CHAPTER ONE

Making the case for public oversight of intelligence-driven surveillance: Key issues and core concepts

Jane Duncan and Allen Munoriyarwa

Introduction

Technological developments, government obsessions with secrets and legal vacuums across different countries have conspired to give the intelligence communities unprecedented insights into people's private lives and power over their private conduct (Granick, 2017). Digital surveillance has been used to hinder or monitor groups and individuals that seek to change the political, economic and social conditions of their communities. For example, in 2022, Botswana's intelligence agencies attempted a major power grab. They sought wide-ranging powers through a draft law that would allow them to intercept communications on a warrantless basis, including the communications of journalists. These powers would have weakened basic democratic controls over surveillance for intelligence purposes, especially judicial controls over surveillance through prior authorisation. However, their power grab was thwarted by the public (Ndlovu, 2022). The media, civil society and trade unions objected to the draft law, the Criminal Procedure and Evidence (Controlled Investigations) Bill, but dubbed the 'Spy Bill' by its critics. The ensuing controversy was so huge and impactful that it forced the government to walk back draconian provisions in the Bill, although the law that was passed eventually was far from perfect (Balule and Dambe, 2023, pp. 1–14).

Botswana provides a very recent example of a poorly understood but, at times, highly effective form of oversight of intelligence-driven surveillance, namely public oversight. Similar surveillance scandals have erupted across Southern Africa, where publics have exposed and reacted to surveillance by intelligence agencies, when it has been used for improper and even unlawful purposes. In an earlier case in Angola, in 2015, and in what has become known as the 15+2 or Luanda reading-club case, 17 activists were charged with preparatory acts of rebellion, and plotting against the president and other state institutions. Their crime? Holding a reading group on non-violent resistance, which included a translated version of a Gene Sharp book, entitled *Tools to Destroy a Dictator*. Angolan intelligence officers used covert digital video surveillance to monitor the reading group, and the recordings were then used in the trial. Concerned citizens groups launched a major international solidarity campaign, leading to the Supreme Court granting their conditional release followed by an amnesty law that was applied to them (Verde, 2021, pp. 7–9). In South Africa, and over a decade starting in 2011, a major multi-class campaign led by civil society and social movements prevented two successive presidents from signing a Bill into law that would have drawn a shroud of secrecy over the police and intelligence agencies (the 'Secrecy Bill'), and an investigative journalism non-profit organization, the amaBhungane Centre for Investigative Journalism, successfully challenged the country's main law (under) regulating digital surveillance. In Mauritius, from 2013 onwards, a public push-back against the surveillance potential of a government smart identity card led to the government having to abandon its ambitions to establish a centralised biometric database of all personal citizen data (Duncan, 2022, pp. 121–2).

As the chapters in this book will show, these scandals have followed familiar patterns across time and space. Intelligence agencies are meant to use surveillance capabilities for pressing public purposes, such as protecting national security and solving serious crimes when they have exhausted other, less intrusive, investigative methods. However, the notoriously secretive work of intelligence creates the potential for abuse, especially in circumstances where intelligence agencies focusing on national security are poorly controlled and overseen, and digitisation has compounded these problems (Gill and Phythian, 2012, pp. 92–3; Munoriyarwa and Mare, 2023, pp. 6–8). Governing parties concerned about maintaining their grip on the levers of power may well be tempted to use (and as this book will show, have used) these capabilities to put perceived and actual critics under surveillance to provide them with the upper hand. Yet, time and again, the law and oversight practices have not kept up with intelligence agencies' technological capabilities to surveil. It is more likely that details about law-enforcement surveillance will come into the public domain, given its focus on collecting intelligence for prosecutorial purposes, and hence police surveillance practices are more likely to be scrutinised in court. National security intelligence, on the other hand, and the surveillance practices used to collect it, is often more wide-ranging and even speculative, as it is focused on broader, longer-term threats to a country (strategic intelligence) and measures to counter them (counter-intelligence). As it is generally not prosecutions-focused, this form of intelligence, and the surveillance used to collect it, may be even more open to abuse than police intelligence. However, increasingly, there is a blurring of the lines between law-enforcement intelligence and national-security intelligence, with secretive practices from the latter being transported into the former, which can heighten the potential for abuse of the former.

Consequently, when it occurs, surveillance overreach may come into the public domain only through public exposures, leading to surveillance controversies and even scandals and, in countries where organisational capacity exists to take these issues up, activism to rein these powers in. Some of these scandals have led to major democratic victories, where organised public responses have forced intelligence agencies to become more transparent in how they use these capabilities on a long-term basis. Other controversies have led to mixed outcomes and still others have failed to achieve any meaningful concessions. This book examines the lessons to be learnt from key moments when publics have attempted such oversight in eight Southern African countries (Angola, Botswana, Democratic Republic of the Congo, Namibia, Mauritius, Mozambique, South Africa and Zimbabwe). These countries were chosen because they span the spectrums of equality and democracy in Southern Africa, and the major linguistic divides in the region. They also have different, but still ever-present, colonial histories that continue to shape how their intelligence and security sectors operate, making them ripe for comparison.

This introductory chapter deals with the main objectives and key questions of the research project that informs this edited volume, the methodology used, some of the core concepts engaged in this book and how they are understood. It also introduces the chapters in the book. The chapter also sets the basis for the analyses that follow on the practices of the media and civil society organisations as a neglected but much needed dimension of oversight (Kniep et al., 2023, p. 7).

Objectives and key question

Governments justify digital surveillance as being necessary to fight crime and terrorism: social ills that could undermine attempts to ensure that citizens enjoy substantive freedoms and real opportunities. Consequently, digital surveillance is becoming increasingly popular in policing and intelligence work in Southern Africa, where data protection rules and intelligence oversight are generally weak. Such surveillance involves unique risks to privacy, in that it enables automated tracking of individuals across widening geographical distances on a continuous, real-time basis, which has tilted corporate and state modes of surveillance increasingly towards everyday life (Lyon, 2018, p. 12). Since the September 11, 2001 terrorist attacks on the United States (US), intelligence agencies and private sector companies have developed an elective affinity (Zuboff, 2019, p. 116). The agencies had a vested interest in collecting as much data as possible, ostensibly to prevent further intelligence failures on the scale of the one that allowed the September 11 attacks to happen, while private companies, such as Google, had a vested interest in preventing restrictions on their business models on privacy grounds. This convergence of interests led to unprecedented collaborations between intelligence agencies and Silicon Valley firms, and to conditions for what Shoshana refers to, with reference to Giorgio Agamben's states of exception, as surveillance exceptionalism (Zuboff, 2019, p. 116), or a situation where secret public–private intelligence collaborations are stitched together that greatly expand intelligence powers while making oversight even more difficult than it was.

