A qualitative analysis of how INVESTIGATIVE JOURNALISTS, CIVIC ACTIVISTS, LAWYERS AND ACADEMICS are adapting to and resisting communications surveillance in South Africa

Research conducted by Admire Mare

admiremare@gmail.com

Research Associate

Media Policy and Democracy Project

March 2016

Table of Contents

ABSTRACT

This report examines how investigative journalists, civic activists, lawyers and academics are adapting to and resisting communications surveillance[1] in South Africa. In order to explore these issues, I interviewed 23 respondents, including four academics, two lawyers, three journalists and 14 civic activists, about their concerns and the ways in which communication surveillance has changed their work in the wake of media reports indicating the pervasive nature of communications surveillance. I also interviewed experts in the area of communications surveillance from Privacy International (PI). The study found that all these vulnerable constituencies of South African society have begun to change their communication practices. Most of them indicated that they have reverted to analogue communication methods which they saw as secure and safer. Journalists, lawyers and civic activists revealed that they are using end-to-end email encryption technology, face-to-face communication and code language to circumvent surveillance procedures. In light of state surveillance practices, most academics expressed concern that academic freedom was being seriously undermined. Academics also indicated that they have changed the way they communicate with research participants and store their data. Whilst some journalists indicated that they use cloud computing services for data storage, academics said that they have ceased relying on such tools. They indicated that third party cloud services are vulnerable to hacking and phishing. This report demonstrates that despite the absence of overt political struggles against communication surveillance, responses from academics, journalists, activists and lawyers suggest that everyday forms of resistance are prevalent in South Africa.

[1] Communications surveillance encompasses the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing, or similar actions taken with regard to information that includes, reflects, arises from or is about a person's communications in the past, present, or future (Human Rights Watch, 2014: 1).

Background and introduction to the study

Surveillance[2] encapsulates various modes of categorisation and social sorting, where discrimination and privilege are entrenched through the unplanned consequences of data gathering and analysis (Lyon, 2001 & 2003). The collection and analysis of information about populations conducted as part of surveillance is aimed at governing people's activities (Haggerty and Ericson, 2006: 3). As a social practice, it facilitates the observation and tracking of people and objects, their labelling and subsequent organisation, and the value judgments based on these orderings. Writing about analogue (i.e., bureaucratic and electro-mechanical) and digital surveillance. Graham and Wood (2003: 228) argue that digital methods facilitate more pervasive surveillance in real time. For Graham and Wood (2003), the digitisation of surveillance which is accompanied by automation shifts the role of human operators during the process. Because of this process of automation, human discretion is displaced by operators who merely programme, supervise and maintain systems (Graham and Wood, 2003).

The advent of computer databases, surveillance cameras and other technological advances are said to have given rise to "new surveillance[3]" (Marx, 2002) comprising of "surveillant assemblages" (Haggerty and Ericson, 2000) which operate well beyond the confines of the central state. As Lyon (2001: 1) observes, digitisation has been accompanied by the emergence of "surveillance society" which has seen surveillance proliferate beyond the bureaucratic field to become a routine and mundane feature that is "embedded in every aspect of life". It has also been accompanied by both quantitative (in terms of size, coverage, speed, intensity and so forth) and qualitative changes. It has brought information that is more amenable to storage, transmission and computation, as well as algorithmic surveillance (Introna and Wood, 2004). This ability to easily and efficiently store, sort, classify, retrieve and match information in digital systems becomes increasingly significant, amplifying the capacities of the surveyor and the effect on the surveilled far beyond the potential of analogue methods (Norris and Armstrong, 1999). As Loftus and Goold, 2012: 276) observe, "whereas in the past the surveillance powers of the state were directed only at particular individuals who were deemed to be at risk or undeserving of trust, today it would seem that surveillance powers are directed against everybody".

[2] Surveillance refers to "any collection and processing of personal data, whether identifiable or not, for the purpose of influencing or managing those whose data have been garnered" (Lyon, 2001:1). At the core of this definition is the acknowledgement that surveillance involves power. It involves the collection of information for the purposes of "influencing or managing" some individual or group. Another important aspect is that surveillance is relational, involving a power dynamic likely to unfold in complicated ways.

[3] This refers to "the use of technical means to extract or create personal data" (Marx, 2002; 12).

There is a burgeoning literature (Mathiesen, 1997; Lyon, 2002; Andrejevic, 2012; Bakir, 2015; Mann, 2013) on surveillance, focusing on its metamorphosis "from the situation where the many see the few to the situation where the few see the many" (Mathiesen, 1997: 217) and its subsequent impact on everyday life. These studies (Deleuze, 1990; Lyon, 2003; Marx, 2002) also foreground the logics, operations, and consequences of the underlying systems, and the attendant ethics. They demonstrate how surveillance facilitates the control of populations and affects people's life chances and choices thereby obfuscating how different constituencies in democratic and non-democratic settings resist these practices. Some scholars (Lyon, 2002 & 2015; Simon, 2005; Graham and Wood, 2003) have focused on how societies over time become "surveillance societies" and the unintended but nevertheless harmful outcomes of these transformations. Whereas some scholars (Foucault, 1977; Lyon, 2014; Andrejevic, 2012) view surveillance as predominantly negative in all its manifestations, Giddens (1981 & 1985) describes it in a positive light. For Giddens (1985), surveillance phenomena also enable modern organisation and simplify human existence. He defines surveillance as the accumulation of information defined as symbolic materials that can be stored by an agency or collectivity, as well as the supervision of the activities of subordinates by their superiors within any collectivity (Giddens, 1981: 169).

Unlike Giddens, Fuchs (2011) argues that surveillance cannot be extricated from modern nation states because it is concerned with the collection and storage of information on citizens (births, marriages, deaths, demographic and fiscal statistics, "moral statistics" relating to suicide, divorce, delinquency, etc.) in order to organise administration. Contrary to the positive evaluation advanced by Giddens (1985), critical political economists like Fuchs (2011) view surveillance as constituted by violent and coercive aspects. This means that surveillance signifies a coercive process that always is embedded into dominative systems.

Surveillance can have a significantly constraining effect on political debate and protest, and hence reduce the broader public debate on socially contested issues and the ability of weaker groups to resist power (Brown, 2013). This suggests that surveillance in all its various manifestations has a chilling effect on civic activism. Research (Lim, 2013; Gerbaudo, 2012; MacKinnon, 2010) demonstrates that in authoritarian regimes surveillance "deters demonstrations and other disorderly behaviour" (Ullrich and Wollinger, 2011: 27). As Hintz (2014: 354) notes, blanket surveillance and pervasive monitoring of people's movements, actions and communication undermine critical debate and dissident voices; thus, key features of a functioning democracy. This chimes with a report published in June 2013 by the United Nations Special Rapporteur on Freedom of Expression and

Opinion which highlighted that the right to privacy is an essential requirement for the realisation of the right to freedom of expression. Discussing the rise of networked authoritarianism in China, MacKinnon (2010) shows that control over major backbones and access points can allow governments to draw a virtual fence around a state territory and restrict access to both services and information from outside that territory. The Egyptian government also tried, with little success, to shut down internet access during the Arab Spring uprising in January 2011(Gerbaudo, 2012). A combination of censorship and surveillance was used to identify activists and arrest them in Syria. According to the Electronic Frontier Foundation (2011), mass communication surveillance technologies have been misused to spy on politicians, dissidents, judges, human rights organisations and activists in Latin America. These surveillance systems demonstrate how communication interception is being used as a political tool to identify, control and stifle dissent. State surveillance directed at protesters can have a 'chilling effect' on social movement activity to the extent that many activists are afraid to attend a protest, and those who do are compliant and self-policing.

Several studies have suggested that covert forms of repression can result in challengers substituting violent behaviour for non-violent activity (Lichbach, 1987; White, 1989). As surveillance increases the cost of action to social movement actors, it can contribute to the decline of organisations and movements (Tarrow, 1998: 147-8). Linking behavioural changes to the suppression of free speech, Greenwald (2014: 177-178) argues that "mass surveillance kills dissent in a deeper and more important place as well: in the mind". Repression including surveillance may also turn dissidents underground (away from more public, restricted spaces toward more private 'free' spaces), or alternatively away from overt collective forms of resistance[4] toward more covert, individualistic forms of resistance (Davenport, 2006; Johnston, 2005). As della Porta (1995) notes, while individuals are concerned to participate, surveillance also threatens the bonds between organisations in networks. In their study on the impact of surveillance on civic activism, Starr, Fernandez, Amster and Wood (2007) note that surveillance forecloses political opportunities in a number of ways. One of the ways in which surveillance changes the climate is that it creates an atmosphere of threat, which intimidates participants and would-be participants; thus, surveillance has a powerful intimidating effect.

Surveillance has begun to replace censorship as the weapon of choice for both democracies and repressive regimes intent on silencing and intimidating journalists (Rispoli, 2014). It undermines

[4] Resistance can take many forms. For Martin et al. (2009), resistance incorporates varying notions of action, interaction, opposition, awareness, and power. Similarly, Hollander and Einwohner (2004, 534) identify four consistent properties of resistance: its interactional nature, the central role of power, how the concept of resistance is socially constructed, and the complex nature of resistance.

critical and investigative reporting which requires confidential communication with sources and, occasionally, the anonymity of authors. These days all kinds of governments are spying on journalists' emails to identify confidential sources. They're hacking journalists' computers and infecting them with malware. They're tracking journalists via their phones. This kind of surveillance makes it that much more difficult for the press to challenge powerful institutions, bear witness and represent the public interest. As Rispoli (2014) observes, surveillance not only impedes journalists' ability to do their work but also endangers the safety of sources that trust reporters to keep their correspondence confidential. Edward Snowden's revelations have shown that a number of intelligence agencies, including the United States of American National Security Agency (NSA) and the British intelligence agency General Communications Headquarters (GCHQ), collected the emails of journalists at top international media outlets and labelled investigative journalists as "threats" alongside terrorists and hackers. Surveillance also has a chilling effect, where the mere threat of spying leads people to self-censor. Surveillance in the United Kingdom (UK) is having a hugely negative effect on the ability of journalists to work in the public interest and protect their sources (Rispoli, 2014).

Research (Human Rights Watch, 2014; Pew Research Centre, 2015) on the impact of surveillance programmes and government crackdowns on unregulated contact between officials and the press have combined to constrict the flow of information concerning government activity. Surveillance of this nature has led to changes in journalistic sourcing strategies, as well as cutting away at the ability of government officials to remain anonymous in their interactions with the press, as any interaction—any email, any phone call—risks leaving a digital trace that could subsequently be used against them (Human Rights Watch, 2014). These concerns are serious in the context of ubiquitous surveillance, especially in settings where mandatory Subscriber Information Management (SIM) card registrations have been legislated. This puts journalists and their potential news sources in a quandary given the potential vulnerabilities associated with accessing metadata[5] and contents of communication without warrants. The danger in metadata is that it allows the surveiller to map our networks and activities, making journalists think twice before communicating with sources. A study conducted by the Human Rights Watch (2014) found that news sources are

[5] Meta-data or communications data is often distinguished from the content of the message (that is the message itself. This distinction is based on the traditional model of postal mail, where information written on the outside of an envelope is distinguished from the content of the envelope. This distinction is, however, rendered nearly meaningless by modern surveillance methods, which can capture far more than the destination of a communication, and en masse. Meta-data can include the length of phone calls, the phone numbers of the caller and the recipient, the serial numbers of the devices used and sometimes the locations of those who made the call. The meta-data includes information about who phone users call, when they call and for how long.

substantially less willing to be in contact with the press, even with regard to unclassified matters or personal opinions.

The impact of surveillance on human rights lawyers is another area which is extremely under-researched. One of the few studies was conducted by the Human Rights Watch (2014) in the wake of the Snowden revelations about mass surveillance programmes administered by the United States of America and her allies. According to the Human Rights Watch (2014), lawyers have a professional responsibility to maintain the confidentiality of information related to their clients on pain of administrative discipline. They also rely on the ability to exchange information freely with their clients in order to build trust and develop legal strategy, which is especially important in the realm of criminal defence. Increased government surveillance undercuts these longstanding and central elements of the practice of law, creating uncertainty as to whether lawyers can ever provide true confidentiality while communicating electronically with clients. Like journalists, lawyers interviewed by the Human Rights Watch (2014) felt under pressure to adopt strategies to avoid leaving a digital trail that could be monitored; some noted that they use burner phones. Others indicated they preferred encrypted technologies and others reported travelling more for in-person meetings.

Surveillance becomes extremely worrying when it violates human rights and transgresses constitutionally guaranteed provisions. Surveillance practices can also have a deleterious impact on academic freedom[6]. Academic freedom constitutes the bedrock of teaching, research and publication in most institutions of higher education. However, intrusive state surveillance has begun to weaken and violate this constitutionally guaranteed right across the world. Surveillance impacts negatively on the work of academics that relies on confidentiality to carry out research on a wide range of issues. Academic freedom is dependent on a researcher's ability not only to gain access to information but also to explore ideas and knowledge without fear of surveillance or interference. As Gerstmann and Streb (2006) observe, allowing the police unfettered access to files stored on university-provided computers at state universities compromises free speech and academic freedom. This can lead to self-discipline and side-lining of research topics. Thus fear and a constant sense of potential surveillance can be an even more effective form of control than punishment (Gerstmann and Streb, 2006: 186).

[6] Academic freedom is a social compact. It is based on the willingness of those involved in the academic enterprise to adhere to its core ideas and the willingness of those outside the academic enterprise to refrain from undue interference.

Theorising Surveillance

Surveillance studies can be situated within two broad theoretical frameworks: the panopticon and assemblage. Panopticon theories focus on the few watching the many, as evidenced by the Bentham, Orwell and Foucault's panopticon theories. This strand of theorisation sees surveillance as generally more powerful as a form of social control than outright repression, because it makes social control less visible. It makes people internalise acceptable conduct and regulate their own behaviour rather than having the state or some other external force doing so. These representations of surveillance tend to reinforce the 'Big Brother' stereotype, neglecting a more nuanced understanding of the subject. As Mathiesen (1997: 207) observes, this Foucauldian view fails to acknowledge the rise of the spectacle in mass mediated societies where the many watch the few (symbolised by "synopticism"). Theories of assemblage which borrow heavily from Deleuze and Guattari's (2000) postulation are therefore concerned with the many watching the few, as illustrated by concepts such as sousveillance, "veillance" (mutual watching) (Mann, 2013) and liquid surveillance (Bauman, 2004). Consistent with post-modernist theories, assemblage theories view surveillance as diffuse, pervasive and deeply embedded in all social relations and formations. In this section, I will tease out the main theoretical tenets of panopticon theories of surveillance and then proceed to discuss assemblage theories.

