention-purposes/#.WEhB99J97IU.

91 Email interview with Heidi Swart, 1 November 2016.

92 Shaun Smillie and Graeme Hosken, 2015, 'Crooks Rica havoc', Times Live, 6 November. Available at: http://www.timeslive.co.za/thetimes/2015/11/06/Crooks-Rica-havoc.

93 Email interview with Heidi Swart, 1 November 2016.

94 Interview with Alison Tilly, 11 October 2016.

95 Interview with Gareth Newham, 27 September 2016. Newham is head of the Governance, Crime and Justice division at the Institute for Security Studies in Pretoria.

96 Email interview with Heidi Swart, 1 November 2016.

97 Jane Duncan, 2015, 'Spies are all set to grab your metadata', Mail & Guardian, 11 September. Available at: http://mg.co.za/article/2015-09-10-spies-are-all-set-to-grab-your-metadata.

98 Jane Duncan, 2014, 'Monitoring and Defending Freedom of Expression and Privacy on the Internet in South Africa. Available at: https://www.apc.org/en/system/files/SouthAfrica_GISW11_UP_web.pdf.

99 Heidi Swart, 2015, 'Say nothing – the spooks are listening', Mail & Guardian, 18 April. Available at, http://mg.co.za/ article/2015-12-17-say-nothing-the-spooks-are-listening.

100 Kevin P. Donovan and Aaron K. Martin, 2014, 'The rise of African SIM registration: The emerging dynamics of regulatory change', First Monday, Vol.19, No.2, 2-3 February. Available at: http://firstmonday.org/ojs/index. php/fm/article/view/4351/3820.

101 Nicola Jentzsch, 2012, 'Implications of Mandatory Registration of Mobile Phone Users in Africa', Paper for the German Institute for Economic Research. Available at: https://www.diw.de/documents/publikationen /73/diw_01.c.394079.de/dp1192.pdf.

102 'The Right to Privacy in South Africa', Stakeholder Report, Universal Periodic Review 27th Session – South Africa, Submitted by Right2Know Campaign and Privacy International, September 2016.

103 Kevin P. Donovan and Aaron K. Martin, 2014.

104 Morgan Marquis–Boire et al., 2013. 'For their eyes only: The commercialization of digital spying', Citizen Lab, 30 April. Available at: https://citizenlab.org/2013/04/for-their-eyes-only-2/.

105 Interview with Alison Tilly, 11 October 2016.

106 All subsequent references are taken from the initial FICA and subsequent amendment bills as follows: 'Financial Intelligence Centre Act 38 of 2001';'Regulations in terms of the Financial Intelligence Centre Act 38 of 2001: Money Laundering and Terrorist Financing Control Regulations' (as amended in May 2005, October 2010, December 2010); 'Financial Intelligence Centre Amendment Act, No. 11 of 2008'; 'Financial Intelligence Centre Amendment Bill of 2015'; and Financial Intelligence Centre, 2016, 'Notice: Amendment of the Schedules to the Financial Intelligence Centre Act 38 of 2001', September.

107 The original FICA listed the following as 'accountable institutions': Attorney, Trust Company, Board of Executors, Estate Agent, financial instrument trader, Unit Trust Company, regular or mutual bank, insurer, gambling business , foreign exchange, money lending, investment and broking advice, Post Bank, stock broker, money remitter and financial advisor.

108 These include: professional accountants; persons providing trust and/or company services; dealers in high value goods; co-operatives which provide financial services; short-term insurers; credit providers; money or value transfer providers; auctioneers; dealers in copper material; and, virtual currency exchanges.

109 Lameez Omarjee, 2016.

110 PricewaterhouseCoopers, 2016, 'Financial crime is of increasing concern to most financial services institutions', PwC Global Head of Financial Crime. Available at: http://www.pwc.co.za/gen/press-room/financial-crime-is-of-increasing-concern-to-most-financial-servi.html.

111 PricewaterhouseCoopers, 2016, 'Economic Crime: A South African pandemic', March. Available at: https://www.pwc.co.za/en/assets/pdf/south-african-crime-survey-2016.pdf.

112 Davis Tax Committee, 2014, 'Addressing Base Erosion and Profit Shifting in South Africa', Interim Report. Available at: http://www.taxcom.org.za/docs/New_Folder/1%20DTC%20BEPS%20Interim%20Report%20-%20The%20Introductory%20Report.pdf.

113 Department of Justice, 2016, 'Annual Performance Plan 2016/2017'. Available at: http://www.justice.gov.za/mtsf/dojcd-app.pdf.

114 Ibid.

115 Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

116 Fred Cate, 2006, 'The Failure of Fair Information Practice Principles'. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972

117 Interview with Nora Li-Loideain, 3 October 2016.

118 For example, see 'Proposed recommendations' in, 'The Right to Privacy in South Africa', Stakeholder Report, Universal Periodic Review 27th Session – South Africa, Submitted by Right2Know Campaign and Privacy International, September 2016.

119 Maciej Cegłowski, 2016, 'The Moral Economy of Tech'.