The available evidence points to Southern African societies facing a major – and under-analysed – surveillance problem, where the technological capabilities of intelligence agencies have run far ahead of the capabilities of the judiciary, administrative and legislative bodies, to perform effective oversight, and where there is limited evidence of these capabilities being used for legitimate public purposes. The chapters will include contextual information where this state of exception following the September 11 attacks played out in Southern Africa, which, despite being somewhat removed from the immediate aftermath of 9/11, saw some governments seizing on the war on terror to expand surveillance powers, and enlisting the private sector or other governments to assist with their compliance with the requirements of bodies such as the Financial Action Task Force to combat terrorism financing. Other governments were galvanised mainly by domestic factors – such as rising protest action – to expand their capabilities by buying surveillance technologies from an increasingly globalised and privatised industry.

The background to this book is that one of the editors, Jane Duncan, was awarded a British Academy Global Professorship, lasting four years and starting in January 2023, and she set up a research project to explore public oversight practices in eight Southern African countries, using a comparative case-study methodology. The contents reflect on the findings of the first two years of the project. It assesses the adequacy of oversight in the eight countries, based on the conviction that the mere establishment of formal oversight institutions is unlikely to deliver substantive accountability, where intelligence contributes in meaningful ways to ensuring the kinds of radical justice and equality that have evaded these countries, despite liberation from colonialism and apartheid. This is not to say that there should not be aspirations to establish such institutions, particularly in semi-authoritarian countries, where their establishment could be a galvanising force in society. However, truly effective oversight and, ultimately, accountability will most likely have reach beyond these institutions and incorporate a mobilised public, as there is little sense in prescribing the same remedies to digital surveillance overreach that have been implemented elsewhere, but with unsatisfactory results. Therefore, this book takes these weaknesses into account and uses them to analyse moments when public oversight has been attempted as a supplement to, and even a replacement for, more conventional forms of oversight, and lessons to be learnt from them.

A challenge the authors faced was that intelligence is notoriously difficult to study, as primary sources of information, including interviews, may be limited by secrecy (van Puyvelde, 2018, pp. 375–91). These limitations apply especially to national security intelligence, where countries typically tend to tolerate executive discretion in using surveillance, coupled with higher levels of secrecy, when compared to other areas of government, and this problem is compounded in countries with serious democracy deficits. In view of these difficulties, researchers may be tempted, understandably, to focus on structural accounts of intelligence systems, including oversight, by using publicly available sources such as laws and policies. Assessments of their democratic or authoritarian content may be made depending on the presence or absence of legislative or policy checks and balances, summarised in international standards (Wegge and Wentzling, 2018, pp. 26–8). We, on the other hand, have chosen to adopt an agential approach to oversight: in other words, while documenting the dangers of surveillance overreach, we also proceed from the assumption that intelligence systems are not static and that, in certain conditions, publics can and do have causal power in shaping and reshaping these systems. We are interested in those forms of agency that increase the accountability of these most secretive areas of government and allow publics to exercise informed digital citizenship and challenge state and private surveillance power (Hintz et al., 2019, pp. 123–43; Choudry, 2018, pp. 3–22). We intended the research to be forward-looking, addressing the question of what kinds of agency are possible, even in the most difficult of contexts.

Crucially to the authors, the risks of intelligence abuses, and of digital technologies being used in ways that mainly benefit dominant elite interests, are tightly connected to public acceptance or rejection of levels of surveillance (Duncan, 2018, pp. 185–204; Hintz et al., 2019, pp. 117–21), which in turn impacts on whether sections of the public are open to being galvanised on this issue. As data-mining practices increase, publics risk becoming resigned to living without any reasonable expectation of privacy, and with no expectation of being able to associate and organise freely and without state intervention. Where there is little or no expectation of privacy, such societies risk being subjected to near-ubiquitous uses of dragnet digital surveillance, where huge quantities of data are collected and analysed, irrespective of whether there is a reasonable suspicion of criminality. Intelligence abuses thrive in societies that are not informed about surveillance and that are resigned to the perceived 'realities' of security overreach and surveillance realism (Dencik, 2018, pp. 31–43). Therefore, understanding the role of public perceptions and the circumstances in which these perceptions translate into opposition and, ultimately, action directed towards strengthening oversight of intelligence on a more sustained basis (especially in contexts where strong official oversight is lacking) is crucial to understanding how we limit a potential spiral of surveillance overreach.

This agential approach, and its possibilities and limits, is particularly relevant in a peripheral region of the world like Southern Africa, whose insertion into the global economy has been shaped fundamentally by colonialism, imperialism and, more recently, apartheid. Popular struggles against these forms of repression and exploitation led to substantial democratic gains, but subsequent transitions to independence and democracy failed to provide a genuine incorporation of the masses into the resulting political systems (Saul, 2005, pp. 17–31). Consequently, post-apartheid and postcolonial government efforts to transform intelligence systems from being tools of repressive rule to ones that were more representative of the publics they were meant to serve and protect, were incomplete and subject to democratic reversals (Duncan, 2022, p. 37–68).

Where public oversight has been studied, attention has been confined mainly to the Anglosphere and the global north, where there is a long and rich history of public oversight (see, for example, the role of journalists and public-interest groups in relation to Church Committee on intelligence abuses in the US; van Puyvelde, 2012, pp. 139–58), particularly in the wake of the whistleblowing on surveillance abuses by Wikileaks founder Julian Assange and former National Security Agency (NSA) contractor Edward Snowden (Shiraz and Aldrich, 2019, pp. 1,313–29). While their claims to the status of whistleblowers have been contested, as their disclosures of classified information went beyond what would be considered acceptable whistleblower conduct (see, for example, US House of Representatives (2016)), there can be little argument that their main motivations were to expose government wrongdoings, which is what they did, and there can also be little argument that the formal oversight structures failed to correct the wrongdoings. This book attempts to correct these biases, and to focus attention on what can be learnt from the postcolonial, post-apartheid contexts across Southern Africa, with unstable political systems that range from the superficially democratic to the semi-authoritarian. Contrary to what may be assumed at the outset, it is very possible to research intelligence and its oversight in such systems, precisely because of their relative instability.

The question is, how best can we make intelligence serve the public interest: that is, focus only on real threats (Granick, 2017) to national security and public safety? Public mobilisation can lead to successful court cases to limit surveillance powers, as was the case in South Africa, or those with technological know-how can use defensive technologies to shield themselves from surveillance (Granick, 2017). However, not all publics have access to independent judiciaries or the technological means to defend themselves, which raises the question: in circumstances where there may be limited options of litigation, and if anti-surveillance technologies are expensive, where do we go from here? The answer is to the public. However, this response triggers further questions. For example, how should publics constitute themselves to hold intelligence agencies to account for how they use digital surveillance? Are there any specific practices that public oversight should focus on and what are their strengths and weaknesses? Thus, the main research questions could be distilled as follows:

- What are the examples for successful public oversight, what accounts for the successes and what are the indicators of success? To what extent are these successes sustainable in the context in which they happened?
- What are the examples of failed public oversight and what accounts for the failures?
- What are the examples of attempts at public oversight with mixed outcomes and why did they fail to achieve complete success or complete failure?
- To what extent could the successes be replicated elsewhere across time and space and the failures or unclear outcomes avoided? What are the elements that would go into the development of a set of theoretical propositions that could be applied and guide public oversight elsewhere?