(a) Panoptic theories of surveillance

Deleuze's (1992) concept of control has several similarities with the Foucauldian notion of "discipline". Reflecting on the technological advances since Foucault's characterisation of modern societies as "disciplinary societies[7]", Deleuze depicts the present day as a "control society" where technology is used to track, monitor and control populations through technological means, rather than focusing on disciplining and monitoring populations through traditional institutions. It is important to note that the idea of Big Brother can be traced to the writings of Orwell (1949). According to Orwell (1949), citizens are monitored in their homes by a telescreen, a device which both projects images and records behaviour in its field of vision. He saw "thought police" as co-ordinating this extensive monitoring effort by operating as agents of a centralised totalitarian state. For him, surveillance was used primarily as a means to maintain social order and conformity (Orwell, 1949). Although Foucault (1977) extends Orwell's theoretical cloth, it is important to note that his views on surveillance situate it in the context of a distinctive theory of power. Borrowing

[7] He uses the term to refer to totalitarian mechanisms of power which regulates the behaviour of individuals in the social body. This is done by regulating the organisation of space, of time and people's activity and behaviour. He identifies disciplinary institutions such as prisons, hospitals, asylum, schools and army barracks.

Jeremy Bentham's (1791) prison design known as the panopticon, Foucault proposed that the panopticon served as a socio-material template for a new model of power which extended beyond the prison to take hold in the other disciplinary institutions characteristic of modern societies, such as the factory, hospital, military, and school. At the core of the metaphor are its centralising, state-oriented and disciplinary functions where the state is seen as all-seeing and all-powerful entity synonymous with Orwell's notion of Big Brother.

He was concerned with explicating how surveillance and power are distributed in modern society. This led him to theorise that surveillance is conducted by the few on the many, with the many unaware or unsure of this surveillance and thus driven to self-monitor and modify their behaviour (Foucault, 1977). Thus, surveillance means that someone "is seen, but he does not see; he is the object of information, never a subject in communication" (Foucault 1977: 200). Panopticon highlights the exercise of power through self-discipline, self-reflection and training of one's soul under the eye of authority. Surveillance is a power that is "capable of making all visible, as long as it […] [can] itself remain invisible" (Foucault 1977: 214). According to Foucault (1977: 201), "the major effect of the Panopticon" was "to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power". The result was the internalisation or interiorisation of the watchtower's gaze, such that the prisoner became his own overseer. Foucault makes it clear that surveillance is a repressive, coercive process:

> 'Our society is one not of spectacle, but of surveillance. (…) the individual is carefully fabricated in it, according to a whole technique of forces and bodies' (Foucault, 1977: 217).

Foucault (1977) stresses that discipline and potential punishment are important aspects of surveillance in the sense that the latter aims at the control and subjugation of bodily movements (Fuchs, 2010). Because of his deterministic theorisation, Foucault is seen as denying the existence of human agency and resistance to surveillance practices. This is because panopticism is characterised by immobility through enclosure, isolation and disciplinary practices. Subjects of panopticism are viewed as limited agents overwhelmed by surrounding structural pressures and determinations. However, Lyon (1994) argues that a structuralist reading of *Discipline and Punish* which obfuscates the role of human agency in panopticon societies is rather misplaced. He proposes that *Discipline and Punish* must be read as a voluntaristic rather than deterministic. Critics (Bauman, 2000; Boyne, 2000) of the panopticon metaphor of surveillance argue that instead of immobility, isolation and enclosure envisaged by Foucault, modern surveillance societies are characterised by mobility and the permeability of boundaries as citizens come and go at will. The population is not containable and therefore it is not isolatable. Citizens cannot be held in place long

enough for the panoptic mechanism of 'being seen without being able to see' to work its magic. Because of these social conditions, Norris (2002) posits that the panopticon model is analytically limited beyond the forced enclosures of "total" institutions (Goffman, 1959).

Adding their voice to the critiques which have been levelled against Foucauldian theorisation, Haggerty & Ericson (2000) argue that the deployment of the panopticon metaphor is not suitable for analysing surveillance in the information society, because surveillance would no longer serve the single coherent purpose of control. Haggerty argues that the panopticon directs scholarly attention to a select group of surveillance attributes while neglecting "a host of other key qualities and processes of surveillance that fall outside of the panoptic framework" (2006: 23). Haggerty goes further with this same criticism stating that "the panoptic model does not contain an image of resistance" (2006: 36). There are two problems with the Foucauldian literature outlined above. First, surveillance subjects are portrayed as "passive" subjects or "docile bodies", rather than social agents who may negotiate, modify, evade or deny surveillance practices (Coleman and McCahill, 2011). Second, Foucauldian accounts of "the movement of panoptic principles into new settings [are] often presented as entirely frictionless" and lacking any "sense of a surveillance politics" (Haggerty, 2006: 34). Their conceptualisation of modern-day surveillance captures its plural manifestations rather than the singular and an all-powerful force envisaged in Foucauldian writings. This represents a sort of postmodern mutation of earlier practices that is decentralised, polycentric and only very partially predictable (Lyon, 2003). They highlight the ways in which contemporary surveillance no longer follows an exclusively unidirectional "top down" or panoptic model, thereby opening up spaces to explore the ambiguities and ramifications of surveillance power. Next, I look at post-panoptic approaches to surveillance.

(b) Post-panoptic theories of surveillance

Post-panoptic approaches to surveillance seek to account for Information and Communication Technologies (ICTs) and technological advances which took place after the Foucauldian theorisation, as well as to raise the shortcomings of panoptic theories to explain contemporary practices. As a result, most scholars (Haggerty and Ericsson, 2000; Mathieson, 1997; Marx, 2002; Caluya, 2010) have turned their attention away from Foucault in an attempt to understand contemporary social and technological developments in surveillance and society. For instance, Simon (2005) argues that Foucault's over-emphasis on the state as the agent of surveillance appears too restricted in a society where both state and non-state institutions are involved in massive efforts to monitor different populations. Although "Foucault continues to reign supreme in surveillance studies", Haggerty (2006: 27) proposes that "it is perhaps time to cut off the head of the king".

Unlike modernist theories of surveillance which are largely structuralist and deterministic, thereby affording little space for human agency to resist repression, enclosure and total institutions, post-modernist surveillance scholars (Lyon, 2006; Haggerty, 2006; Marks, 2005) question the analytical relevance and power of the panopticon metaphor. Contrary to Orwell's prediction that the "proles" (which means members of the working class) would largely be exempt from surveillance, post-modern theorists of surveillance argue that the multiplication and intensification of surveillance leaves no one safe from its reach. As Bogard (2012: 33) observes, the disciplinary model of surveillance has proved too inflexible "to organise the mobile labour forces and financial flows of complex information economies". Within the Foucauldian theorisation, "the movement of panoptic principles into new settings" is "often presented as entirely frictionless" (Haggerty, 2006: 34). This assumes that surveillance is not resisted at any level by individuals and there is absence of both overt and covert mobilisation against such practices. The central argument presented here is that the Foucauldian- and Deleuzian-inspired literature outlined above does not adequately address the politics of surveillance by explaining why or how new surveillance technologies have come to play such a central role in contemporary society.

In what has been termed the Deleuzian turn in surveillance studies, Haggerty & Ericson (2000) propose the notion of "surveillant assemblages" as a break from Foucault's panopticism. Drawing on Deleuze and Guattari's notion of "assemblage", Haggerty and Ericson use the term "surveillant assemblage" to render visible processes of surveillance in which information is abstracted (or deterritorialised) from human bodies in data flows and reassembled (or reterritorialised) as "data doubles" (2000: 606). Centralised panoptic control is less an issue than polycentric networks of surveillance, within which personal data flow fairly freely (Boyne, 2000). These polycentric surveillance flows are as much a part of the so-called network society as the flows of finance capital or of mass media signals that are taken to herald the information age or postmodernity (Lyon, 2003). This suggests the liquidity of surveillance, societies which abound with surveillance—formless and diffuse—'liquid surveillance' (Bauman, 2000). Unlike the Panopticon which was presented as a neat pyramid-like structure of control (Foucault, 1977), the "surveillant assemblage" is much more like a creeping plant that sends out shoots here and there, growing rhizomically (Haggerty and Ericson, 2000). In this "surveillant assemblage", surveillance is considered to be a dispersed and rhizomatic phenomenon, being conducted by an unrelated multiplicity of groups and practices. The conglomerate of surveillance entities instead seeks to break the individual into a desired set of discrete data, called flows. These flows represent the many streams of information that contribute to databases, circulate in information networks, and form an individual's data self. It

draws attention to processes of information extraction in late modernity, the rhizomatic expansion of surveillance and non-disciplinary forms of surveillance.

In the same vein, Braman (2006) points out that the traditional notion of panopticon-style surveillance has been replaced by the "panspectron", in which information is gathered about everything, all the time. Other scholars (Bogard, 2006; Clarke, 1988; Albrechtslund, 2008) have coined various terms to account for the shift from traditional panoptic approaches to surveillance towards post-modernist theorisation. For instance, Clarke (1988: 2) coined the term "dataveillance" to denote the "systematic monitoring of people's actions or communications through the application of information technology". Bogard (2006) propounds the notion of as "hyper-surveillance" in line with the Baudrillardian vision of simulated surveillance. He views the future as characterised by surveillance without limits, which aspires not only to see everything, but to do so in advance. Bogard connects this with the desire for control as the long-term goal of many technologies, insisting that simulation's seductive claim is that "any image is observable, that any event is programmable, and thus, in a sense, foreseeable" (1996: 16). In the same vein, Albrechtslund (2008) coins the term participatory surveillance. According to him, "the practice of online social networking can be seen as empowering, as it is a way to voluntarily engage with other people and construct identities, and it can thus be described as participatory' (Albrechtslund, 2008).

Several scholars (Mathiesen, 1997; Poster, 1997; Bigo, 2006; Bakir, 2015) have experimented with the term "panoptic" to capture contemporary mediated, technological surveillance. These include the synopticon (the "viewer society" where the many watch the few (Mathiesen, 1997: 219)); the super-panopticon (where computer databases construct subjects with dispersed identities (Poster, 1997)); the banopticon (the security state's power to ban inadequate individuals (Bigo, 2006)); and the oligopticon (a networked form of surveillance nodes comprising special places such as parliaments, court-rooms and offices where sturdy but narrow views of the (connected) whole are generated, as long as connections hold (Latour, 2005)). In contrast to such terminological playfulness with the central metaphor of panopticon, Bakir (2015) posits that conceptual clarity of the post-Snowden condition is heightened by maintaining intact the term 'panoptic' (with its centralising, state-oriented and disciplinary functions) and coupling it with 'assemblage' (highlighting the multi-site and fluctuating nature of data capture to form data-doubles)) and bringing these together with 'veillance[8]' (highlighting that flows of watching are multidirectional

[8] This refers to the processes of mutual watching and monitoring by surveillant organisations and sousveillant individuals (Mann, 2013).

involving citizens, retail and communications companies, and state agencies) accurately describes the contemporary condition of mutual watching.

In an attempt to address the complicated post-Snowden condition of mutual watching, Bakir (2015) introduces the concept 'veillant panoptic assemblage' as a new way of foregrounding resistive possibilities to surveillance. Given the various types of veillance possible (including not just surveillance but also sousveillance[9], counter-veillance, univeillance and equiveillance), 'veillant panoptic assemblage' suggests that resistance to surveillance may be attempted in different ways. Bakir (2015) demonstrates that flows of watching and monitoring are multidirectional: they may comprise citizens monitoring themselves and others (including power-holders), retail and communications companies monitoring customers, and the state monitoring everybody. Third, that resistance to surveillance is mostly about personal 'protection measures' that makes the individual feel better, but are likely not much more 'secure'. More important, 'protection' from the 'surveillance threat' is often understood as a series of measures undertaken by individuals, hiding the collective possibility for resistance (Fernandez and Huey, 2009).

Similar to panoptic theories, post-panoptic approaches to surveillance have also been criticised for adopting a structural focus, thereby ignoring the individual's perspective and the broader implications of surveillance (Caluya, 2010; Friesen, Chung and Feenberg, 2006). For instance, post-panoptic approaches view individuals as collected pieces of data, or flows, that are removed from any individual context to be reassembled as a 'decorperealised body, a data double of pure virtuality' (Haggerty and Ericson, 2000:611). The approach therefore divorces an individual from their context. As Lee-Ashlin (2012) observes, post-panoptic theories have also failed to explore the role of the individual within totalitarian institutions. Scholars (Caluya, 2010; Lee-Ashlin, 2012) suggest that Foucault recognises the individual in greater detail than post-panoptic theories, providing a framework for understanding aspects of an individual experience. Post-panoptic approaches also fail to answer how individuals make sense of, resist or even embrace surveillance in their everyday lives (van Brakel and Bernhard, 2009:213).

Although the field of surveillance studies is dominated by many valuable perspectives on surveillance in terms of describing how surveillance functions, detailing cases of surveillance, the expansion of surveillance, as well as theoretical perspectives on surveillance, there is very little on resistance to

[9] Sousveillance is 'watching from below,' a form of inverse surveillance in which people monitor the surveillors. It includes citizen video, watchdog web sites, or the monitoring of authorities (corporations, military, and government). It also embraces the idea of transparency as an antidote to concentrated power in the hands of surveillers.

surveillance (Geesin, 2012). This is aptly corroborated by Fernandez and Huey (2009: 198) when they say that 'surveillance scholars have paid relatively little attention to the issues of resistance'. Despite being central to the dynamics of surveillance, the concept of resistance remains underdeveloped within the surveillance studies corpus (Martin, van Brakel and Bernhard, 2009: 213). Haggerty (2006: 34) partly addresses this lacuna in literature when he highlights the importance of surveillance politics, which include 'processes of public claims-making, civil disobedience and more theatrical and artistic interventions to eliminate or mitigate the perceived excesses of surveillance'.

Resistance against Surveillance

Resistance to surveillance refers to 'any active behaviour or interest groups that oppose the collection and processing of personal data, either through the micro-practices of everyday resistance to defeat a given application or through political challenges to wider power relations contest the surveillance regime per se' (Coleman and McCahill, 2011: 147). As Geesin (2012) notes, practices of resistance can be developed through practices which uncover the flaws and limitations of surveillance, practices which allow individuals to evade surveillance and practices which allow individuals to subvert the surveillance technologies for other purposes. This can also be done through subverting surveillance technologies' intended use. In this sense, surveillance technologies are often *détourned* where individuals re-appropriate the technologies to either suit their own purposes or, more significantly, as a subversive method of turning the surveillance practices' backs upon those wielding control (Geesin, 2012). Mann (2013) proposed the concept of sousveillance to analyse the various ways individuals resist surveillance. He discusses two types of sousveillance: hierarchical and personal. Hierarchical sousveillance involves recording surveillance systems, proponents of surveillance and authority figures to uncover the panopticon and 'increase the equality' between surveillee and surveiller (Mann et al., 2003: 333). It also encapsulates sousveillant individuals using tools (such as camera-phones) to observe organisational observers, enhancing people's ability to access and collect data about their surveillance in order to neutralise it, and to act as a consciousness-raising force to the surveillance society. Activists use technologies such as video recording against the surveillance authority, photographing police officers, photographing government officials and beaming satellite shots of security forces harassing protestors. Personal sousveillance denotes the recording of an activity by a person who is party to that activity, from first-person perspectives, without necessarily involving political agendas (Mann, 2004). This includes the use of social media, whereby people curate and create content, thereby revealing their lives, thoughts and feelings.