Methodology

The authors of these chapters were contracted under the global professorship to conduct the in-country research. To that end, they established research teams based in each Southern African country, and collected data through key informant interviews, focus-group discussions with key activists, document and policy analysis, and content analysis of media and news content. They identified case studies consisting of events that triggered public controversies or scandals about possible surveillance overreach. These events included moments when draft legislation or policies on surveillance, or initiatives with surveillant potential (for example, smart Identity (ID) card or Subscriber Identity Module (SIM) card registration systems) were introduced, or when information about unjustifiable surveillance of politicians, activists or journalists erupted into the public domain. They examined public responses to these moments and the factors that influenced the extent to which the public challenges to unaccountable surveillance were successful or not. The authors sought out actors from key constituencies that were central to these moments, including parliamentarians and members of government, the private sector, lawyers, the media, non-governmental organisations (NGOs) and social movements, and approached them for interviews. They sought ethical clearance in all eight countries, as well as the United Kingdom (UK), and the process of doing so was fraught with complexity due to the sensitivity of the research, and the difficulties of identifying ethical clearance bodies that were independent from the state and the ruling party.

The key question the authors focused on was how could the public perform more effective oversight digital surveillance for intelligence purposes? This question drove them to examine the factors that strengthened and weakened attempts at effective public oversight, the forms of public oversight that were the most and least effective, how they were organised and to what end. They also examined how effective public oversight could be sustained over time.

The chapters of this book provide historical and contemporary evidence of intelligence surveillance violations that, therefore, make a case for a publicly driven oversight mechanism in which the public make periodic assessments and evaluation of both surveillance practice and technologies' purchase. The actors constituting these publics included more well-organised formations with or without significant social bases, such as NGOs, social and political movements, including trade unions and youth movements, the media, lawyers, public intellectuals and academics, as well as outpourings of public opinion that took less well-organised forms, such as responses to media articles, signatories to petitions, participants in protests and public debates and the like.

The research that informed this book used a comparative case study methodology, which allowed for large-scale contextual comparisons and for both depth and scope in analysis (Voltmer and Kraetzschmar, 2015; Esser, 2019, pp. 85–101). This combination enabled explorations of the eight countries, while allowing for higher-order generalisations about what works and what does not when it comes to public oversight and recognising that it is important not to overdetermine the ability of surveillance to discipline and punish dissent (Choudry, 2018, p. 7). The comparative elements were grouped into four major themes: historical legacies, institutional organisation of oversight, mobilisation of public oversight and dynamics of conflict escalation/settlement around intelligence oversight. The research followed a most similar systems design, as all country case studies are based in Southern African countries that have similar histories of colonialism, intelligence abuses and anti-colonial/anti-apartheid struggles, and contemporary surveillance practices that have not broken sufficiently from their apartheid/colonial pasts. The intention was to identify the differences or variables that account for successful public oversight of intelligence-driven surveillance: so why has such oversight been more successful in some countries than in others, despite these shared histories and geographic proximities?

While this book focuses mainly on the case studies, it makes reference to the above-mentioned comparative elements too, as they guided the data collection across the different countries. Each researcher pursued separate case studies of critical moments when public oversight had been attempted, but using an interview guide that contained cross-cutting, common question areas that enabled comparability of the case studies. The case studies were instrumental in that they were conducted to achieve a larger goal, which was to develop more general theories around possibilities for public oversight that apply across all cases and are of more general application (Micova, 2019, pp. 71–84).

The approach adopted was inductive, as the researchers developed the case studies and then compared them to explain conditions for successful public oversight, and qualitative, as the intention was not to prove a hypothesis, but to open possibilities for better oversight. However, there were assumptions that underpinned the research, which it would be fair to spell out at the outset. We proceeded from the assumption that public oversight of digital surveillance is a poorly acknowledged, but important and, at times, decisive factor in the success or failure of oversight and, intelligence accountability. We also suspected that, when there is surveillance overreach, then organised responses are more likely to be effective than individual responses. We had suspicions that divisions in the political elite and the presence of mass movements supported by

NGOs, coupled with weak social contracts, can increase the potential for effective public oversight, as elite consensus around the need for surveillance may be weaker. We decided to put our assumptions and suspicions to the test, while remaining open to new possibilities that we had not considered.

The authors' eclectic approaches and theoretical outlook

The chapters are written by researchers with backgrounds in communication and media studies and law, who draw on the insights offered by their various fields, as well as politics and sociology, civil society practitioners and journalists, and the chapters offer a mix of more descriptive and theoretical approaches. The authors have deep knowledge of these societies and were well placed to develop bottom-up solutions to oversight problems. They were acutely aware of the risks of undertaking this research but were convinced that the potential benefits far outweigh the risks and, in fact, that not undertaking the research posed the greater risk to these societies.

The authors adopted eclectic approaches to their case studies, which is fitting for a project traversing several disciplines. No attempt was made to force a theoretical outlook on the authors, with approaches ranging from radical democratic and Marxist to political process theory: however, overall, the volume aligns most closely with the critical paradigm. For example, researchers were concerned, not only with focusing on surveillance and its impacts on individual privacy, but with surveillance and its roles in maintaining unjust and unequal societies (see, for example, Fuchs, 2010, pp. 1–22; Bellamy Foster and McChesney, 2014; Yong Jin, 2015; Giroux, 2015, pp. 108–40; Hintz et al., 2019; Couldry and Meijas, 2019, pp. 336–49; Mann and Daly, 2018, pp. 379–95), which the countries being studied largely are, despite transitions from colonialism and apartheid. Focusing on surveillance in this way means that it becomes understood as one of several social-control mechanisms that need to be tackled if substantive emancipation is to be achieved. Its oversight then becomes understood as a practice that needs to extend beyond the assumptions of representative democracy, where official oversight bodies are touted as a panacea for intelligence abuses. The researchers were also motivated by a commitment to using their research to call the powerful to account – rather than engaging in administrative research that aims to solve practical problems without changing the power structures in which they operate – and in the process aimed to change how intelligence is organised to include a broader range of oversight actors as legitimate actors.

There is, however, a paucity of literature on intelligence and surveillance oversight from a critical perspective, perhaps due to the lack of critical distance between scholarship in intelligence studies and the intelligence institutions and practices being studied (Kniep et al., 2023, p. 3). The existing literature on these issues tends to be dominated by definitions of 'oversight' that are influenced by liberal democratic thinking, informed by consensual rather than conflictual views of democracy, and revolve largely around examinations of official institutional actors and practices, such as ministers, parliamentary committees and ombuds offices (Kniep et al., 2023, p. 2). In this world-view, the state is a politically neutral instrument of the will of the people, and state institutions that perform oversight of surveillance are understood as inherently technocratic institutions with the innate potential to serve the broader public good. Oversight institutions that stray from their ultimate objectives of ensuring intelligence, lawfulness and efficacy veer towards regulatory capture perspectives, where regulators (or, in this case, overseers) prioritise sectional interests over the broader public interest (see, for example, Pillar, 2010, pp. 423–78; Gill and Phythian, 2012, pp. 179–99). When that legitimacy is damaged by rogue spies, then reforms are intended to restore that legitimacy. However, the liberal account ignores the legacy of racism, class oppression and colonialism, where certain social groups attract intelligence interest by virtue of their already diminished position in society (Choudry, 2018, pp. 7–9). Such accounts cannot conceive of a situation where entire intelligence agencies can be discriminatory, abusive or unprofessional. A key theme of this edited volume is how postcolonial intelligence agencies have continued colonial-era surveillance practices of containing dissent, with little interruption in the social control purposes of intelligence despite independence.

Core concepts used in this book

It is necessary to set out how we understand some of the core concepts used in this book, as a number of them tend to suffer from the deficiency of weak conceptualisation. Our working definition of surveillance is a set of practices that involve the systematic, routinised collection and analysis of information and the accessing of personal data for the purposes of social control. This definition separates surveillance out from other forms of periodic monitoring or information collection and analysis for more routine everyday functions. There are dangers in defining surveillance too broadly, such as the systematic collection, storage and processing of information by a variety of actors in many fields of life and for a variety of purposes (see, for example, Lyon, 1994, pp. vii–x; Clark, 1988, pp. 498–9; Marx, 2012, p. xxv). Overly broad definitions can lead to surveillance becoming normalised as a routine part of everyday life. Such routinisation will most likely lead to 'surveillance realism' (Dencik and Cable, 2017, pp. 763–81) setting in, resulting in publics accepting their fate and failing to organise against it (Fuchs, 2010, pp. 1–22; Duncan, 2018, pp. 28–36). This narrowed definition does not negate the fact that contemporary surveillance often operates in highly complex, distributed ways, but recognises that such a surveillant assemblage can, in fact, enhance social control in that it can extend the capabilities for intelligence-driven surveillance.

We understand intelligence to be knowledge of an adversary using all sources of information, including those that may have been gained by clandestine means, and aimed at protecting collective security to prevent an adversary from causing harms of major significance to it. This definition avoids one of the major dangers of intelligence, which is to define the term too broadly, leading to intelligence agencies being provided with mandates that intersect with, and even replace, other policy areas. It also avoids state-centric definitions (see, for example, the definition offered by Warner (2002, pp. 15–22) as secret state activity designed to understand or influence foreign entities) by recognising implicitly that a broader range of actors can practise intelligence. Such was the case during emancipatory struggles across Southern Africa, where national liberation movements formed their own intelligence capabilities. Beyond the more conventional roles of preventing violent attacks and other threats of national significance, increasingly governments are requiring intelligence agencies to ensure that policymakers enjoy decision advantages, by providing them with relevant conflict-winning information over issues that are vital to the welfare of the country. These additional tasks have become incorporated into definitions of intelligence that emphasise its role in supporting national interests, especially economic interests such as trade advantages, particularly on the global stage, and not just protecting against threats. Once intelligence mandates include not just threats, but interests too, including economic interests, then all manner of abuses become possible and even likely (Hager, 1996, pp. 241–3; Duncan, 2022, pp. 14–18).

We understand intelligence oversight to mean the superintendence of intelligence in a manner that is independent from the everyday management and practices of intelligence and the institutions that collect, analyse and store it (Caparini, 2007, p. 3). Exercising oversight is the key to ensuring accountability (Hotzel, 2014; Moser, 2018). Hotzel (2014) notes that oversight, in governance terms, means 'watchful care', that is, society keeping an eye on certain processes, their implementations, and the plans and decisions that, in the first instance, led to them. The intention of such oversight is to ensure that intelligence practitioners comply with their mandates, with controversies remaining over whether overseeing should be post hoc or extend to the authorisation of covert actions before they occur (Gill and Phythian, 2012, p. 173). Oversight is a precondition for intelligence accountability, where practitioners are required to explain and justify their actions (Gill 2020), deliver effective intelligence, prevent intelligence failures and build public trust (Goldman, 2016, pp. 207–34). Accountability is a counterweight to the exercise of public power on the basis of formal and informal procedural and institutional arrangements. Those who hold power should be and are, expected to explain and justify its use (Moser, 2018). The threat or shadow of sanctions can indeed influence the behaviour of actors who are aware of the fact that their conduct or performance will be analysed and, eventually, evaluated by an accountability forum. Ensuring effective accountability is likely to include demands for radical transparency in how surveillance operates that move beyond mere demands for disclosure of information (McCarthy and Fluck, 2016). Instead such transparency would need to tackle the social conditions that allowed interactions between intelligence agencies and publics to become so asymmetric and disempowering, and empower these publics with the capabilities needed to act if their demands for information are successful.

The liberal democratic 'ideals' of intelligence oversight

Democratic oversight of intelligence is meant to be an alternative to more authoritarian systems, where governments or dominant political parties may exercise stewardship over agencies. Such systems may lack any oversight structures at all or, where they exist, they are likely to be extensions of the authoritarian system rather than providing checks on it. Democratic oversight promises to check intelligence excesses and prevent surveillance overreach to ensure that intelligence agencies fulfil the broader public interest, as opposed to sectional, partisan interests.

The liberal democratic accounts of oversight that dominate intelligence literature are animated by certain guiding principles. These include ensuring that intelligence agencies respect the rule of law, where governments use laws and policies to limit state power to conduct stewardship. While recognising the need for secrecy in relation to legitimate intelligence methods, these agencies need to operate with some degree of openness and transparency. Accountability to the public through their elected representatives, and usually through a parliamentary committee, is also another key principle. The bodies that practise oversight are also meant to be independent of the agencies they oversee, have access to the information needed to facilitate effective oversight, and conduct regular reviews. There are also meant to be checks and balances between the different spheres of government to guarantee this independence and they communicate their findings to the public while maintaining legitimate secrecy. As an additional check, some countries have also institutionalised the practice of including opposition parties in intelligence briefings, to prevent capture of intelligence by ruling parties (Leigh, 2006, pp. 70–1).

In terms of its basic architecture, intelligence oversight for national security purposes is meant to cover all areas of intelligence activities, but not be reduced to micromanagement (Gill, 2020, p. 973), and can start at the executive level, taking the form of guidelines or ministerial directions, as ministers are not meant to become involved in day-to-day operations of the agency they oversee (Caparini, 2007, p. 10–11). Requiring intelligence agents to report illegal actions can also provide important information for executive oversight (Born et al., 2005, p. 46). However, in a field where executive authority is traditionally strong (Goldman, 2016, p. xvii), the executive alone cannot be relied on to police intelligence agencies, as the politicians responsible for executive oversight may have a vested interest in keeping surveillance overreach secret, to protect themselves from potentially politically damaging scandals about surveillance overreach (Goldman, 2016, p. xiv).