In his work on welfare surveillance, Gilliom (2001) describes a variety of measures welfare recipients use to resist invasive surveillance, including changing living arrangements and not declaring paid work. Because poor and underprivileged people often lack the resources to organise formal protests and resistance campaigns, they resort to ad hoc resistance techniques, including food stamp fraud and withholding information from the welfare administration (Gilliom, 2001; Gilliom and Monahan, 2012). This kind of research suggests that even seemingly powerless actors can successfully undermine the surveillance mission. Anderson and Snow (1995: 191) identify different strategies and practices used by low income Americans to circumvent donor surveillance systems through over-hydrating in order to meet the weight requirements of for-profit plasma firms who buy blood. These illustrations show how people go an extra mile to beat the surveillance system in everyday life.

There is a debate amongst scholars (Gilliom, 2001; Gilliom and Monahan, 2012; Handler, 1992; Marx, 2003) on the efficacy and relevance of everyday forms of resistance with regard to political struggles. Scholars like Gilliom (2001) point out that everyday resistance represents one of the most important dynamics in understanding the politics of 'movements' of staggering proportions. He argues that these practices of everyday resistance mobilised a trenchant critique of the compelled visibility of surveillance. Thus the critiques of surveillance are found in the actions of evasion, in the practices of trickery, in the tactics of masking—these actions simultaneously critique the goals and policies of the surveillance system. As Gilliom and Monahan (2012) note that these people engage in practices of everyday resistance; the central characteristics of everyday resistance practices are that they are unorganised, not explicitly tied to broader ideological critiques and originate from the direct concerns of everyday life. On the other hand, scholars like Handler (1992) argue that the focus on practices of everyday resistance glorifies petty acts of individualistic crime and deviance and saps attention from the important work of more public and organised groups and movements. Handler (1992) argues that progressive scholars should focus on learning about potentials for strong, public, transformative movements and eschew the celebration of often petty, unthinking, individualistic moments of everyday resistance. Below, I look at the everyday forms of resistance as a conceptual resource to analyse how surveillance subjects adapt to and resist communication surveillance in South Africa.

Everyday forms of resistance

The dearth of conventional collective action among the subaltern groups (the poor, peasants, and women) in the developing countries, 'together with a disillusionment with dominant socialist

parties, pushed many radical observers to 'discover' and highlight different types of activism, however small-scale, local or even individualistic' (Bayat, 2010: 43). Because focusing on grandiose movements of collective protest has sapped attention from examining the 'more enduring, everyday forms of resistance constantly present in the behaviours, traditions and consciousness of the subordinate' (Haynes and Prakash, 1991), scholars like Scott (1976) and Bayat (2010) have directed our attention to small-scale and quiet encroachment into daily life. Scott's theory of micro-politics and everyday resistance benefited extensively from post-structuralist writings, especially Foucault's 'decentred' notion of power, and neo-Gramscian politics of culture (hegemony). In his three books, *The Moral Economy of the Peasant: Rebellion and Subsistence in Southeast Asia* (1976), *Weapons of the Weak: Everyday Forms of Peasant Resistance* (1985), and *Domination and the Arts of Resistance: Hidden Transcripts* (1990), Scott founded his theory on the bedrock of the Foucauldian idea that 'wherever there is power there is resistance' (1978: 95). Despite popularising the idea of panopticism as discussed earlier, Foucault acknowledges that there is a symbiotic relationship between forms of resistance and control. Unlike Foucault who under-theorised resistance by over-emphasising pervasive constraints and their changing logics over time, Scott's theory foregrounds small-scale, everyday, tiny activities that the agents could afford to articulate given their political constraints. Instead of revolutionary social and political change, everyday forms of resistance acknowledge that local should be recognised as a significant site of struggle as well as a unit of analysis; that organised collective action may not be possible everywhere, and thus alternative forms of struggles must be discovered and acknowledged (Bayat, 2010: 48). This approach expands the domain of politics to practices of everyday life (to what Scott calls the 'infrapolitics of the powerless') beyond formal organisations and collective mobilisations.

Scott (1985) devised the theory of everyday forms of resistance after studying the politics in the relations between the rich and the poor in a small Malaysian village. As Scott (1990: 128) observes, 'If the logic of a pattern of domination is to bring about the complete atomisation and surveillance of subordinates, this logic encounters a reciprocal resistance from below'. It follows that as the state erect different governmentality strategies to exercise hegemonic power, ordinary citizens construct their own to resist this power. Similar to Bourdieu who focused on everyday forms of 'symbolic violence' that are harder to detect than 'real' violence, Scott foregrounds insidious forms of resistance practised by the weak at the expense of the powerful. Scott and Tria Kerkvliet (1986: 1) analyse forms of resistance that share common features: 'They require little or no co-ordination or planning; they often represent forms of 'self-help'; they typically avoid any direct symbolic affront to authority; and they are generally underwritten by a sub-culture of resistance'. As Bayat (2010)

observes, these 'weapons of the weak' should not to be confused with survival strategies. Everyday forms of resistance are conscious and are, therefore, acts 'intended either to mitigate or deny claims asserted by superordinate classes' (Scott 1985: 290). Although Scott's theory was developed to understand hidden forms of peasant resistance in Malaysia, Eckstein (1989: 8) has extended the theoretical cloth to understand 'other economically subordinate groups'. Eckstein also acknowledges that 'such quiet forms of defiance rarely result in major change (1989: 8).

In his seminal book, *The Practice of Everyday life*, de Certeau (1984) appropriated Scott's theory of everyday forms of resistance when he discusses tactics as the art of the weak in Latin America. De Certeau notes that tactics constitute individual moments of resistance to institutional strategies of control. Although he used the theoretical template from a linguistic and cultural perspective, de Certeau (1984) wrote about the subtle ways in which ordinary people resist systems from within and poach upon structural constraints through a series of fluid, agential tactics. Individual action, de Certeau observes, is never totally reducible to the structures in which it occurs. Like Scott, de Certeau calls for scholarly attention to resistance and other tactics as an optimistic, affirmed response to the over-determined construct of discipline and control (as evidenced in Foucauldian theorisation). De Certeau writes:

> If it is true that the grid of 'discipline' is everywhere becoming clearer and more extensive, it is all the more urgent to discover how an entire society resists being reduced to it, what popular procedures (also miniscule and quotidian) manipulate the mechanisms of discipline and conform to them only in order to evade them (1984: xiv).

For de Certeau, all resistance tactics automatically occur at the margin of society. He sees '*l'homme ordinaire*' (the ordinary man; for the author, a hero) as a silent master of everyday experience because he/she does not interpret or translate his/her experience as 'experts' do; but he/she creates his or her own text as he/she goes along. As de Certeau (1984) notes, the task is not to discover how discipline works but instead how people work within disciplinary structures (surveillance societies) to create and live—not as passive, 'docile bodies,' but as social actors and community members. This is very important for this particular study which is interested in understanding how a selected constituency of social actors in South Africa adapt to and resists communication surveillance. According to de Certeau (1984), discipline is constantly deflected and resisted by those who are caught in its 'nets', and their 'dispersed, tactical, and makeshift creativity' constitutes an 'anti-discipline' (counter-surveillance) which was under-theorised by Foucault. De Certeau's postulation is based on the idea that ordinary people extract ways of resisting from the products and goods that they acquire each day as consumers—items as mundane as newspapers, television programmes and

groceries. This means that although consumers (social actors) cannot totally escape the dominant cultural economy, they can adapt it to their own ends. De Certeau uses the French term *la perruque* to refer to various tactics and strategies of everyday resistance. Scott and de Certeau have been criticised for celebrating resistance, thereby obfuscating the density of official sensors. For Scott (1985: 292) to discount everyday resistance fundamentally misconstrues the very basis of the economic and political struggle conducted daily by subordinate classes in repressive [surveillance] settings'. Relationships of power are produced, in part, through the many invisible and half-seen, acknowledged or ignored, quotidian practices of resistance.

Everyday resistance is a unique subset of resistance and opposition to surveillance: the category specifically excludes organised movements, traditional ideology and public confrontations. Anti-surveillance protests by labour unions or litigation over privacy rights are not practices of everyday resistance to surveillance (Gilliom and Monahan, 406). Lying, evading, asking and cheating are some of the often invisible forms of everyday resistance to surveillance. This does not mean that public and formal opposition to surveillance are not important – but spotlights attention on the frequency of everyday resistance to surveillance. In '*A Tack in the Shoe: Neutralising and Resisting New Surveillance'*, Marx (2003) documents 11 categories[10] of tactics that individuals use in everyday struggles against surveillance. He criticises what he refers to as 'the sky is falling' approach which is synonymous with panoptic theories of surveillance and insists that 'the potential of a technology for harm needs to be kept distinct from its realisation' (Marx, 2003: 371). The argument here is that everyday strategies of resistance' (Scott, 1990) might be carried out under the nose of a totalitarian state regime.

In *Overseers of the Poor*, Gilliom (2001) indicates that interviewed women had very little interest in conventional forms of politics, but engage in widespread patterns of everyday resistance as they subvert the surveillance regime when they feel it prevents them from being good parents. As Bourdieu and Wacquant (1992: 102) observe, while 'those who dominate in a given field in a position to make it function to their advantage…they must always contend with the resistance, the claims, and the contention…of the dominated. This also chimes with Giddens' (1985) 'dialectic of control' which underscores the inter-relational conception of power, emphasising the roles of both dominant and subjected actors to the normalisation of control. For Giddens, 'all forms of

[10] These include: discovery moves, switching moves, avoidance moves, piggy backing moves, distorting moves, blocking moves, masking moves, breaking moves, refusal moves, cooperative moves and counter-surveillance moves.

dependence offer some resources whereby those who are subordinate can influence the activities of their superiors' (Giddens, 1985, 16).

The South African Political Context

The Snowden revelations of mass communications surveillance have provided unprecedented information on state-based surveillance mechanisms (Hintz, 2014). Questions have been raised as to whether South Africa is safe from mass communications surveillance. As Duncan (2014) highlights, the communications of South Africans are probably already being caught in the National Security Agency (NSA) dragnet, given that cloud services like Google, Microsoft and Yahoo store their information on US servers. Whilst South Africa is not a terrorist target, Duncan (2014) argues that high incidences of social protests and xenophobic attacks against foreign nationals suggest that the temptation is there for less principled members of the security apparatus to abuse the state's surveillance capabilities to advantage the faction currently in control of the ruling African National Congress (ANC) and disadvantage their perceived detractors. High rates of service delivery-related protests have seen Alexander (2012) characterising South Africa as the 'capital of social protests in the world', although there is no comparative measure of protests around the world. Another key area which makes South Africa an interesting case for studying communication surveillance is its strong tradition of investigative journalism, protest culture and academic freedom. As Duncan (2014) notes, the state could easily misuse its surveillance capabilities to harass investigative journalists and expose their confidential sources of information, especially if they threaten ruling interests.

Despite the fact that South African legislation does not allow for mass communications surveillance of people even if they are not considered suspects, academics, investigative journalists, political activists and trade unionists have raised concerns that state intelligence structures may be monitoring their work (Duncan, Finlay, Groome, Comninos, & Esterhuysen , 2014; Right2Know Campaign, 2014). As the R2K Campaign (2014) argues, this is seen as part of a local 'rise of the securocrats[11]', where South Africa's security cluster is becoming increasingly powerful, secretive, and involved in political affairs of the country. Media reports (*Mail & Guardian*, 2014; *The Sunday Times*, 2014; Swart, 2015) in South Africa also show that state surveillance has been carried out outside of the Regulation of Interception and Communication-Related Act (RICA) legal framework (this law governs targeted communication interceptions) in ways that violate the right to privacy as

[11] Securocrats are officials located within the security establishment – the police, intelligence services or the military – that have the power to influence government policy in their favour (Duncan, 2014).

enshrined in the Constitution. For instance, in 2005, the state's mass surveillance capacity was misused to spy on perceived opponents of the then contender for the presidency, Jacob Zuma (Duncan, 2014). In a related incident, some of the leading figures in the Scorpions[12] had their phone calls listened to while they were finalising corruption charges against Jacob Zuma during his ascendency to the Presidency. This constituted mass surveillance practices in contravention of the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) of 2002 which regulates targeted surveillance. Public officials in South Africa have also had their communications intercepted by the state. For instance, the former Chief of the South African Revenue Service, Oupa Magashula, was caught on tape making an improper offer of employment to a young woman (Duncan, 2014). The tapes were intercepted as part of a sting operation on the former South African Police Service (SAPS) chief, Bheki Cele (Duncan et al., 2014). It is important to bear in mind that although the media has been instrumental in raising red flags on mass surveillance practices, it tends to focus on exceptional cases involving the elite and public officials at the expense of the ordinary everyday workings of the RICA process.

The Crime Intelligence Division of the South African Police Service (SAPS) also took advantage of the low threshold of targeted surveillance as set out in RICA to obtain judicial approval to intercept the mobile phones of two *Sunday Times* journalists (Stephan Hofstätter and Mzilikazi wa Afrika) in 2010 by giving fictional names and suggesting such interception was needed to investigate a criminal syndicate. Subsequently, the *Sunday Times* took the case to court and two officers were charged with violations of RICA. This incident has fuelled fears that other applications to tap the communications of journalists and public figures may have been granted under false pretences. Not only journalists have been targeted for state surveillance, but trade unionists have not been spared either, with media reports indicating that state intelligence officers were spying on senior National Union of Metalworkers of South Africa[13] (NUMSA) officials as well as attempting to recruit some of their members work as spies. A document titled *Exposed: Secret Regime Change Plot to Destabilise South Africa,* identified NUMSA general secretary, Irvin Jim, and deputy general secretary, Karl Cloete, as leading the plot against the state. The document also named former intelligence minister Ronnie Kasrils, Professor Chris Malekane, Professor Patrick Bond, Professor Noor Nieftagodien, Professor Peter Jordi and Moeletsi Mbeki, brother of former president Thabo Mbeki, as some of the plotters (*Mail and Guardian,* 2014). Following the leak, NUMSA indicated

[12] The Directorate of Special Operations (also, DSO or Scorpions) was a multidisciplinary agency that investigated and prosecuted organised crime and corruption. It was a unit of The National Prosecuting Authority of South Africa. It is now known as the Hawks.

[13] The union was recently expelled from COSATU for rejecting the tripartite alliance with the ANC. It is in the process of forming the United Front (a political platform) aimed at merging workplace and community struggles.

that they would approach the Inspector-General of Intelligence's Office to ascertain whether there has been any surveillance of their senior officials and allies.