Other state institutions that are meant to be independent of intelligence agencies can also exercise oversight and can include the judiciary, ombuds or Inspector General offices and oversight committees. Judges can direct agencies to undertake or refrain from certain actions or oversee agencies through after-the-fact inquiries and are more likely to focus on the propriety or legality of agency actions, while parliamentary committees are likely to focus on their efficacy (Caparini, 2007, p. 3), with judicial oversight functioning effectively only when there is an independent judiciary and proper controls inside agencies (Caparini, 2007, p. 15). Parliamentary committees may be established that are responsible for adopting intelligence budgets, passing intelligence legislation and interrogating reports from agencies (Johnson, 2018, pp. 31–68; Caparini, 2007, pp. 12–13). Parliamentary oversight is important to cement civilian control of intelligence, thereby preventing militaries misusing intelligence for internal repression of dissent (Caparini, 2007, p. 3). Some countries have established single parliamentary committees to oversee all intelligence agencies, ensuring that knowledge and expertise on intelligence is retained in the same committee, some may be restricted to scrutinising matters of policy and law while others may enjoy powers to inquire into operational matters, with the former more likely to hold hearings in public than the latter (Leigh, 2006, pp. 71–2).

The existence of several layers of oversight is meant to ensure that higher levels of oversight will step in and compensate for any failures at a more subsidiary level. Ombuds or Inspector General offices, for example, could strengthen executive oversight by reporting to parliament on any failures in executive control. Parliaments, which may supposedly be at the centre of democratic oversight as they consist of elected representatives may, in fact, lack the ability to conduct investigations of their own, despite having legislative responsibility for oversight, and having administrative oversight bodies that are tasked with doing just that, assist them to detect wrongdoing that may otherwise remain secret, even to them. The oversight agencies themselves are typically legislated into being, with powers and responsibilities being set out in law and policy, and these responsibilities may extend beyond oversight entities considering the legality of intelligence actions but their propriety too, where their ethical conduct is considered (Gill and Phythian, 2012, p. 175).

Governments may also establish ad hoc committees of inquiry, particularly in the wake of a significant intelligence failure or surveillance scandal, and these too can provide an additional layer of oversight. In providing a concentrated focus on a specific issue, they can generate valuable findings, command significant media attention and galvanise the public. However, to do so, the inquiry's members would need to be independent from vested interests, their procedures would need to be robust, and they would need to operate as transparently as possible.

Systemic failures in oversight: Bringing the public back in

The liberal democratic 'ideal' of intelligence oversight provides a basic schema for how intelligence oversight is meant to operate. However, as became apparent from the Snowden revelations, it has failed to keep up with the growth in digital surveillance capabilities. It is too easy to blame lapses on the failings of individual spies instead of structural biases in how intelligence operates and systemic failures in how oversight functions, as Loch K. Johnson has argued:

> Neither the inability to predict future events with precision . . . nor the acknowledgement that secret government organisations can be a danger to open societies . . . should astound. After all, intelligence agencies are comprised of human beings – flawed by nature and devoid of a crystal ball; consequently, one can anticipate failures and abuses (Johnson, 2012, p. 6).

By individualising and exceptionalising abuses, explanations of intelligence failures and abuses risk sidestepping difficult questions about how oversight may have been structured to evade accountability. Mechanisms that have been set up, such as parliamentary committees or Inspector Generals for Intelligence, often struggle to hold the agencies they oversee accountable, and they may even be captured by these very institutions. Attempts to rein in intelligence abuses have, all too often, focused narrowly on reforms, such as improving internal controls, strengthening oversight institutions such as parliament and ombudsman, improving training and clarifying mandates. This narrow focus has led to a proliferation of oversight institutions that have not challenged sufficiently the legitimacy of modern intelligence as it is understood and practised. Typically, these oversight bodies are inadequate and continue to treat state spying on activists and journalists, infiltration of social movements and the like, as departures from what these agencies do, rather than being integral to what they do (Choudry, 2018, pp. 3–16). Judges can become captured by the very agencies they are meant to oversee and fail to take independent decisions (Gill, 2020, p. 972). Official oversight bodies may become inscribed into a circle of secrecy, where they become integrated into secretive intelligence culture, particularly if the senior officials who staff these agencies come from the very institutions that are being overseen. Therefore, the mere existence of formal oversight bodies may not prevent the growth of accountability gaps, and greater corporate involvement in intelligence is making the problem worse (Gill, 2020, p. 983), with the gaps likely to be more pronounced in so-called 'transitional societies' in the global south (Caparini, 2007, p. 21).

Accountability gaps have become even more pronounced in relation to digital surveillance, as oversight based on supervision of the national sphere of government and state intelligence activities has proved to be inappropriate in an era when intelligence is practised increasingly on a decentralised and transnationalised basis. Intelligence is also practised increasingly through public–private partnerships or by private contractors and these changes have led to intelligence capabilities outstripping the abilities of their overseers (Goldman, 2016, pp. xx–xxiii; Gill, 2020, p. 983).

The repeated failures of formal oversight to prevent intelligence abuses could be attributed to naïve assumptions about representative democracy being a substantive expression of 'the will of the people', held in check by the supposed rationality of bureaucratic power, but which can all too easily boil down to government by elites. These ideals are unlikely to be sufficient to ensure substantive intelligence accountability, which may well need to be animated by more participatory forms of democracy that can occur in contrast to, and even in defiance of, the formal institutions of representative democracy. Consequently, real moments of effective intelligence oversight have occurred through public mobilisation, using strategies such as litigation, advocacy and whistleblowing (Kniep et al., 2023, p.2). In the wake of the Snowden disclosures, whistleblowing has received more attention. By virtue of their proximity to classified information, whistleblowers can expose intelligence abuses, but they can do so only if they are protected and not persecuted. This may be the case especially in situations where internal organisational cultures rest on codes of professional ethics that require adherence to the highest standards of conduct (Caparini, 2007, p. 11).

When the media, NGOs and citizens are acknowledged as part of the oversight system, their role often seems secondary to the main discussion about oversight structure. However, these groups can support parliaments in their oversight duties by highlighting abuses through research, journalism, legal action and advocacy (Gill and Phythian, 2012, p. 175). Their roles in exposing intelligence scandals when they occur – what Loch K. Johnson refers to as a shock theory of intelligence accountability, where intelligence scandals or alarms lead to intense bursts of intelligence accountability (Johnson, 2018, pp. 209–46) – can lead to lasting changes to intelligence law, policy and practice. Their success often depends on their ability to generalise claims about injustice, which many social actors have failed to do when confronted with major, generalised government claims around national security, and where their counterarguments may be in defence of singular groups or rights (Aradau and McCluskey, 2022, pp. 1–19).

But who exactly is the public? How publics have been constituted differ from one context to another and depends largely on the politics of the day (Ku, 2000). For example, in more liberal and democratic contexts, public oversight of state institutions may not only be tolerated, but encouraged (Brennan Centre for Justice, 2021). But the question would be: who exactly constitutes 'the public' that we are talking about? Some of the earliest conceptualisations of 'the public' in Africa (for example, Mamdani (1996) dichotomise them into two: the elite (the citizens with power) and the subjects (those acted upon by power)). In this book, we understand the public in a rather clear and straightforward sense. For a start, we use the term 'the public' in this book only in reference to intelligence oversight. We, therefore, mean citizen agency, meaning those citizens who are not part of the institutions tasked with surveillance. We also mean those who are not part of the policy-making circles. This means, rather in a paradoxical sense, citizens who are constituted to provide a layer of oversight on data-driven intelligence. In other research, public oversight has been interpreted to mean community oversight of surveillance (Cole, Eppert and Kinzelbach, 2008). Public oversight, hence, means a broad coalition of local groups and activists working to end the unchecked surveillance of communities by local agencies – including law enforcement and military and civilian intelligence – and to ensure that people have a say in whether, what, and how surveillance technology is acquired and used in their country or locality. In all this myriad of interpretations of what exactly constitutes the public, there are key points of convergence about this question. Firstly, the public are 'outsiders'. In other words, they are civilians who have little or no connection to the agencies of surveillance which they should watch over. Secondly, they are civilians (Ku, 2000) exercising independent agency on surveillance practices and institutions. Thirdly, they have one major objective – to hold institutions accountable for the work they do, ensure they do it within the limits and provisions of the law, and safeguard civilian rights and fence them off from intrusion by surveillance institution. When this objective is met, it, possibly, can bridge the distrust between the institutions of surveillance and the communities of the surveilled.

However, and as Mamdani (1996) alludes to, publics in Southern Africa are deeply divided along the lines of class, race, gender and other social fault lines. They may be constituted in elite ways that claim to represent the public, but in reality, represent organisations with no real social base. Others may be constituted in more mass-based, popular ways. Under certain conditions, and if pushed far enough by public pressure, private companies may switch sides and defend citizen privacy if it is in their business interests to do so, thereby contributing to public oversight. So, apart from examining how privatisation of intelligence functions has contributed to the weakening of official oversight, and presented new challenges for public oversight, the chapters will also examine the following questions: under what conditions can the private sector contribute to public oversight rather than evading it?

In short, the chapters interrogate how publics have been constituted for surveillance oversight, which forms of mobilisation have had lasting, positive effects and which forms have been less successful.

Outline of chapters

The chapters in this edited volume include contextual information about the country's intelligence agencies, how they are organised and their oversight, as well as (to the extent that is possible, given the often secretive nature of the information) information about their capabilities for surveillance. The articles will focus on drawing out the lessons for public oversight, particularly as they relate to digital surveillance practices or practices with considerable surveillance potential. The practices examined in these chapters are diverse, and include smart cities and surveillance (Mauritius); state intelligence surveillance and its oversight (Botswana); targeted surveillance and oversight (Angola, Zimbabwe and the DRC); transnational signals intelligence surveillance and its oversight (Mozambique and South Africa); SIM-card and mobile-device registration and public responses (DRC, Namibia and Mozambique) and biometric surveillance in the context of identity management (Mauritius). The chapters then proceed to illuminate different elements of public oversight, and what it takes to build it, sustain it and make it effective. This book makes several but closely related arguments. The broader argument we sustain throughout the interlinked chapters is that, beyond judicial and executive surveillance models that are common, a new model of public oversight of surveillance is possible and, arguably, functions better than extant approaches to surveillance. In making this argument, our starting point is that extant oversight mechanisms have declined in efficacy and in some other contexts, been circumvented by partisan institutions. There is, hence, the need for a new model of oversight, especially one that is novel enough to include civilians. A publicly driven model, which we will outline some essential elements of in the concluding chapter, would likely increase transparency of intelligence surveillance and substantive accountability. It can do this by providing another layer of oversight existing independently from, and at times even in antagonism to, state/corporate power. Each chapter of this book sustains this argument in several ways.

Rui Verde explores the role of international pressure in public oversight, to compensate for a grossly inadequate formal oversight of state intelligence in Angola, which he characterises as an anocratic regime. As he discusses, such a regime, is neither completely open to political contenders due to autocratic tendencies nor is it completely closed to moments of democratic opposition. Such a moment occurred in relation to the 15+2, or Luanda Reading Club case, touched on earlier. Verde shows how public oversight forced the hasty approval by parliament of an amnesty law after a massive international outcry at their conviction. Verde also explores whether or not international pressure opened up meaningful spaces for local activism.

In the case of Botswana, Tachilisa Badala Balule explores the role of public oversight driven by popular agency of a constellation of civil society and social-movement actors and is another example of successful public oversight. While local networked activism was more of a feature in this case than in the Angolan case, it has yet to translate into more nationally sustained oversight, but nevertheless the potential is there. Balule discusses how the controversies around the Criminal Procedure and Evidence Bill mentioned earlier, led to the government having to walk back some of the worst elements of the Bill that threatened basic democratic rights and freedoms. There is, however, evidence that popular agency oversight over the security sector in the country remains limited despite this victory, and the question Balule attempts to answer is, why?

Trésor Maheshe Musole examines the factors that militate against successful public oversight in the DRC, and seeks to answer two questions: what are the explanatory factors for the low interest of Congolese civil society in the issue of surveillance and how could civil society actions limit the abuses of surveillance? The chapter utilises two cases – one successful and relating to opposition to the registry of mobile devices, and the other unsuccessful and relating to the surveillance of public figures – to account for low monitorial interest on the part of civil society organisations and suggests ways through which the public, through organised formations, can be engaged in action that limits surveillance abuses. By analysing these two cases, the chapter clearly articulates how public oversight can be successful, and the inhibiting factors that can make it fail.

Sarah Chiumbu discusses the factors influencing public oversight of digital surveillance in Mauritius, which provides arguably the most impressive example of local activism discussed in this edited volume, and one that has reduced the scope for surveillance overreach on a more sustained basis as popular consciousness of the dangers remain embedded in the social fabric. Chiumbu discusses how in 2013 the Mauritian government introduced the smart ID card to replace the previous National ID Card as a public-public partnership with Singapore, and how through opposition from the public, activists and civil society organisations, who were concerned that the government could use this information for surveillance purposes or to track the activities of citizens, the government suspended the project in 2015. It looks at why sections of the public were open to being mobilised and how a popular campaign around surveillance can be built and achieve lasting gains, and emphasises the importance of relating surveillance to bread-and-butter issues.

Ernesto Nhanale and Borges Nhamirre offer a much more sombre analysis of the structural environment for the failing of oversight mechanisms in Mozambique, both formal and public. They examine the continuities between colonial authorities and the post-liberation state as a key factor that has limited scope for meaningful oversight. They argue that the absence of such oversight mechanisms could be attributed, not only to the political culture of colonial control continuing into the post-colony, reaching deep into society and exacerbated by military conflicts, but also to an institutional and legal model with its roots deep in colonialism, and which the government is still reluctant to restructure. This reluctance is an important factor in the maintenance of Frelimo as the only actor in the political system and national governance.