According to the *Mail and Guardian* (2014), academics based at the University of Johannesburg who were at the forefront of research projects focusing on the Marikana massacre have experienced a series of thefts which have raised the question of whether they are targeted by the state or non-state actors for their investigation of service delivery protests. These include Professor Peter Alexander, who is the South African Research Chair in Social Change and Dr Carin Runciman. Another academic, Patrick Bond, of the University of KwaZulu-Natal, had his office broken into and ransacked in 2014. This suggests that academic freedom and critical engagement in South Africa is under siege (*Mail and Guardian*, 2014). The foregoing illustrative cases of investigative journalists, politicians, trade unionists and academics being surveilled by the state demonstrate the corruptible nature of South African interception capabilities.

The South African government directly provided public funding to a surveillance technology company, VASTech in 2008 and 2010. According to the *Mail & Guardian*, the South African government continues to fund VASTech. In the mid '2000s, VASTech supplied mass surveillance technologies to the Libyan government of Colonel Gadhafi. A leaked report also reveals that sometime in 2005, an Iranian delegation met with the South African government and companies such as VASTech in a bid to obtain surveillance technology (Privacy International, 2015). In 2011, VASTech sold of one of its surveillance products, Zebra[14], to the Libyan government during the height of the Arab Uprising. This suggests that South Africa can be characterised as a 'surveillance state' (Lyon, 2002) in terms of being involved in the manufacturing surveillant technologies and using them to spy on their own citizens and people from other countries. In an article titled: *Big Brother is listening on your phone*, Heidi Swart (2015) highlights that it is easier for law enforcement agencies in South Africa to obtain meta-data illegally from telecommunications operators. Rather than following the procedure which requires law enforcement officials to apply to a high court judge, a regional court magistrate or a magistrate for a court order, interviewed police officers indicated that they simply approached service providers and requested information related to specific cellphone numbers relevant to their cases. One of the police officers noted that the major reason for circumventing the RICA process is because it is a lengthy process which could hamper case investigation (Swart, 2015). These cases show that it is easy to get access to someone's meta-data without a warrant as outlined in RICA. It also demonstrates that even telecommunication

[14] Zebra enable the security services to capture 30 to 40 million minutes of mobile and landline conversations a month and archived them for years. It helps security services identify relationships between individuals based on analysis of their calling patterns.

service providers or the RICA judge can be bypassed by the OIC and police crime investigation division when it comes to interception of communications.

According to the *Sunday Times* (2015), the parliament of South Africa has recently launched an aggressive onslaught against its own staff in an attempt to root out spies and whistleblowers. It reports that employees have been told to remove their batteries from their cellphones during meetings. Members of the State Security Agency[15] (SSA) have also told parliament staff that they would not hesitate to screen communications such as WhatsApp, SMSes and email. Swart (2015) also reports that the SSA and SAPs crime intelligence unit have acquired surveillance equipment like the grabber[16], which enables them to track the whereabouts of a mobile phone and monitors the communications in real time. Reports indicate that there are also private citizens who are using grabbers illegally in South Africa. These are generally used by moneylenders to locate evasive debtors. The use of these surveillance gadgets which are not regulated by RICA suggests the violation of law on the part of the police and intelligence agencies. In the context of mandatory SIM card registration as required by RICA, the use of grabbers further undermines citizens' rights to privacy and freedom of expression.

In view of the foregoing social context, it is necessary to know more about resistance to surveillance practices in order to document and publicise on best practices which can be replicated by constituents. These best practices can also be used by various constituents to conduct capacity building workshops and to mount covert resistance movements against surveillance practices. It is therefore of the upmost importance that any proposed changes have a solid research base and are supported by a broad, persuasive campaign. This is also important because it enables us to know the various kinds of support networks which exist or are needed to assist individuals. It helps us to understand the complex interaction between structure (surveillance technologies) and agency (human creativity) which Giddens (1984) calls 'structuration'. For Giddens, "all forms of dependence offer some resources whereby those who are subordinate can influence the activities of their superiors" (Giddens, 1984: 16).

[15] The department of state security is part of the South African government with overall responsibility for civilian intelligence operations. It was created in October 2009 to incorporate the formerly-separate National Intelligence Agency, South African Secret Service, South African National Academy of Intelligence, National Communications Centre and COMSEC (South Africa).

[16] The grabber, generally installed in the back of a van, consists of a laptop, one or more antennae and a compact base station the size of a shoebox or desktop computer tower, depending on the model. It forces a cellphone to connect to it instead of a real cellphone tower.

Methodology Approach

This report deploys qualitative research methodology. The advantage of qualitative research is that it allows one to understand social phenomena from the perspective of social actors, to retrieve experiences from the past and to gain insight into the everyday practices of social actors (Babbie & Mouton, 1989). It starts from the assumption that in studying people, researchers are examining a creative process whereby humans produce and maintain forms of life, society and systems of meaning. Qualitative research methodology puts emphasis on 'thick descriptions' (Geertz, 1973), which are the detailed description of the phenomenon under study. As Bryman (1988: 63) observes:

> This emphasis on description entails attending to mundane detail; the apparently superficial, trivia and minutiae of everyday life are worthy of examination because of their capacity to help us understand what is going on in a particular context and to provide clues and pointers to other layers of reality.

In-depth interviews

In order to answer the main research question of this study, interviews were conducted with purposively and snowball sampled civic activists, investigative journalists, academics and human rights lawyers. These 'surveillance subjects' (McCahill and Finn, 2014) were chosen from organisations that have experienced different kinds of surveillance. An interview is a conversation where an interviewer seeks responses from an interviewee for a particular purpose (Gillham, 2000). The qualitative research interview seeks to describe and analyse the meanings of central themes in the life worlds of the subjects. The main task in interviewing is to understand the meaning of what the interviewees say (Kvale, 1996). The purpose of data collection through in-depth individual interviews in this study was to get detailed descriptions of first-hand experiences from interviewees (Rubin and Rubin, 2005: 2-3). An in-depth individual interview is a process of obtaining detailed data on how and why interviewees construct meaning (Babbie and Mouton, 2001: 291).

'Surveillance subjects' for this study were recruited for interviews through a combination of personal contacts and purposive and snowball sampling. Interviewees were purposively sampled from a population of people who have experienced physical and electronic surveillance by the state. Some of the respondents have had their communications incepted, computer passwords tampered with, houses broken into and telephone conversations intercepted by the authorities. An activist handbook produced by the R2K Campaign (2014) titled: *Big Brother Exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements* also provided a list of

possible interviewees and their contact details. This handbook was produced by R2K's focus group on secrecy & securitisation. The researcher also took advantage of the 'Resisting Surveillance Workshops' (19 to 20 October 2015) hosted by the Right2Know Campaign in Johannesburg to solicit further information from activists, lawyers and communication surveillance experts (from Privacy International). The main concern of this report was to explore how journalists, academics, civic activists and human rights lawyers experience and respond to threats of surveillance. With this in mind, I conducted a total of twenty three interviews with a constituency of social actors who have been identified as at risk of communications surveillance. In line with Yar's (2003: 264) suggestion, the rationale behind my choice of 'surveillance subjects' was to explore the experiences of those who regularly find themselves in specific 'interactional contexts and social scenarios' where attention to new surveillance is required.

Most of the interviews took place in Johannesburg. Data for this report is based on qualitative interviews conducted between 1October and 30 November 2015. Respondents were interviewed face-to-face, by email and telephonically. Some of the interviewees volunteered to answer the questions sent to them via their professional and personal emails. Semi-structured interviews were chosen, as they permitted participants considerable opportunity to elaborate and expand on issues they considered of importance within the context of thematic questions devised by the researchers (Wilson and Serisier, 2010). Because of the political proclivities around the research, some of the respondents from trade unions (the National Union of Metalworkers of South Africa (NUMSA) and Association of Mineworkers and Construction Union (AMCU)) pulled out of the study during the data collection stage. The researcher repeatedly requested interviews with senior officials from NUMSA and AMCU, but after initially stating they would consider our request, the representatives stopped replying to my emails. These trade unionists were pursued because as stated earlier they have experienced various kinds of surveillance. The reluctance to take part in the study on the part of NUMSA could be attributed to their recent encounters with fly-by-night 'researchers'. According to the R2K Big Brother Exposed handbook (2014), one of the NUMSA members in Port Elizabeth was approached by a person who identified himself as a 'researcher' at the University of KwaZulu Natal (UKZN), who was interested in finding out more about the United Front (UF). After getting some documentation on NUMSA's activities, and interviewing several NUMSA members and UF affiliates, the 'researcher' disappeared into thin air.

Ethical considerations in communications surveillance research

Qualitative researchers face unique, and often ambiguous, ethical dilemmas in disseminating their fieldwork data (Kaiser, 2009). At the core of this dilemma is the conflict between conveying detailed, accurate accounts of the social world while simultaneously protecting the identities of the individuals who live in that particular social world. This constitutes what Guillemin and Gillam (2004) call 'ethically important moments', which are often seemingly routine, that cause researchers to make decisions that have ethical implications. The reflexive nature of qualitative research, its use of unexpected ideas that arise through data collection and its focus upon respondents' meanings and interpretations renders the commitment to informing respondents of the exact path of the research unrealistic (Parry and Mauthner, 2004: 146). The situation is further complicated by the fact that most ethical codes of professional associations and universities offer virtually no specific, practical guidance on disguising respondents' identities and preventing deductive disclosure in qualitative research (Tolich, 2004). Deductive disclosure, also known as 'internal confidentiality' (Tolich, 2004) occurs when the traits of the individuals or groups make them identifiable in the research reports (Sieber, 1992). As Kaiser (2009) observes, breaches in confidentiality can shatter the researcher-subject relationship and can damage public trust in researchers.

Anonymity refers to the process of not disclosing the identity of a research participant, or the author of a particular view or opinion (Grinyer, 2002). Anonymisation is done to 'protect' or hide the identity of research participants and to protect participants from being identified through research locations. As Tolich (2004) notes, the primary concern is whether the people with whom respondents have relationships will be able to identify the respondent given their knowledge of him or her. This is particularly important in this kind of research where confidential information was disclosed during the research process which may cause the participant distress should surveillance authorities get hold of such information. Confidentiality denotes the process of not disclosing to other parties opinions or information gathered in the research process. As Sieber (1992: 52) aptly avers, confidentiality encapsulates the researcher's 'agreements with persons about what may be done with their data'. Taking a very extreme position, Weiss (1994: 131) advises qualitative researchers that, 'Nothing reported from the study, in print or lecture, should permit identification of respondents'.

According to Kaiser (2009), the dominant approach to maintaining confidentiality assumes that the issue can be addressed during data collection, data cleaning and dissemination. This is done through filling in consent form statements, anonymisation and changing all identifying characteristics, such

as occupation, city, and ethnic background of the respondents (Sieber, 1992: 52). Guillemin and Gillam (2004) refer to the process of obtaining approval to conduct research as 'procedural ethics.' They note that procedural ethics, while useful for prompting researchers to think about ethical issues, is largely a formality that cannot address the specific ethical dilemmas that arise in qualitative research. By seeking informed consent prior to the fieldwork process, I was able to alert my research participants on how I would handle the data. Because of the sensitive nature of this kind of research, all the respondents are anonymised to protect their privacy and confidentiality. Instead of adopting 'blanket anonymisation', whereby all names, places and other identifying features are disguised across a data set – including from interview transcripts, diaries and field notes – I deployed 'partial anonymisation' where some important information like the location of the respondent are disclosed. In cases where the respondent agreed to full disclosure, verbatim statements and the name of the organisation are presented without alterations. Similar to Kaiser (2009), I changed very few details in my respondents' quotations. I also withheld incriminating information such as names of people and organisations where the right of reply was required before publication. In this vein, I concur with Singleton and Strait (1999) that complete anonymity in most social research is impossible to achieve.

The next section focuses on the study's findings by giving a synthesised overview of how investigative journalists, civic activists, lawyers and academics are adapting to and resisting communications surveillance in South Africa.

Summary of Findings

This section is divided into four thematic issues. The first thematic area looks at responses from investigative journalists; the second deals with civic activists; the third discusses interview responses from academics and, finally, responses from human rights lawyers. The main thrust of the study is find out how people are adapting to or resisting communications surveillance practices, and how this differs, if at all, from individual to individual. It also documents and analyses the various kinds of support networks which exist or are needed to assist individuals.

(a) Investigative journalists

Research (Human Rights Watch, 2014; Pew Research Centre, 2015) has shown that increased surveillance, combined with the tightening of measures to prevent both leaks and government officials' contact with the media have a profoundly detrimental impact on public discourse. Communications surveillance also affects the role that journalists can play in holding the government to account for its actions. It impedes news coverage of matters of great public concern. Four investigative journalists from Mpumalanga, Cape Town and Johannesburg in South Africa observed that communications surveillance has significantly impacted on their profession. As intimated in the methodology section, all respondents were guaranteed anonymity given the nature of this research. Some of them pointed out that it was now difficult to cultivate reliable sources in various spheres of local, provincial and national government for fear of being surveilled by the security apparatuses. They revealed that while the mobile phone was generally hailed as a tool which has brought efficiency and effectiveness to the journalism profession, it has brought them into the 'dragnet'. This corroborates findings from the Pew Research Centre (2015) which found that about two-thirds of investigative journalists surveyed (64%) believe that the U.S. government has probably collected data about their phone calls, emails or online communications, and eight-in-ten believe that being a journalist increases the likelihood that their data will be collected. On the question why investigative journalists in South Africa are being surveilled by the state, three of the respondents observed that:

> I have been targeted for communication surveillance because of the investigative stories that … newspaper… has been publishing. In my case, he [name withheld], confronted me and accused me of having spoken to a source. The only way he could have known about my telephone discussion could only have been through listening to my telephone conversations. I also noticed that there was a person stationed in front of my offices and I go to the offices infrequently (respondent, Mpumalanga).

> The state—and sometimes private—actors want to discover the sources of embarrassing stories. During the Jackie Selebi investigation, for example, an attempt

> was made to get close to me by a police agent posing as a source. The agent recorded our conversations and details of where I lived, etc. I was also tipped off that he had planned to plant drugs on me. Fortunately, I suspected him from early on and took precautions, such as only meeting in public places (respondent, Cape Town).
>
> We were targeted for our investigative stories which focused on political killings in Mpumalanga and corruption cases involving the Mbombela stadium in Nelspruit (respondent, Johannesburg).

The foregoing interview extracts also highlight that journalists have been targeted for surveillance purposes because of the investigative stories which focus on political killings in Mpumalanga, corruption cases involving the Mbombela stadium in Nelspruit and the Jackie Selebi [former South African Police Service (SAPS) chief) investigation.