Frederico Links and Phillip Santos explore the systemic failure of digital surveillance oversight of the Namibia Central Intelligence Service (NCIS), despite the country being touted as a postcolonial democratic success story. They explore how official oversight has been set up to fail and, consequently, how the media have stepped into the breach and used judicial activism to roll back the culture of secrecy around surveillance. Links and Santos utilise a critical incident to make their argument. In August 2018, in the High Court of Namibia, lawyers acting on behalf of the NCIS and the Namibian government argued on the record that the intelligence agency should ‘be insulated from both parliamentary and judicial oversight’. This they did as part of their attempt to prevent a local newspaper from revealing evidence of corruption and mismanagement in the NCIS. However, the NCIS lost the case.

Jane Duncan explores the difficulties of maintaining public oversight over surveillance. She uses a successful campaign in South Africa as a case study to illustrate her points. She examines the campaign around a controversial ‘Secrecy Bill’, which was broadened to focus on the inappropriately large roles of surveillance, intelligence and security institutions in the governance of contemporary society, and why it could not be sustained. Through the lens of political process theory underpinned by a critical approach, this chapter examines the factors that contributed to the rise and fall of anti-surveillance activism in South Africa. She shows how the anti-surveillance activism that was taken forward in the wake of the campaign, was done so in less mass-based and more elitist ways, such as strategic litigation in the absence of a mobilisation strategy, which has led to the considerable capacity that has been built in civil society struggling to curtail surveillance powers on an ongoing basis.

Allen Munoriyarwa seeks to envision a new civilian-driven model for countering state authoritarianism in surveillance regulation bolstered by private actors, especially from China and Iran, using two surveillance scandals in Zimbabwe as the backdrop. He explains how Zimbabwe is contending increasingly with a slew of digital surveillance practices ranging from location surveillance, digital communication, public-space surveillance and many more. Drawing on the critical-incidents method and on limited interviews with civic-society actors, legislators and activists, Munoriyarwa seeks to answer three questions: to what extent can the state lead a transparent and effective surveillance regime which does not, by design or by accident, unnecessarily infringe on individual privacy; how can surveillance institutions be held accountable for their actions; and, lastly, what pathways exist to bolster collective civilian inclusion in surveillance regulation?

In the concluding chapter, Jane Duncan and Allen Munoriyarwa tie up the arguments made in the book. They reflect on the current trajectories of intelligence surveillance in the region, and What it is likely to morph into both the long and the short term. In addition to this, they also reflect on the elements of a publicly driven models of intelligence oversight, drawing on the evidence presented in the chapters. Doing so allowed them to start developing a theoretical basis to predict conditions in which public oversight is likely to succeed.

As the editors, we hope that this book will be of immediate benefit to some of the most socio-economically deprived countries in the world, where the risks of using surveillance powers to stabilise existing power structures, instead of addressing the root causes of inequality, are high. We also believe that the lessons to be learnt from these countries are of global relevance because bottom-up change is more likely to occur in political systems with less social consensus and consequently more political ferment.

References

Aradau, C. and McCluskey, E. 2022. Making digital surveillance unacceptable? Security, democracy, and the political sociology of disputes. *International Political Sociology*, 16, pp. 1–19. [Online]. [Accessed 20 July 2023]. Available from: https://doi.org/10.1093/ips/olab024.

Balule, B.T. and Dambe, B.J. 2023. Surveillance within the law: A critique of the legal framework for surveillance of digital communications by Law Enforcement Authorities in Botswana. *Statute Law Review.* 44(2), pp. 1–14.

Bellamy Foster, J. and McChesney, R. 2014. Surveillance capitalism: Monopoly-finance capital, the military-industrial complex, and the digital age. *Monthly Review.* 66(3).

Born, H., Johnson, L. and Leigh, I. 2005. *Who's watching the spies?: Establishing intelligence services accountability.* Sterling, VA: Potomac Books.

Bovens, M.W, Thomas, S. and Goodin, E. 2014. Public accountability. In: Goodin, T. ed. *The Oxford Handbook of Public Accountability*. Oxford: Oxford University Press, pp. 114–120.

Brennan Center for Justice. 2021. The public oversight of surveillance technology (POST) Act: A resource page. [Online]. [Accessed 24 August 2023]. Available from: https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page.

Caparini, M. 2007. *Democratic control of intelligence services: Containing rogue elephants.* Aldershot: Ashgate.

Choudry, A. ed. 2018. *Activists and the surveillance state: Learning from repression.* London: Pluto Press.

Clarke, R. 1988. Information technology and dataveillance. *Communications of the ACM*. 35(5), pp. 498–9.

Cole, E., Eppert, K. and Kinzelbach, K. 2008. *Public oversight of the security sector: A handbook for civil society organizations.* UNDP Bratislava Regional Centre; Geneva Centre for the Democratic Control of Armed Forces (DCAF). [Online]. [Accessed 10 August 2023]. Available from: https://www.undp.org/publications/public-oversight-security-sector-handbook-civil-society-organizations.

Couldry, N. and Mejias, U.A. 2019. Data colonialism: Rethinking big data's relation to the contemporary subject. *Television and New Media.* 20(4), pp. 336–49.

Dencik, L. 2018. Surveillance realism and the politics of imagination: Is there no alternative? *Krisis: Journal for Contemporary Philosophy*. 1, pp. 31–43.

Dencik, L. and Cable, J. 2017. The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*. 11, pp. 763–81.

Duncan, J. 2022. *National security surveillance in Southern Africa: An anti-capitalist perspective*. London: Bloomsbury Academic & Professional.

Duncan, J. 2018. *Stopping the spies: constructing and resisting the surveillance state in South Africa*. Johannesburg: Wits University Press.

Esser, F. 2019. Comparative research. In: Van den Bulck, H., Puppis, M., Donders, K and Van Audenhove, L. eds. *The Palgrave Handbook of Methods for Media Policy Research.* Palgrave Macmillan, pp. 85–101.

Fuchs, C. 2010. How can surveillance be defined? Unified Theory of Information Research Group. *The Internet and Surveillance Research Paper Series,* 1, pp. 1–22. [Online]. [Accessed 2 August 2023]. Available from: http://www.sns3.uti.at/wp-content/uploads/2010/10/The-Internet-Surveillance-Research-Paper-Series-1-Christian-Fuchs-How-Surveillance-Can-Be-Defined.pdf.

Gill, P. 2020. Of intelligence oversight and the challenge of surveillance corporatism. *Intelligence and National Security.* 35(7), pp. 970–89. doi: 10.1080/02684527.2020.1783875.

Gill, P. and Phythian, M. 2012. Intelligence in an insecure world. Cambridge: Cambridge University Press.