Interviewees indicated that they have changed the way they store and share sensitive data. For instance, some of them indicated that they now rely on end-to-end encryption to secure their data. Research by the Pew Research Centre (2015) also indicates that nearly half (49%) of the journalists interviewed have at least somewhat changed the way they store or share sensitive documents, and 29% say the same of the way they communicate with other reporters, editors or producers. In South Africa, investigative journalists pointed out that they are relying more on face-to-face meetings with sources as opposed to telephonic and email interviews. They observed that online communications could easily be surveilled, thereby putting their news sources and whistleblowers at risk of being harassed, killed, fired and tortured. As McCahill and Finn (2014) observe, the ability to make 'discovery' or 'avoidance' moves is shaped by the distribution of capital in the social field and by the 'set of dispositions which incline agents to act and react in certain ways' (habitus). Blocking, distorting, masking, refusing and counter-surveillance moves (Marx, 2003) are relevant for less powerful groups that lack resources to undertake political campaigns of resistance. Although journalists interviewed did not single out specific stories which they haven't been able to pursue because of surveillance or the suspicion/ fear of it, it was noted that stories related to national security, political killings and corruption in high offices were likely to attract targeted surveillance from the state.

Changing investigative journalistic practices and routines?

In an attempt to protect their sources, their data and themselves, some of the respondents reported modifying their practices – their tradecraft – for investigating stories, communicating with sources and protecting their notes. Four strategies were mentioned by the respondents in South Africa as usable to circumvent communication surveillance. These include: end-to-end encryptions email and messaging tools, coded language (with sources), face-to-face communication and drop-off (people

come and drop off documents at newsroom reception). Some journalists have changed their practices in response to surveillance practices they have experienced at a personal level, as well as media reports about the breaches of the RICA process. Investigative journalists from newspapers in Johannesburg indicated that they have also developed their own counter-surveillance techniques with the support of IT and security experts. As Greenwald (2014: 173) observes, 'people radically change their behaviour when they know they are being watched'. Similar to findings by the Human Rights Watch (2014) report, this study found that South African investigative journalists have adopted three broad types of changes in journalistic behaviour aimed at obscuring parts of the reporting process: increasing use of advanced privacy enhancing technology, decreasing reliance on electronic tools and modified use of conventional methods of protecting information and sources.

Like their counterparts in the United States, interviewees in South Africa indicated that they used various forms of encryption software for their communications with sources or colleagues, including emails, chats, texts and phone calls. One of the respondents observed that, 'One either reverts to older practices, such as meeting in person, or much newer ones, such as encrypted communications'. Another journalist from Cape Town noted: 'I ensure encryption of my entire hard drive and specific encryption of some information. And I do not use email and other relatively hackable technologies for specifically sensitive information. Some information does not go onto my computer or cellphone at all'. This corroborates Greenwald's (2014) suggestion that all users should adopt encryption and browsing-anonymity tools. The deployment of encryption tools demonstrates that journalists in South Africa are engaging in 'blocking and masking moves' (Marx, 2003). Masking involves blocking, in that the original information is shielded, but it goes beyond it to involve deception with respect to the identity, status and/or location/locatability of the person or material of surveillance interest (Marx, 2013). These strategies fit with micro-resistance strategies associated with Scott's idea of everyday forms of resistance, as well as Foucault's notion of transversal struggles. According to Foucault (1983), transversal struggles are small acts of resistance to a form of power as a whole. They criticise power for its effects, challenge state control over the individual and fight against privileges created by knowledge or secrecy (Foucault, 1983).

Interviewees from Johannesburg indicated that they did not use cloud-based storage systems because of their inherent vulnerabilities. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centres. Despite their popularity in the global North, investigative journalists pointed out that the cloud-based system is vulnerable to hacking. Another male journalist from the Johannesburg said that 'we

don't use the cloud at all, it's not fool proof. We use Free dome[17] which has a remote server (based in Spain)'. Decryption of cloud-based systems requires a huge amount of computer processing power, forensic software and a lot of time. They also bemoaned that cloud services utilise more complex security methods than the average computer user is able to master. One respondent said that 'intelligence [officers] have backdoors to these technologies'. Respondents indicated that they relied heavily on writing down notes in their notebooks. They took additional precautions with their notes—such as writing them by hand and encoding them. Others indicated that they used coded language for discussing stories or sources. Another journalist from Mpumalanga revealed: 'I ensure that the sensitive information that is provided is stored electronically and any reference or link to the sources is removed. I'm storing information in different physical and virtual locations'. The large variety and complexity of these strategies illustrate the fear that journalists and their sources hold of government surveillance. This means they avoided carrying electronic recording equipment which can easily be switched on, confiscated or stolen. As one of the respondents put it:

> It makes sense to meet your source with only a notebook and a pen. I avoid writing incriminating information like names and phone numbers on the notebook. Sometimes shorthand is used to protect the source and information.

It is clear from the foregoing that investigative journalists are resorting to old ways of news gathering and storage of information in order to protect whistleblowers and news sources. Rather than using smartphones to record conversations with news sources, most of the respondents indicated that they prefer to use simple phones to make calls and appointments. Smartphones are considered too vulnerable to surveillance because of their features which allow for meta-data retention and geo-location identification. Similar findings were reached by the Human Rights Watch report (2014). They found that many journalists have ratcheted back their use of technology. This is largely because calling or emailing can leave a trail between the journalist and the source. Due to the traceability of GPS information from smartphones and the possibility of turning them into listening devices (even if they are off), several journalists reported turning off cellphones or taking out their phone batteries before speaking with people in person, or even leaving phones behind altogether when visiting sources (Human Rights Watch, 2014). In terms of which technologies journalists thought put them at risk of communication surveillance, two of them had this to say:

> Cellphones, particularly when you have the location activated. Another one is Facebook where location is activated.

> I generally consider cellphones very dangerous, followed by landlines and email.

[17] This is a remote virtual private network (VPN) which allows users to browse and save information anonymously online.

> Technologies like Skype and WhatsApp may be safer and specific tools such as GPG, RedPhone and Telegram may be much safer. But there is always the risk of Trojan infiltration, meaning no electronic method should ever be trusted entirely.

Many journalists reported that they now prefer face-to-face meetings with news sources for security reasons. Although they observed that these meetings are expensive and time consuming, it was indicated that the safety of news sources was more important than getting a news article. As one respondent point out:

> People are scared, some get killed for whistleblowing and others get fired. The question is it worth it to endanger other people's lives in order to expose wrongdoings. Are we doing any public good by putting people's lives at risk? It's a constant struggle to balance the public interest and journalism ethics.

Others indicated that there were chances that if a source is found leaking classified information, he/she can be fired, killed, harassed or tortured. Although there are no reported cases of someone being killed for leaking classified stories, journalists interviewed indicated that in a country where unregistered guns are ever-present such incidents could not be ruled out. Another journalist indicated that 'if a source is found guilty of whistleblowing in government, he or she can be victimised or face disciplinary investigations'. As the Human Rights Watch (2014) report show, many of these techniques entail additional costs for journalists – not just the financial costs of additional technology and equipment, but perhaps even more burdensome costs in the time it takes for journalists to go through all the elaborate steps they now need to take to keep their sources protected.

Unlike in the U.S, where investigative journalists use postal services to transmit documents rather than electronic means, in South Africa interviewees noted that whistleblowers preferred to secretly drop off documents at their newsroom office. Journalists and sources have also made creative use of common technologies to hide their interactions. One interviewee from Mpumalanga revealed: 'I have limited the use of telephone and cellular phones and replaced these with physical meetings for discussing sensitive issues'. Respondents in both Johannesburg and Cape Town indicated that they used simple phones and pre-registered SIM cards to make calls to news sources. The importance of this circumvention strategy is that pre-registered SIM cards cannot be traced back to anyone, unlike registered numbers. Marx (2003) argues that people will break rules if they regard certain surveillance procedures as unacceptable or illegitimate, untrustworthy or invalid, irrelevant, demeaning, unnecessary or irrelevant. As one respondent opined:

> Although surveillance authorities may know we talk to them [news sources within government] but because our phone numbers are not registered according to RICA

> requirements they won't know us [journalists]'. Can't use it as official information to catch sources or discipline them.

Thus, 'burner' phones – cell phones with limited identifiable links to the owner and which can be disposed of after a matter of days or weeks – allow journalists to limit their traceability and locatability. In order not to raise red flags with surveillance authorities, these burner phones are often used for a short period. In their study of resistance against mandatory SIM card registration in Africa, Donovan and Martin (2014) found that the most widespread resistance has taken the form of illicit access to pre–registered SIM cards. This type of everyday form of resistance is similar to Marx's (2003) 'switching moves'. Thus, instead of using registered SIM cards, investigative journalists circumnavigate surveillance procedures through switching to pre-registered cards. This further cements the argument that despite government surveillance and other factors that militate against Africans' ability to freely communicate and associate, investigative journalists in South Africa are devising creative ways resisting the 'celebration of victimhood' (Nyamnjoh, 2005).

In a study conducted by the Pew Research Centre (2015), journalists revealed that they have changed the way they communicate with sources. Roughly four-in-ten (38%) have, in the past year, at least somewhat changed the way they protect and communicate with sources (Pew Research Centre, 2015). When it comes to the specific actions journalists are deploying to protect their sources, the most common technique is to meet them in person, followed by turning off electronic devices when meeting sources (18%), avoiding the use of third-party email servers when communicating with sources (17%), using email encryption (14%), using 'fake' or anonymous email and online accounts (14%) and using voice encryption on phones (2%) (Pew Research Centre, 2015). Similar to investigative journalists in the United States of America, respondents in South Africa indicated that they are struggling harder than ever before to protect their sources and sources are more reluctant to speak. It was found from the interviews that some of the interviewees have opted for 'cooperative moves' (Marx, 2003). This entails working with sympathetic agents within the surveillance apparatuses. In such a context, investigative journalism has become very expensive, time consuming and relatively slower. Two respondents had this to say about the impact of communications surveillance on their work:

> It puts a lot of pressure on the journalist to ensure that they cover their digital traces while at the same time meeting pressing deadlines. This slows you down, especially when you need follow up face-to-face discussions.

> I have not avoided platforms altogether, but one takes risks into account before using them. Particularly sensitive conversations are not pursued via phone or email, for example, and in some cases only in person.

In the wake of the Snowden revelations, the *Guardian* and the *Washington Post* established a whistleblower platform called SecureDrop, which allows sources to share information with media organisations anonymously and securely. Some of the South African news media are also members of AfriLEAKS[18]. These news organisations have a dedicated person who is able to receive leaks from AfriLEAKS. One news media organisation based in Johannesburg also makes use of the SecureDrop platform. AfriLEAKS is an online system which enables users to anonymously send material to investigative media organisations of their choice. Besides making use of secure whistleblowing platforms, respondents indicated that some news sources preferred dropping off documents at the offices.

On the question of whether there are any social networks amongst journalists which are assisting them with digital security training and counter-surveillance strategies, one of the respondents emphatically said none. Two respondents indicated that the R2K Campaign was the only organisation working on communications surveillance although they indicated that there was need for more digital security workshops. They also revealed that anti-surveillance campaigns amongst journalists were still non-existent, given the fact that most believed that they are safe and secure. Besides the R2K Campaign, investigative journalists from Johannesburg indicated that they had contacts within IT security companies who helped them with tactics and strategies on how to ring-fence their content and sources. Similar experiences were echoed by another respondent from Cape Town who noted: 'I have sought ad hoc advice from experts and consumed information published by some groups, but I have not had ongoing interaction with specific groups'. Respondents from Johannesburg observed that although they have taken their case of arbitrary surveillance to the court, there was little progress on that front. Respondents felt that security is an individual responsibility since there are so many loopholes at an institutional level. One respondent observed that 'the weakest link in any surveillance practice is the human factor. For instance, cleaners can be bribed or recruited as informers at the shop floor level'. Unlike most journalists interviewed, one interviewee from Mpumalanga indicated that he has devised 'veillant panoptic assemblage' (Bakir, 2015) strategies such as photographing all suspicious people following him or stationed at his offices. He said, 'but I also took photographs of the 'suspect[s]'. This kind of 'counter-surveillance move' (Marx, 2003) involves turning the tables and surveilling those who are doing the surveillance. As Wilson and Serisier (2010) note, the rationale of video and photographic activism is to counter the escalating visual surveillance of protest events undertaken by police.

[18] AfriLEAKS is run by an alliance of African news organisations that are committed to speaking truth to power. The secure web service, developed in partnership with Italy's Hermes Center for Transparency and Digital Human Rights and the Africa Network of Centres for Investigative Journalism (ANCIR)

In terms of what other investigative journalists can do to protect themselves and their sources from surveillance, respondents indicated that 'if you going to go to a meeting with your smartphone then carry a Faraday bag'. Faraday bags enable users to securely seize, transport and examine portable digital devices. These tools ensure that devices are secure from any external interceptions and prevent: remote wiping of the date and losing critical data in a case or tribunal, tracking the device, bugging by remotely using the devices microphone and/or camera and allowing users immediate access to data on a device in a secure manner. Faraday bags are often used by military and intelligence agencies to prevent unwanted applications being invoked remotely or data altered after devices are seized. This entails undertaking 'blocking and masking moves' (Marx, 2003). Masking shares with one form of blocking the goal of eliminating genuine identifying marks. As such, the Faraday bag blocks electronic transmissions. One respondent from the Cape Town recommended that 'A risk-based approach is best. When the risk is great, don't do electronic [communication and storage]'. Another one added that:

> Just assume that your telephonic communication can be surveilled. Never open attachments unless you know the person who has sent them. Go for face to face meetings as a rule and if you are going to mobile phones then use end to end encryption. If you are using phones then recommend you can use cheap [and simple] ones and not smartphones. Encrypt your data and back it up and also use double passwords. The issue is that you need to add too many hurdles so that people won't be able to break through.

The above quotation indicates the various kinds of precautionary steps which journalists ought to take in the era of ubiquitous surveillance. It includes both analogue and electronic ways of circumventing communications surveillance. On the issue of what kind of digital security training would assist investigative journalists in South Africa to resist communications surveillance, one respondent from Cape Town observed that 'hands-on, i.e. people who spend time with individual journalists like myself, analyse our risk profiles, systems and ways of doing things, and helping to implement specific solutions'. A journalist from Mpumalanga also recommended that there was need for the creation and training on of off-site storage facilities on platforms such as iCloud with strict security mechanisms and the development of local applications or platforms for anonymous whistleblowing like SecureDrop and AfriLEAKS. This was supported by another journalist from the Cape Town who said that:

> If whistleblowers and other confidential sources speak to journalists off the record, they have an absolute right to privacy. Not granting them that will discourage them and cut off the flows of essential information. This undermines the constitutional rights of freedom of speech and the media, and of the public to be informed.

From this interview extract, it can be noted that journalists are concerned with communications surveillance which undermines the privacy and confidentiality of news sources.

(b) Academics

This study also interviewed academics at two universities – one in Grahamstown and another Johannesburg – who have experienced what they suspect to be communications surveillance. Some of these respondents have been in the news for having their computers stolen, passwords compromised and houses broken into. These 'surveillance subjects' were interviewed because their narratives shed light on communication surveillance as well as resistance practices they are putting in place to secure their data and research participants.