Giroux, H.A. 2015. Totalitarian paranoia in the post-Orwellian surveillance state. *Cultural Studies*. 29(2), pp. 108–40.

Goldman, Z.K. 2016. The emergence of intelligence governance. In: Goldman, Z.K. and Rascoff, S.J. eds. *Global intelligence oversight: Governing security in the twenty-first century*. New York: Oxford Academic, pp. 207–34.

Granick, J.S. 2017. *American spies: Modern surveillance, why you should care, and what to do about it*. Cambridge: Cambridge University Press.

Hager, N. 1996. *Secret Power.* Nelson: Craig Potton Publishing.

Hintz, A., Dencik, L. and Wahl-Jorgensen, K. 2019. *Digital citizenship in a datafied society*. Cambridge: Polity Press.

Hotzel, S. 2014. The concept of oversight, its connection to memory keeping and its relevance for the medium term: the findings of the RK&M Initiative. Constructing Memory – International Conference & Debate on the Preservation of Records, Knowledge and Memory Across Generations. Verdun, France: 15–17 September 2014.

Johnson, L.K. 2012. *National security intelligence*. Cambridge: Polity Press.

Johnson, L.K. 2018. *Spy watching: intelligence accountability in the United States.* Oxford: Oxford University Press.

Kniep, R., Ewert, L., Reyes, B., Tréguer, F., Cluskey, E. and Aradau, C. 2023. Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies.* pp. 1–21. doi:10.1017/S0260210523000013.

Ku, A.S. 2000. Revisiting the notion of 'public'. *Sociological Theory*. 18(2), pp. 216–40.

Leigh, I. 2006. The accountability of security and intelligence agencies. In: Johnson, L.K. ed. *Handbook of intelligence studies*. Abington: Routledge, pp. 67–81.

Lyon, D. 1994. *The electronic eye: the rise of the surveillance society.* Minneapolis: University of Minnesota Press.

Lyon, D. 2015. Keynote presentation to the International Association for Media and Communications Research, 14 July 2015. [Online]. [Accessed 15 July 2023]. Available from: https://www.youtube.com/watch?v=Vzgok3kUl0o.

Lyon, D. 2018. *The culture of surveillance: watching as a way of life.* Cambridge: Polity Press.

Mamdani, M. 1996. *Citizen and subject: contemporary Africa and the legacy of late colonialism.* Princeton: Princeton University Press.

Mann, M. and Daly, A. 2019. (Big) data and the north-in-south: Australia's informational imperialism and digital colonialism. *Television and New Media*. 20(4), pp. 379–95.

Marx, G. 2012. 'Your papers please': Personal and professional encounters with surveillance. In: Ball, K., Haggerty, K.D. and Lyon, D. eds. *Routledge handbook of surveillance studies.* Oxford: Routledge, pp. xx–xxxi.

McCarthy, D.R. and Fluck, M. 2016. The concept of transparency in International Relations: Towards a critical approach. *European Journal of International Relations*. 23(2), pp. 416–40. [Online]. Available from: https://doi.org/10.1177/1354066116651688. Accessed 5 July 2023.

Micova, B.S. 2019. Case study research. In: Van den Bulck, H., Puppis, M., Donders, K. and Van Audenhove, L. eds. *The Palgrave Handbook of Methods for Media Policy Research.* Cham: Palgrave Macmillan, pp. 71–84.

Moser, C. 2018. Conceptualising accountability in the legal and institutional framework of the OSCE. Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper. [Online]. [Accessed 20 August 2023]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228528.

Munoriyarwa, A. and Mare, A. 2022. *Digital surveillance in Southern Africa*. Cham: Palgrave Macmillan.

Ndlovu, T. 2022. Botswana civil society rebuff Criminal Procedures Bill. Association for Progressive Communications. 23 August. [Online]. [Accessed 5 July 2023]. Available online: https://www.apc.org/en/news/botswana-civil-society-organisations-rebuff-criminal-procedures-bill.

Pillar, P. 2010. The perils of politicisation. In: Johnson, L. ed. *The Oxford handbook of national security intelligence.* Oxford: Oxford University Press, pp. 472–84.

Saul, J. 2005. *The next liberation struggle: Capitalism, socialism and democracy in Southern Africa.* Toronto: Between the Lines.

Schedler, A., Diamond, L.J. and Plattner, M.F. eds. 1999. *The self-restraining state: power and accountability in new democracies*. Boulder, CO: Lynne Rienner Publishers.

Shiraz, Z. and Aldrich, R.J. 2019. Secrecy, spies and the global South: Intelligence studies beyond the 'Five Eyes' alliance. *International Affairs.* 95(6), pp. 1313–29. [Online]. [Accessed 20 July 2023]. Available from: https://doi.org/10.1093/ia%2Fiiz200.

US House of Representatives. 2016. Review of the unauthorised disclosures of former National Security Agency contractor Edward Snowden. [Online]. [Accessed 10 January 2024]. Available from: https://www.congress.gov/committee-report/114th-congress/house-report/891/1.

Van Puyvelde, D. 2013. Intelligence accountability and the role of public interest groups in the United States. *Intelligence and National Security.* 28(2), pp. 139-158, Available from: https://doi-org.ezproxy1.lib.gla.ac.uk/10.1080/02684527.2012.735078.

Van Puyvelde, D. 2018. Qualitative Research Interviews and the Study of National Security Intelligence. *International Studies Perspectives*. 19(4). November, pp. 375–391. [Online]. [Accessed 1 August 2023. Available from: https://doi-org.ezproxy1.lib.gla.ac.uk/10.1093/isp/eky001.

Verde, R. 2021. *Words and actions: a realistic enquiry into digital surveillance in contemporary Angola.* Johannesburg: Media Policy and Democracy Project. [Online]. [Accessed 15 August 2023]. Available from: http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/report_03_2021_words_and_actions_angola_masterset.pdf.

Voltmer, K. and Kraetzshmar, H. 2015. *Investigating the media and democratisation conflicts: Research design and methodologies of media, conflict and democratisation*. Media Conflict and Democratisation (MeCoDEM). [Online]. Accessed 12 July 2023. Available from: https://eprints.whiterose.ac.uk/id/eprint/117317/1/VoltmerKraetzschmar-2015_Investigatingmediaanddemocratisationconflicts.pdf.

Warner, M. 2002. 'Wanted: A Definition of Intelligence'. *Studies in Intelligence.* 46(3).

Wegge, N. and Wentzling, T. 2018. Contemporary and Future Challenges in Effective Intelligence Oversight. In: Leigh, I., & Wegge, N. Eds. *Intelligence oversight in the twenty-first century: accountability in a changing world* (1st ed.). Oxford: Routledge. https://www.routledge.com/Intelligence-Oversight-in-the-Twenty-First-Century-Accountability-in-a/Leigh-Wegge/p/book/9780815393344.

Yong Jin, D. 2015. *Digital platforms, imperialism and political culture.* Oxford: Routledge.

Zuboff, S. 2019. *The age of surveillance capitalism.* London: Profile Books.