One aspect of communications surveillance is that it chills academic freedom which constitutes a defining characteristic of a university in a democratic society. This chilling effect corrodes academic freedom and free speech on campus, thus weakening the cornerstones of a healthy learning community. This also has a huge impact on national discourse and the broader public sphere. Academic freedom is premised on the belief that teaching and research should take place in an environment free from domination by the churches and free of government regulation and control (Cary & Watt, 1999). The centrality of research, freedom for teachers to determine what to teach and the freedom of universities from external regulation and control of their activities are the core ideas of academic freedom. As Cary and Watt (1999) point out, academic freedom ensures that research and teaching take place in an environment of free thought, experimentation and creativity. Surveillance tends to induce self-censorship and tilt the research agenda towards topics which are considered palatable to the ruling elite. From the outset, academic freedom was designed at once to protect the independence of disciplinary inquiry and to protect individuals from the exercise of political and economic power, including the power of those who pay professors' salaries (Gerstmann and Streb, 2006).

In the case of this study, it was found that academics who question the dominant neo-liberal ideology which informs ANC's policy making thrust have been targeted for communications surveillance. Researchers working on national issues which the African National Congress (ANC) consider to be 'sensitive', such as the Marikana massacre, xenophobic attacks and fragmentation of the trade unions, were also subjected to varying levels of physical and electronic surveillance. Besides communications surveillance impacting negatively on academic freedom through promoting self-censorship and changing research practice and agenda, one of the interviewees pointed out that there was a lot of gatekeeping, intimidation and harassment by senior academics at

some universities in South Africa. Discussing the ways in which communication surveillance erodes academic freedom and contributes to self-censorship in terms of research interests and projects, one of the respondents from Grahamstown said:

> I need to be clear that I don't know what sort of surveillance I may have been, or may be under. I have had computers and drives taken, with nothing else, and no forced entry. On one occasion that people that came into my house and took my computer identified themselves as agents of the government. I have also been told by the police that I am being watched and once, while I was under arrest and being questioned by officers from crime intelligence, they said they same. But I don't know how credible these statements are, if surveillance is sustained, or what form it may or not take. In my own experience the general conservativism, and racism, of the academy, and the extraordinary authoritarianism within the academic left, have led to far more self-censorship than anything that the state has done. Since 2005 I have known of a number of academics and some students who have told me that they have self-censored due to fears of harassment by [name withheld] and others close to him [name withheld]. I am not personally aware of anyone who has self-censored their academic work due to fear of the state. I have been subject to state harassment due to my journalism (including being told by the police and intelligence, while under arrest, to cease writing in newspapers) but I have never been subject to any intimidation from the state relating to my academic work. However he [name withheld] and others close to him [name withheld] have subjected me to sustained harassment and attempts at intimidation including, over a ten period, a number of written demands for me to withdraw academic work.

The above interview extract illustrates that self-censorship in the academia is not largely fuelled by the fear of the state. One of the respondents from Johannesburg pointed out that they have been targeted for state harassment because of their ground-breaking research on service delivery protests and the Marikana massacre. She had this to say:

> I think we have been targeted because of our research on service delivery protests and the Marikana issue. For me, it's even worse because I am a foreigner working in South Africa focusing on the ills of the post-apartheid democracy. Our research focuses on things that puts the current regime on the spot and goes against the grain in the sense that it disputes the notion that Marikana was caused by the third force. Instead our study shows that protesters were not part of some third-force agenda aimed at destabilising the government. There was very little correlation between the elections and the number of protests, and the protests were for the most part not politically orientated. We found that miners' grievances included: housing, water and sanitation, political representation and electricity.

It is discernible from the above statement that the state is increasingly becoming edgy when it comes to dealing with service delivery protests research. Even the way the police have been handling these accountability conflicts suggests that there is a shift towards militarisation and heavy handedness. Interviews with researchers at the University of Johannesburg indicated that although surveillance was indirectly planting the seed of fear within them, they will continue to research on

service delivery protests. According to one respondent from Johannesburg, the break-ins at her house and the tampering with her Dropbox folder where she stored her interviews with protesters suggest that 'it has got to be state intelligence or someone working with them.' However, some of the junior researchers expressed deep-seated fear about being surveilled by the state. As one of the respondents from Johannesburg noted: 'I am scared just to know that the National Intelligence Agency[19] (NIA) are interested in your whereabouts is reason to fear. Those people mean business when they follow up on you'. Another female researcher noted that:

> Yes, I am afraid but all of a sudden I have realised how important the work we doing is. Because if the NIA are interested in our work it means we are doing something in the public interest.

Interviewees were asked to explain how 'ubiquitous surveillance' (Andrejevic, 2012) has changed the way they communicate with their research participants and professional colleagues. Most of the respondents pointed out that they are now cautious about how they communicate with their research participants. They pointed out that no amount of academic pursuit is worth endangering people's lives. Others pointed out that they have changed their academic practice, although they are not oblivious of the fact that they are still under surveillance:

> We cannot reveal all our new strategies we have developed following our surveillance experiences. But we have certainly changed how communicate with our respondents. We have relooked at the way we store of data and the use of the cloud and services like Dropbox. After losing access to our Dropbox[20] project account [which contained crucial audio recordings of interviews conducted with protesters] last year we have become cautious with so many things.

> We are no longer using mobile phones to keep in touch with the field unless it's extremely necessary. We have other ways of safeguarding the confidentiality of our research respondents. The lesson we've learnt is that researchers need to be less naive, and more vigilant. But I have realised the importance of using focus group discussions in the South African context which allow participants to hold their fellow comrades to account. Participants are not comfortable with individual face-to-face interviews.

Another surveillance subject from Grahamstown revealed that in cases of extreme repression, he has been forced to change his communication practices:

> I have nothing to hide and so I generally speak and write freely. Given that there are also paid informants in political organisations secrecy is not helpful. I write,

[19] The National Intelligence Agency was the previous name of an intelligence agency of the South African government. Currently it is known as the Domestic Branch of the State Security Agency. It is responsible for domestic and counter-intelligence. It has since been absorbed into the State Security Agency (SSA).

[20] Dropbox is a file hosting service that offers cloud storage, file synchronisation, personal cloud, and client software. It is operated by Dropbox, Inc., headquartered in San Francisco, California.

> communicate and engage freely and openly but in the knowledge that one cannot ever assume that communication is not being monitored. The only exception to this is when I have been involved in responding to serious repression, particularly when it has involved death threats, and there are discussions with activists about arranging safe houses, getting people out of Durban for a bit etc. Then I don't use email, cellphones etc. We use face to face communication (with no live phones present), payphones etc. We also would not use our own cars to travel to safe house. However discussions with academic colleagues are always open.

This suggests that academics like journalists increasingly prefer analogue means of communication such as face-to-face meetings and focus group discussions. The use of face-to-face meetings indicates that academics are deploying 'avoidance moves' in Marx's (2003) terminology. Avoidance moves are passive rather than active and involve withdrawal. There is no effort to directly engage or tamper with the surveillance. Rather, there is a temporal, geographical or methodological displacement to times, places and means in which the identified surveillance is presumed to be absent or irrelevant (Marx, 2003). This means that the absence of overt resistance against communications surveillance in South Africa should 'not be equated with an absence of resistance' (Willems, 2010: 1). Rather, a holistic approach to resistance must encapsulate 'everyday forms of resistance', such as use of coded words, fake house addresses, pseudonyms and pre-registered SIM cards to challenge state communications surveillance.

He also noted that he also sometimes backed up his data due to the theft of computers and failures of hard drive. The respondent also indicated he has not avoided any communication platforms because of surveillance. He observed that:

> No. Not in the academic context. In the activist context I wouldn't use the internet or cellphones to engage in practice discussions relating to repression.

Academics interviewed also revealed that mobile phones and online communication were most likely to put them at risk of state communication surveillance. One of the respondents noted that:

> As I said I don't take any measures or academic communication but avoid cellphones, frequently used landlines and email or other internet communication when dealing with practical matters relating to serious repression.

On the issue of the availability of social networks which assist academics to deal with surveillance, most of the interviewees said it was non-existent. They pointed out that they relied on their friends and contacts within various strategic institutions for tip-offs and protection. Those interviewed at the University of Johannesburg indicated that they relied on their university administration for support and advice on IT security matters. One respondent from Grahamstown observed that:

> What is required, ultimately, is political pressure against state repression. This is the most important thing. It needs to be rooted in mass based struggle under the direction

> of oppressed people. I don't find the NGO networks to be helpful. For instance an NGO in Durban [name withheld] is experienced as seriously patronising by many black grassroots activists. They say that they feel that they are not included in decision making but are just expected to be bussed in to make up the numbers at protests. There is a clear elitism in how things work, and it is also plainly raced…. If censorship by a black state is bad but censorship by a white … academic is not a problem then we are dealing with a fairly gross and evidently racialised hypocrisy.

As intimated from the foregoing interview extract, NGO networks do not seem to be helpful for academics compared to journalists, human rights lawyers and civic activists. The absence of academic-oriented social networks dealing with communication surveillance issues is also complicating issues. As respondents from Johannesburg noted, the lack of collective action amongst academics has led to personalised action frames against communication surveillance. They pointed out that:

> In our case we received a lot support from our university administration. Other academics told us that they have experienced similar state harassment but have done nothing about it. The problem is that people don't protest after being surveilled. They complain behind closed doors and also put in place individual coping mechanisms to deal with surveillance. There is need for a broad-based coalition which puts anti-surveillance politics at the centre of national discourse.

Overall, it can be deduced from these narratives that academics are concerned about the shrinking of academic freedom in South African universities. Although all the respondents pointed out that they have not abandoned their research projects after encountering surveillance practices during their professional work, they indicated that their research participants are reluctant to take part in some projects. This was pointed out by researchers from the University of Johannesburg who revealed that their participants preferred focus group discussions when compared to face-to-face individual interviews. Interview extracts above also demonstrate that unlike journalists who rely on formalised social networks to build counter-surveillance capacities, academics are too individualised to mount any collective resistance efforts and to seek redress. This explains why individualised action frames dominate accounts of surveillance practices amongst academics when compared to collective action frames which accompany civic activists and journalists' fight against surveillance.

(c) Civic activists

A total of 14 civic activists were interviewed during the 'Resisting Surveillance Workshops' (19 to 20 October 2015) hosted by the Right2Know Campaign in Johannesburg. Most of the interviewees came from Durban, Johannesburg, Cape Town and Rustenburg Most of these people were engaged

in struggles such as social justice, freedom of expression, housing and service delivery and lobbying against neo-liberal policies in general. Civic activists interviewed for this study noted that communications surveillance has complicated their mobilisation efforts and affected their right to organise. They complained that fear of being harassed by officials from the SSA has slowed down their coordination of demonstrations and marches. Activists highlighted that surveillance was meant to instil fear and make it difficult for them to organise and demonstrate against societal injustices. Most of the interviewees pointed out that they had or heard of someone who had experienced physical surveillance. Communication surveillance was generally something new to them although they pointed out that they had already started to secure their online communications. It is therefore not clear how widespread electronic surveillance is amongst civic activists in South Africa.

On the question why civic activists were targeted for surveillance purposes by the state, some of the interviewees pointed out that it is because of the work they are doing to conscientise the populace to stand up for their rights. They noted that the government felt threatened by the work of social movements which demanded better service delivery, respect for human rights and good governance practices. According to the respondents, the government was now resorting to brutal means of quelling service delivery protests because they feared that people would end up rising against the ANC. Three of the interviewees noted that activists were vulnerable to surveillance because of the nature of their work:

> It is because of what we do. The government is interested in knowing who funds us, who do we talk to and how do we mobilise people to fight for our rights. Because they want to know all this information, they end up resorting to communication surveillance so that they know our plans before we execute them. It's about intelligence gathering on their part (activist from Durban).

> I think it's because the government is afraid that people can end up rising against them. So activists are an easy target because most of the protests here are coordinated by us. They want to know our friends, our thoughts and our plans (activists from Johannesburg).

> They want to get into our heads. They think we are planning evil against them so they surveil our phones, social networks and emails. They are always building a case against us. Instead of seeing us as concerned citizens who want the best for our people, they think negatively about us. I think that's why we are on the firing line (activist from Cape Town).

As York (2014) points out, the way that activists interact on the internet is undoubtedly changing as a result of their knowledge of mass surveillance. For instance, the Pew Research Centre survey (2013) found that 86% of internet users have taken steps to 'remove or mask their digital footprints'. These included steps like clearing cookies and encrypting email communication. Some

of the users indicated that fear and withdrawal has begun to set in, thereby changing their online communication habits. Most of the interviewees interviewed during the *Resisting Surveillance Workshops* in Johannesburg noted that surveillance of personal data and electronic communications have changed their communication practices in a number of ways. They indicated that instead of over-relying on electronic communication, they have reverted to the use of code language, face-to-face meetings, pseudonyms on social media accounts and the cloud computing tools to store confidential information. While this may prevent physical theft of data from electronic gadgets such as laptops and smartphones, it suggests a level of naivety about how cloud services operate. In his study of Syrian activists, Bitar (2014) found that they have become masters in the art of concealment. They skilfully separated their online identities from their actual selves, using techniques such as pseudonyms and fake friend lists on social media platforms like Facebook and Twitter.

In South Africa, some of the interviewees pointed out that they encrypted valuable information and stored it securely in a bid to circumvent surveillance practices. However, respondents observed that besides providing digital security, encryption had its own drawbacks. They indicated that encryption can raise red flags with security agencies and it also involves a long and cumbersome process, especially for those who are not tech savvy. Because mobile phones can be turned into listening devices through surveillant technologies, some of the respondents observed that they insisted on turning off their cellphones during private and public meetings.

Analogue: Going back to the basics?

During the *Resisting Surveillance Workshops* held in Johannesburg, civic activists from the Johannesburg, Cape Town and Durban indicated that it was high time they reverted back to the basics of human communication and organisation. Besides investing huge amounts of financial resources in acquiring sousveillant technologies such as anti-virus/anti-malware programmes, encryption, sophisticated passwords and non-proprietary software, respondents revealed that they are now talking/meeting face-to-face in a secure environment about sensitive matters and information as opposed to using cellphones, landlines, emails, Skype or other electronic means. They are ensuring that in meetings/engagements where sensitive matters are being discussed all cellphones are not only turned off, but batteries are taken out. Some of these measures are consistent with Julian Assange's advice to journalists that they should use 'snail mail[21]' in order to

[21] http://www.iol.co.za/news/world/assange-urges-journos-to-use-snail-mail...

circumvent electronic surveillance by the state. Assange notes that 'My recommendation, for people who don't have 10 years' experience in cryptography, is to return to old methods (and) use the traditional postal service'. He also urges journalists to learn to use counter-espionage methods to protect their sources. For instance, one interviewee from Cape Town indicated that she felt safer using a Blackberry phone:

> I use a blackberry phones which has encrypted technology unlike other mobile phones. I however share my phone with my children when they want to use the internet and play games.

Activists from Johannesburg and Cape Town revealed that rather than archiving all meta-data on phones calls and social media messages and chats, they have developed a habit of deleting all their browsing history regularly. Deleting meta-data enables the user to protect his/her contacts as well as contents of the message. This demonstrates that some activists are devising individualised tactics and strategies aimed at beating the surveillance system. One of the respondents from R2K Durban pointed out that they had developed their own code language in the informal settlement to hide information from the people manning the surveillance tower. He said:

> We have come up with our own language with is understood by people within a closed knit group. Such that when we use that code people in the know will act because they know we have communicated something.

Another female activist from Johannesburg added that they used coded language within their WhatsApp and Blackberry group chats. She had this to say:

> We have invented our own words which we use on our WhatsApp and Blackberry group chats so that when we use those words we are communicating among ourselves. This is because in some of our community group chats we have members of the ANC who can tell their leaders about our plans ahead of time.

This suggests that activists are using 'distorting moves' (Marx, 2003) in an attempt to foil the optics of surveillance by manipulating the data received by the system; namely, use of coded words. Writing about tactics and strategies used by Syrian citizens to beat surveillance procedures, Bitar (2014) argues that they have developed 'code language'. They use agreed upon substitutes for suspicious words and sentences in daily communication.

Most of the tech savvy activists from Johannesburg and Cape Town observed that they have started pre-screening friends on social media platforms as a way of minimising exposing their communication data to intelligence informers. They also noted that they avoided opening attachments sent by people they don't know in the real world. However, some of the respondents indicated that even friends can be used to send viruses and Trojans by intelligence officers.

Respondents also indicated they have adopted TextSecure – a secure messaging app which allows for the transmission of encrypted messages. Others revealed they use RedPhone which is an app which allows one to make encrypted voices calls. ObscuraCam is also used by technologically literate activists to encrypt images and videos. ObscuraCam is an application for Android devices which was created by the Guardian project in order to obscure the faces of people in photos and videos taken by smartphones. In order to resist communication surveillance, respondents also pointed out that they regularly change their phone and laptop passwords, disable Bluetooth on their electronic devices and set up SIM lock on their mobile phones. In terms of secure browsing of the internet, some of the interviewees indicated that they used anonymising technologies like TOR[22], which assigns an IP address to your internet session that hides your actual location.

During protests and demonstrations, some of the interviewees from Johannesburg revealed that they took photographs and videos of police officers who would be escorting them. This constitutes another 'counter-surveillance move' (Marx, 2003). A counter-surveillance move implies the use of surveillance to combat surveillance, such as turning personal cameras on the agents of the state. This is popular amongst activists in Johannesburg who use personal cellphone cameras to record police details during protests. As Coatman (2009) observes, sousveillance is becoming increasingly coordinated in response to the surveillance of demonstrations. Research in the UK has shown that Fit Watch activists have developed in response to police forward intelligence teams (Fits), which monitor activists at demonstrations and meetings. These activists film the police and upload the evidence to the web and they attempt to block the police cameras with banners and placards (*The Guardian*, 22 June 2009). For Mann (2002), such tactics constitute a form of 'sousveillance' whereby 'cameras are mounted on people in low places, rather than upon buildings and establishments in high places'. This encapsulates sousveillant individuals using tools (such as camera-phones) to observe organisational observers, enhancing people's ability to access and collect data about their surveillance in order to neutralise it and acting as a consciousness-raising force to the surveillance society. Hierarchical sousveillance involves recording surveillance systems, proponents of surveillance and authority figures to uncover the panopticon and 'increase the equality' between surveillee and surveiller (Mann et al., 2003: 333). Mann (2004) also discusses personal sousveillance which denotes the recording of an activity by a person who is party to that activity, from first-person perspectives, without necessarily involving political agendas. With the mass take-up of social media globally, personal sousveillance is rife, involving people curating and

[22] TOR is free software and an open network that helps users defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships and state security.

creating content, thereby revealing their lives, thoughts and feelings (Pew Internet Research Centre, 2014).

It was clear from the interviews that activists who are dealing with service delivery issues and freedom of expression issues are more vulnerable to communication surveillance. This is because most of these people mobilise informal settlement dwellers who are viewed as potential voters by the ruling party. Although respondents pointed out that they will not stop mobilising against poor service delivery, some of them indicated that communication surveillance had the unfortunate ripple effect of engendering a culture of fear and therefore had a demobilising effect. Compared to academics and lawyers, responses show that civic activists and journalists are more vulnerable to communication surveillance because of the nature of their work. Like journalists, civic activists are seen as change agents who can mobilise large masses of people who can topple the ruling elite. Whilst civic activists acknowledged putting in place a raft of counter-measures against surveillance, like journalists, most of their everyday forms of resistance are individualistic and episodic rather than full-blown and sustained.

(d) Lawyers

As intimated earlier, human rights lawyers have not escaped the ever-expanding tentacles of communications surveillance in South Africa and beyond. Some lawyers in the US have had confidential information related to ongoing legal matters and privileged communications between them and their clients surveilled (Human Rights Watch, 2014). In February 2014, the Snowden revelations indicated that the communications of US-based law firm Mayer Brown with its client, the government of Indonesia, came under surveillance by an Australian intelligence agency, which in turn provided resulting intelligence to the United States. Most of the attorneys noted that surveillance undermined their ability to advocate on behalf of their client (Human Rights Watch, 2014). In South Africa, the Legal Resources Centre (LRC) has had their communications intercepted by the British GCHQ. The LRC is South Africa's largest public interest, human rights law clinic which was started in Johannesburg in 1979. They use the law as an instrument of justice for the vulnerable and marginalised, including poor, homeless and landless people and communities who suffer discrimination by reason of race, class, gender, disability or by reason of social, economic and historical circumstances. It has four regional offices (in Johannesburg, Grahamstown, Durban and Cape Town) and employs over 65 lawyers in South Africa. Two interviewees, human rights lawyers based in Johannesburg and Cape Town, pointed out that they have changed the way they store or share confidential information related to their clients. This is because lawyers rely on

the ability to exchange information freely with their clients in order to build trust and develop legal strategies, which is especially important in the realm of criminal defence (Human Rights Watch, 2014). The ubiquitous nature of communication surveillance creates uncertainty as to whether lawyers can ever provide true confidentiality while communicating electronically with clients (Human Rights Watch, 2014).

Lawyers from Cape Town and Johannesburg interviewed for this study acknowledged that communications surveillance has forced them to become cautious and responsible with client information. They indicated that surveillance has also complicated their communication practices with clients and partners. Instead of relying on email communication to disseminate confidential information, some of the interviewees revealed that they prefer face-to-face communication which does not leave behind data traces. With regard to why their organisation had been surveilled by GCHQ, one of the lawyers interviewed in Johannesburg revealed that: 'I honestly don't know why we were targeted. We are in the dark as to how and why this happened. We are currently investigating why this actually happened'. She added that: 'We are now cautious going forward because the mere fact that our communications were being intercepted by the GCHQ suggests that we cannot take things for granted anymore'. Respondents also said that even telephonic interviews can no longer be relied upon because of the fear of communications surveillance. This is because communications surveillance also has a chilling effect on whistleblowing which human rights lawyers rely on to build cases against powerful people in society. In fact, when whistleblowers believe that their online communications are susceptible to surveillance they tend to withhold certain vital information.

In an attempt to resist ubiquitous communications surveillance, respondents pointed out that they are using password protection, encryption technology and face-to face-communication. Citizens adopt resistance tactics to surveillance, inventing new ways of ensuring degrees of autonomy and satisfaction or at least tolerance in the face of expanding networks of control (Gilliom and Monahan, 2012: 409; Monahan, 2006). As with the journalists, lawyers increasingly feel under pressure to adopt strategies to avoid leaving a digital trail that could be monitored; some use burner phones, others seek out technologies they feel may be more secure and others reported travelling more for in-person meetings (Human Rights Watch, 2014). They also indicated that some people within the organisation were undertaking training courses in ICT security so that they can educate others on digital security and counter-surveillance. It was clear from the interviews that lawyers had limited knowledge when it comes to digital security and surveillance. Although interviewees from Johannesburg and Cape Town indicated that they are currently working on their digital security

infrastructure in order to protect themselves and their clients, responses suggested that it was something that had been delegated to a small group of people to deal with on behalf of the who organisation. Unlike in America where some lawyers expressed reluctance to take on certain cases that might incur surveillance, in South Africa, attorneys indicated that despite pervasive surveillance they were doing their work as before. In order to protect client's confidentiality, some of the respondents observed that they engage in non-electronic communications which do not store meta-data. This corroborates Marx's (2003) view that surveillees adopt 'piggy backing or switching moves' which involve beating certain types of surveillance using non-surveilled or approved item or individual to mask the presence of or change places with a subject of interest.

In terms of the various kinds of support networks that human rights lawyers use to fight against communications surveillance, interviewees noted that they are affiliated with the R2K Campaign which has been working in the area for the last couple of years. 'We support the R2K Campaign because it brings together various organisations and activists who share similar difficulties in relation to communication surveillance'. They bemoaned the fact that there is lack of coordination amongst civil society organisations in South Africa when it comes to fighting against communications surveillance. Some of the respondents pointed out that because of the absence of coordinated efforts, it was impossible for them to politicise and build coalitions that picket against the proliferation of surveillance in South Africa. The Snowden revelations within the United States gave rise to an ideologically diverse, trans-partisan coalition pushing for meaningful reform of the surveillance state (Greenwald, 2014: 248). These changes stem from the public sphere and occurred through public discussion. Another respondent from Johannesburg pointed out that they because they are a member of the International Network of Civil Liberties Organisations[23] (INCLO), they are able to institute strategic litigation cases against the GCHQ at the European Human Rights Court. They are also lobbying for the respect of the right to privacy at international level. As she explained: 'Because as a member of INCLO organisations we have benefited immensely from advice we have received from the American Civil Liberties Union and Liberty which has experience handling cases involving communications surveillance'. Greenwald's (2014) research on communications surveillance in the wake of Snowden revelations highlights the importance of both private (everyday forms of resistance) and public sphere resistance. He reminds us that 'it is human beings collectively, not a small number of elites working in secret, who can decide what kind of world we want to live in' (Greenwald, 2014: 253).

[23] It comprises of nine domestic civil liberties and human rights organisations: the American Civil Liberties Union, the Association for Civil Rights in Israel, the Canadian Civil Liberties Association, Centro de Estudios Legales y Sociales, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Kenyan Human Rights Commission, the Legal Resources Centre, and Liberty.

Unlike journalists and academics, interviews with human rights lawyers indicated that they were not well-versed in digital security matters and were prepared to partner with the R2K Campaign and Privacy International who have a wealth of knowledge on communication surveillance. The respondents pointed out that they have started to take their digital security matters seriously following news reports that the British intelligence agency had spied on them. This is contrary to other vulnerable constituencies like journalists who have been with censorship and surveillance for a long time. More capacity building in terms of digital security workshops have to be conducted with human rights lawyers and academics who are still naïve about communication surveillance practices.

Concluding remarks and the way forward

In view of the interview responses from academics, journalists, lawyers and civic activists from South Africa, it is clear that communications surveillance has led to changing practices and routines. Most of the responses show that electronic forms of communication are increasingly being supplanted by face-to-face communication. In view of the pervasive surveillance, respondents from South Africa have adopted a wide range of moves to neutralise surveillance practices. These include blocking, masking, switching, avoidance, refusal, distorting, cooperative and counter-surveillance moves. This report has demonstrated that most of the tactics and strategies fall within the context of everyday forms of resistance. This means that public forms of resistance such as breaking moves are still being avoided by most respondents interviewed for this report. In order to arrive at an 'equiveillance' – their solution for rebalancing the surveillance society – Mann and Ferenbok (2013) argue for increased sousveillance. They also propose that other modes of resistance to surveillance include 'counterveillance[24]' and 'univeillance[25]'(Mann, 2013). These solutions resist surveillance while encouraging people to continue with their normal communicative activities, including sousveillance. Mann and Ferenbok (2013: 26) posit that if sousveillance becomes ubiquitous, and if coupled with political action to enact change from below, then we may reach a state of 'equiveillance' where surveillance and sousveillance balance out. They suggest that equiveillance would be achieved when veillance infrastructures are extensive and the power requirements to enact change from below are marginal. This type of system would likely protect

[24] 'Counterveillance' comprises measures taken to block both surveillance and sousveillance (Mann, 2013: 7).

[25] 'Univeillance' is where surveillance is blocked but sousveillance enabled (Mann, 2013: 7). This can include technological solutions such as anonymisation and end-to-end encryption (which provides security at either end of the communication, so that only the recipient, not the company running the communications service, can decrypt the message).

whistleblowers, encourage public fora and debate, and implement participatory projects and innovations to the system.

In his study of the Snowden revelations and the U.S. surveillance practices, Greenwald (2014: 12) argues that public deliberation is an effective way to resist surveillance and curb surveillance abuses. He views public deliberation as a momentary pause in which we examine political paths, both taken and untaken. Greenwald also argues that power without deliberation is 'the ultimate imbalance, permitting the most dangerous of all human conditions: the exercise of limitless power with no transparency or accountability' (2014: 169). Greenwald encourages 'critique' as espoused by Foucault (1977) through public deliberation about the limits of the surveillance state. Critique is one of the everyday forms of resistance proposed by Foucault. He views critique as 'the art of not being governed quite so much' (Foucault, 1977: 45). Critique gives the subject the right to question the truth and the relationship between truth and power (Foucault, 1997). People may engage in critique to negotiate the way they are being governed if they find the rules of governance to be contrary to natural rights. Journalists, activists, academics and lawyers can undertake critique by subverting power in small ways which slightly alter relationships of power. In his book, *Defences of the Weak*, Thomas Mathiesen (1965: 26) demonstrates how inmates in a Norwegian prison used everyday forms of resistance to contest the surveillance regime through the principle of 'censoriousness' which referred to how they criticised 'the ruler for his lack of adherence to his own norms'. According to Mathiesen, one prisoner, known amongst his fellow inmates as the 'amateur lawyer', managed to steal 'a set of regulations for guards, memorised the rules, and . . . used his knowledge intelligently and efficiently, criticising staff members for not adhering to the rules' (1965: 13). Graham and Wood point to the everyday practices of the targeted' as an example of the many forms of resistance against surveillance: 'In British towns young black men have been shown to develop elaborate practices to exploit CCTV system 'blindspots' (2003: 244). Leonard describes 'the exercise of individual resistance, embedded in micro-processes of everyday interaction with the welfare system' as 'necessary but insufficient' (1997: 170). More organised collective forms of resistance are therefore necessary in order to achieve change.

However, the problem is that is usually difficult to move beyond everyday forms of resistance to covert resistance that actually stops surveillance practices in their tracks. Thus, how to build collective social formations which are concerned with implementing 'breaking moves' (to use Marx's (2003) diction) against surveillance techniques is an under-theorised area in surveillance studies. There are very few examples of organised collective resistance directed against surveillance. For instance, Lyon (2007: 374) provides a number of examples of resistance to the

increase in surveillance since 9/11 from around the world. In particular, he singles Japan, where the Japanese Network Against Surveillance Technology was formed and where major protests and uncharacteristic civil disobedience followed the introduction of the national computerised registry of citizens in 2002'. Lyon observes how dissenters are themselves able to use 'the same kinds of technology that enable networked surveillance' to communicate with each other (2007: 374). Leonard (1997: 169-70) also highlights different forms of collective resistance 'manifested in some of the new social movements organised primarily on the basis of social identity and having the potential to be active at every level of the social structure'.

This report also recommends that the South African government must undertake legal reforms in order to curb abuses from the State Security Agency, the Office of Interception Centres and National Communications Centre. Laws which require urgent reform include RICA, the Cyber-security and cyber-crimes Bill and the Intelligence Services Oversight Act. These laws give the government disproportionate powers when it comes to communications surveillance and infringes on individuals' right to privacy as enshrined in the 1996 Constitution. Any reform of these laws must ensure that they are aligned with the International Principles on the Application of Human Rights to Communications Surveillance (also known as the Necessary and Proportionate Principles). The Principles underscore that mass surveillance in all its manifestations is unnecessary, disproportionate and fundamentally lacking in transparency and oversight. For instance, in terms of the RICA a user notification clause should be inserted which notifies an individual of a decision authorising communications surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation. RICA should also establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Furthermore, a clause within the RICA which compels service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for state communications surveillance purposes, should be struck off.

At an individual level, activists, journalists, academics and lawyers must use circumvention and anonymisation tools as well, as other counter-surveillance technologies. Besides these blocking, masking, switching, avoidance, refusal, distorting, cooperative and counter-surveillance moves (Marx, 2003), there is need for these vulnerable constituencies to build an anti-surveillance social movement which focus on 'breaking' these surveillance practices. As it stands, the R2K Campaign has the capacity to lead an anti-surveillance campaign because of their technical expertise and

baseline study on the issue (the 'Big Brother Exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements' handbook). The handbook documents the stories of activists and community leaders who have been monitored and harassed by South Africa's intelligence agencies – especially the State Security Agency and the Crime Intelligence Division of the police. More qualitative research is required to capture the narratives of a number of constituencies which were not interviewed in this report such as trade unionists, student activists from the #Rhodesmustfall Campaign, #Feesmustfall Campaign and #OpenStellenbosch as well as organisers of service delivery protests across the country. These groups can shed light on how they are resisting communication surveillance in their contexts.

.

References

Albrechtslund, A. 2008. Online Social Networking as Participatory Surveillance. *First Monday* 13(3).

Alexander, P. (2012, April 13). A massive rebellion of the poor. Mail and Guardian. mg.co.za/article/2012-04-13-a-massive-rebellion-of-the-poor.

Andrejevic, M. 2012. Ubiquitous surveillance. In Ball, K. Haggerty, K. and Lyon, D. (Eds.), *Routledge Handbook of Surveillance Studies*. New York: Routledge.

Babbie, E. and Mouton, J. 2001. The Practice of Social Research. Oxford: Oxford University Press.

Bakir, V, 2015. 'Veillant Panoptic Assemblage': Mutual Watching and Resistance to Mass Surveillance after Snowden. *Media and Communication,* 3(3): 12-25.

Ball, K. 2005. Organisation, surveillance and the body: Towards a politics of resistance. Organization, 12, 1, 89-108.

Bauman, Z. 2000. *Liquid Modernity*. Cambridge, Polity Press.

Bentham, J. 1791. *Panopticon*. Dublin: T. Payne.

Bitar, K. 2014. Syria- Communications surveillance in the digital age: Circumventing surveillance of internet communications 'Global Information Society Watch 2014: Communications surveillance in the digital age' which can be downloaded from http://www.giswatch.org/2014-communications-surveillance-digital-age. [Accessed on 5 October 2015].

Bogard, W. 1996. *The Simulation of Surveillance: Hypercontrol in Telematic Societies*, Cambridge: Cambridge University Press.

Braman, S. 2006. *Change of State: Information, Policy, and Power*. Massachusetts: MIT Press.

Bogard, W. 2006. Surveillance assemblages and lines of flight. In Lyon, D. (Ed.), *Theorising surveillance: The panopticon and beyond.* Uffculme, Devon: Willan Publishing.

Boyne, R. 2000. 'Post-Panopticism.' *Economy and Society* 29(2): 285-307.

Bryman, A. 1984. The Debate about Qualitative and Quantitative Research: A Question of Method or Epistemology? *The British Journal of Sociology*. 35(1): 75-92.

Bryman, A.1988.*Quantity and Quality in Social Research*. London: Routledge.

Caluya, G. 2010. The post-panoptic society? Reassessing Foucault in surveillance studies, *Social Identities*, 16(5): 621-633.

Cary N. and Watt, S. 1999. Academic Keywords: A Devil's Dictionary for Higher Education, London: Routledge.

Davenport, C. 2006. 'Killing the Afro: State Repression, Social Movement Decline and the Death of Black Power' draft presented at the Workshop on Contentious Politics, Columbia University.

Davenport, C. 2005. 'Understanding Covert Repressive Action' Christian Davenport *Journal of Conflict Resolution* 49:1, Feb 2005. 120-140.

Della Porta, D. 1995. Social Movements, Political Violence, and the State: A the impact of surveillance on the exercise of assembly rights. Comparative Analysis of Italy and Germany. Cambridge: Cambridge University Press.

De Certeau, M. 2002. The Practice of Everyday Life. Berkeley: University of California Press.

Deleuze, G. 1992. Postscript on the societies of control. October, 59, 3-7.

Deleuze, G. and Guattari, F. 1983. *Anti-Oedipus: Capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.

Duncan, J. Finlay, A., Groome, A., Comninos, A. and Esterhuysen. A. 2014. Mapping the ICT policy environment in South Africa, Association for Progressive Communications (APC) May 2014. Retrieved from www.apc.org.zaAPC_PolicyMapping_SouthFrica_20140509. [Accessed on 20 November 2015]

Duncan, J. 2014. Monitoring and defending freedom of expression and privacy on the internet in South Africa. Retrieved from https://www.apc.org/en/system/files/SouthAfrica_GISW11_UP_web.pdf. [Accessed August 23, 2014].

Duncan, J. 2014. Communications surveillance in South Africa: the case of the Sunday Times newspaper. Global Information Society Watch: Communications surveillance in the digital age.

Donovan, P and Martin, A.K. 2014. The rise of African SIM registration: The emerging dynamics of regulatory change. *First Monday*, Volume 19, Number 2 - 3 February 2014. Retrieved from http://firstmonday.org/.... [Accessed 30 October 2015].

Fernandez, L.A. and Huey, L. 2009. Editorial. Is resistance futile? Thoughts on resisting surveillance. *Surveillance & Society*, 6(3), 198-202.

Foucault, M. 1977. *Discipline and punish: The birth of the prison*. New York: Vintage.

Fuchs, C. 2011. New Media, Web 2.0 and Surveillance. *Sociology Compass* 5/2 (2011): 134–147.

Geertz, C. 1973. *Thick Description: Toward an Interpretive Theory of Culture. The Interpretation of Cultures: Selected Essays*. New York: Basic Books.

Gerstmann, E. and Streb, M.J. 2006. Academic Freedom at the Dawn of a New Century: How Terrorism, Governments. California: Stanford University Press.

Giddens, A. 1981. *A Contemporary Critique of Historical Materialism. Vol. 1: Power, Property and the State*. London: Macmillan.

Giddens, A. 1985. *A Contemporary Critique of Historical Materialism. Vol. 2: The Nation-State and Violence*. Cambridge: Polity Press.

Gillham, B. 2000. *The Research Interview*. London: Continuum.

Gilliom, J. 2005. 'Resisting Surveillance' *Social Text* 83, 23 (2): 71-83.

Gilliom, J. 2001. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. University of Chicago Press: Chicago.

Gilliom, J. 2006. Struggling with surveillance: Resistance, consciousness, and identity. In K.D. Haggerty & R.V. Ericson, (eds.), *The new politics of surveillance and visibility*. Toronto: University of Toronto Press.

Gilliom, J. and Monahan, T. 2012. Everyday resistance. In Ball, K., Haggerty, K., and Lyon, D. (eds.) *Routledge Handbook of Surveillance Studies*. Routledge: Abingdon, UK, 405–412.

Graham, S. and Wood, D. 2003. Digitizing surveillance: categorization, space, inequality. Critical Social Policy 23(2): 227-248.

Greenwald, G. 2014. *No place to hide: Edward Snowden, the NSA and the US surveillance state*. New York: Metropolitan Books.

Grinyer, A. 2002. 'The anonymity of research participants: assumptions, ethics and practicalities'. Social Research Update. 36. University of Surry. Retrieved from www.soc.surrey.ac.uk/sru/SRU36.htm. [Accessed 30 November 2015].

Guillemin, M. and Gillam, L. 2014. Ethics, reflexivity, and 'ethically important moments' in research. Qualitative Inquiry. 10:261-280.

Haggerty, K.D. and Ericson, R.V. 2000. The surveillant assemblage. British Journal of Sociology, 51(4), 605-622.

Haggerty, K. 2006. Tear down the walls: On demolishing the panopticon. In D. Lyon, D. (Ed.), *Theorising surveillance: The panopticon and beyond*. Uffculme, Devon: Willan Publishing.

Hintz, A. 6 October 2015; The Next Snowden Casualty: U.S. no 'Safe Harbour' for EU data).

Hintz, A. 2014. Outsourcing Surveillance—Privatising Policy: Communications Regulation by Commercial Intermediaries. *Birkbeck Law Review* Volume 2(2): 349-368.

Hollander, J. and Einwohner, R. 2004. Conceptualising Resistance. *Sociological Forum* 19 (4):533-554.

Human Rights Watch. 2014. *With Liberty to Monitor all: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy*. Washington DC: Human Rights Watch.

Kaiser, K. 2009. Protecting Respondent Confidentiality in Qualitative Research. Retrieved from www.ncbi.nlm.nih.gov. [Accessed on 22 February 2016].

Kvale, S. 1996. *Interviews: an introduction to qualitative research interviewing*. Thousand Oaks: Sage.

Lyon, D. 2003. Surveillance Technology and Surveillance Society. In Misa, T.J, Brey, P. and Feenberg, A. (eds). *Modernity and technology*. London: MIT Press.

Lyon, D. 2001. *Surveillance Society: Monitoring Everyday Life.* Open University Press: Buckingham, UK.

Lyon, D. 2003. *Surveillance after September 11*. Cambridge: Polity.

Lyon, D. 2014. Surveillance, Snowden, and big data: capacities, consequences, critique. *Big Data & Society*, July–December, 1-13.

Lyon, D. 2015. The Snowden stakes: challenges for understanding surveillance today. *Surveillance & Society*, 13(2), 139-152.

Introna, L. D. and Wood, D. 2004. Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society* 2 (2/3):177-198.

Mann, S., Nolan, J. and Wellman, B. 2003. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance and Society*, 1(3), 331-355.

Mann, S. 2013. Veillance and reciprocal transparency: Surveillance versus sousveillance, AR Glass, Lifeglogging, and wearable computing. Retrieved from http://wearcam.org/veillance/veillance.pdf. [Accessed 9 December 2015].

Mann, S. and Ferenbok, J. 2013. New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society*, 11(1/2): 18-34.

Martin, A.K., Van Brakel, R. and Bernhard, D. 2009. Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society* 6(3): 213-232.

Marx, G.T. 2002. 'What's new About the "new Surveillance"? Classifying for Change and Continuity.' *Surveillance & Society* 1(1): 9–29.

Marx, G.T. 2003. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues* 59(2): 369-390.

Mathiesen, T. 1997. The viewer society: Michel Foucault's 'Panopticon' revisited. *Theoretical Criminology* 1(2): 215-233.

McCahill, M. and Finn, R.L. 2014. *Surveillance, Capital and Resistance: Theorising the Surveillance Subject*. London: Routledge.

Monahan, T. 2006. Counter-surveillance as Political Intervention? *Social Semiotics* 16(4): 515-534.

Mail & Guardian, Spy wars: South Africa is not innocent, 21 June 2013, http://mg.co.za/article/2013-06-21-00-spy-wars-south-africa-is-not-innocent and also, Secret state: How the government spies on you, available at: http://mg.co.za/article/2011-10-14-secret-state/. [Accessed 8 August 2015].

Mail & Guardian, 2013. Millions were handed to an SA company that supplied mass surveillance technology to Libya. Retrieved from http://mg.co.za/article/2013-11-22-dti-funded-gaddafi-spyware. [Accessed on 11 August 2015].

Parry, O. and Mauthner, N. 2004. 'Whose data are they anyway? Practical, legal and ethical issues in archiving qualitative research data' *Sociology*. 38(1): 139-152.

Poster, M. 1990. *The Mode of Information*. Cambridge: Polity.

Orwell, G. 1949. *Nineteen Eighty-Four*, New York: Penguin.

Right to Know Campaign, 2014. Big Brother Exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements. Activist Handbook. Retrieved from www.bigbrother.r2k.org.za. [Accessed on 15 June 2015].

Scott, J.C. 1990. *Domination and the Arts of Resistance: Hidden Transcripts*, Yale University Press: New Haven.

Scott, James C. 1985. *Weapons of the Weak*. Yale University Press.

Sieber J. 1992. Planning ethically responsible research: A guide for students and internal review boards. Newbury Park: Sage.

Simon, B. 2005. The Return of Panopticism: Supervision, Subjection and the New Surveillance. *Surveillance & Society* 3(1): 1-20.

Singleton Jr., R. and Straits, B. 1999. *Approaches to Social Research 3rd edition*. New York. Oxford University Press.

Swart, H. 2011. 'Secret State: How the Government Spies on You', Mail and Guardian, 14 October 2011, mg.co.za/article/2011-10-14-secret-state.

Swart, H. 2015. Big Brother is listening on your phone. Mail and Guardian, November 13-19. 9-11.

Swart, H. 2015. How cops and crooks can 'grab' your cellphone and you, 8 Mail & Guardian November 27 to December 3 2015, 8-9.

Tolich, M. 2004. Internal confidentiality: When confidentiality assurances fail relational informants. *Qualitative Sociology*. 27:101–106.

Ullrich, P. and Wollinger, G.R. 2011. A surveillance studies perspective on protest policing: the case of video surveillance of demonstrations in Germany. *Interface*, 3(1), 12–38.

Willems, W. 2010. Beyond dramatic revolutions and grand rebellions: everyday forms of resistance during the 'Zimbabwe crisis'. *Comminicare*, 29: 1-17.

Wilson, D & Serisier, T. 2010. Video Activism and the Ambiguities of Counter-Surveillance. *Surveillance & Society* 8(2): 166-180.

Weiss, R. 1994. Learning from strangers: The art and method of qualitative interview studies. New York: The Free Press.

Wood, D. 2007. Beyond the panopticon?. In Jeremy W. Crampton and Stuart Elden (eds.) *Space, Knowledge and Power: Foucault and Geography*. Hampshire: Ashgate Publishing: 245-264.

York, J. 2014. Communications surveillance in the digital age: The harms of surveillance to privacy, expression and association, Global Information Society Watch 2014.