CHAPTER TEN

Current trajectories and future challenges for public oversight

Jane Duncan and Allen Munoriyarwa

Introduction

In this concluding chapter, we assess the major findings from each of the chapters and return to the original question posed in the introduction, of how the public can perform more effective oversight digital surveillance for intelligence purposes. Each chapter has presented case studies of moments when public oversight has been attempted and either succeeded or failed or achieved mixed outcomes. All the cases discussed could be considered examples of public oversight, or 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, to ensure accountability. They detailed examples of the public engaging in demands for radical transparency in this secretive area of state power, by exercising 'watchful care' over how digital surveillance has been used and abused. The chapters analysed moments when the public required intelligence agencies to explain and justify surveillance and change surveillance practices when they amounted to abuse (McCarthy and Fluck, 2016). Some of these cases involved intelligence and surveillance laws or state-sanctioned data-processing systems that the public feared had surveillant potential. Others followed the shock-driven approach to intelligence reform, where controversies around surveillance abuses came into the

public domain through whistleblowing or the leaking of intelligence information, and these controversies galvanised public action of various kinds (Johnson, 2018, p. 209–46). This chapter uses a summary of the main chapter findings to address key research questions and to develop a set of theoretical propositions about public oversight and the conditions under which it is likely to succeed.

The case studies: Main findings

The Angolan case examined an example of successful public oversight, namely the highly controversial 15+2 case where activists were released followed by a general amnesty after an international campaign following their conviction for organising a reading group the then government considered to be threatening. The 15+2 case saw public oversight compensating for weaknesses in the security services and the courts, both of which were shown to lack independence from the ruling party, resulting in the hasty approval by parliament of an amnesty law after a massive international outcry over the convictions of the accused. The fact that Angola is what the author characterised as an anocratic regime, which is inherently unstable, made it more susceptible to public pressure as its political institutions were weak, the rule of law was applied inconsistently and the government lacked the capacity to maintain central authority and manage conflict effectively. The case study suggested that far from being adept at coercive control, the security services were poorly institutionalised and vulnerable to marginalisation within government when their ineptness became politically embarrassing.

However, the case was marked by a disjuncture between the success around the 15+2 case and the actual capacity on the ground to perform public oversight in Angola. The success of the campaign could not be sustained and deepened into a lasting movement that changed the oppressive state-society relations that continue to beleaguer Angolan society. The public oversight that was performed was very truncated and scandal-driven, focusing particularly on the hunger strike of Luaty Beirão and the embarrassment it caused the government. The government was responsive mainly to international

organisations and adverse publicity in the Portuguese press and the US diplomatic establishment, rather than local pressure. This outsized focus on international outrage suggested a lingering deference to its former colonial power and the US, and a reluctance to take local actors seriously. Consequently, once all the international fanfare around the case had died down, it became apparent that there had been no lasting changes in oversight practices and even journalists, as potentially a more well-organised and resourced social force, were ill-equipped to take on the challenge.

Botswana is widely considered to be on the democratic end of the political spectrum, yet this characterisation masks deeper authoritarian tendencies that manifest themselves in centralised control of civilian intelligence. The author attributes these authoritarian tendencies to a continuity of intelligence and surveillance practices from the colonial-era police Special Branch with its political intelligence-gathering mandate in the furtherance of empire and deliberate lack of oversight, to the democracy-era DIS and notwithstanding the fact that the DIS was a postcolonial creation. The author also pointed to the lack of professionalisation of intelligence, evident from its factionalisation, where different factions of the ruling party misused surveillance capabilities to keep one another under surveillance. The courts provided some respite in performing more independent official oversight and have shown that they would not be deferential to the executive on national-security matters (a term which remains ill-defined). However, the centralisation of the DIS under the presidency undermines accountability, as it gives the president the secretive powers of intelligence to settle scores. Oversight has been introduced begrudgingly and limited in various ways.

Nevertheless, there exists some national capacity for public oversight in Botswana and, as was shown in the campaign around the Criminal Procedures and Evidence Bill, established human-rights and media organisations can collaborate on surveillance overreach when they need to do so, to the point of lobbying parliament effectively on a bipartisan basis before the debate on the Bill. The campaign against the Bill also received strong regional and international support, particularly through the organised media, and

especially from editors. The government was open to changes to the Bill, but not to the extent of including a provision around post-surveillance notification, where surveillance targets are informed that surveillance had occurred once the case reaches a non-sensitive stage. The campaign was also boosted by journalists who had access to whistleblowers within DIS, who tipped them off that they were under surveillance, providing some evidence of abuses and taking surveillance out of the realm of an abstract possibility and into the realm of a real and pressing threat to media freedom. However, the difficulty of obtaining funding for sustained public oversight has proved to be an obstacle, as is the lack of resources for investigative journalism and the lack of independence of civil society organisations and journalists. The lack of accountability of the media also limits their ability to act as credible watchdogs over the intelligence sector.

The DRC provides interesting and instructive examples of public oversight and a possible way forward in terms of how to organise it, in ways that legislate cooperation by all the main actors in relation to surveillance and its oversight. In the case of the campaign around the controversial Registry of Mobile Devices, or RAM, public pressure led to an unpopular RAM tax being abolished, which the author analysed in terms of the theory of affected interests, where action is more likely to be taken by a political community when common interests are affected by a national decision. In contrast, other surveillance cases in the DRC did not lend themselves to mobilisation as the issues were more abstract and individuals were affected. However, in at least one case, where a journalist, Stanislas Bujakera, was convicted for sharing what was alleged to be false information from the internal-security department of the National Intelligence Agency, and on the dubious grounds that the information came from his Internet Protocol (IP) address, public pressure was also brought to bear on the case to the extent that he was released despite having been convicted. In a striking similarity to the Angolan case, the foreign media had a strong role to play in this case, particularly the French press, suggesting that the government was sensitive to foreign criticism. Yet, despite the successes of these two cases, surveillance oversight has not become a specialism of civil society

in the DRC, although there was potential for this to happen given the legislating into being of local-community safety councils with the responsibility to develop local-community safety plans, and the potential to include representatives of public authorities and civil society organisations. These councils could provide the basis for sustained, bottom-up oversight of security powers, including surveillance. However, as legislated bodies they remain vulnerable to political control, evident from the fact that they still require a presidential decree to bring them into being.

Like Botswana, Namibia is an example of a stronger democracy than most in the region, with a highly centralised civilian-intelligence agency but with capacity in civil society to perform sustained and informed public oversight, despite the country's small population. Unlike Angola, Namibian civil society has been able to achieve a more consistent and less scandal-driven form of oversight. The NCIS has poor internal controls and external oversight, but in the case of *The Patriot* newspaper, the judiciary stepped in and asserted its right to perform oversight, which the NCIS accepted, suggesting respect for the rule of law. Namibia has strong domestic civil society capacity to deal with the technical issues around surveillance and to translate them into publicly understandable messages, a case in point being SIM-card registration and its surveillant potential, through consistent civil society and media work on the issues, leading to the media and civil society contributing what the authors have referred to as a democratic subsidy around intelligence oversight. International actors have played a consistent monitoring role and, to that extent, their interventions have been less episodic and scandal-driven than in Angola. Opposition politicians also raise important issues around surveillance, which brings the electoral competition that does exist to bear on the problem. However, even though capacity does exist, public oversight can be, and has been, overridden on key issues, showing that it still lacks the social power needed to act as a brake on surveillance abuses or initiatives with surveillant potential.

Mauritius is a compelling example of a successful case of public oversight and the chapter was one of several that pointed to the diversity of surveillance practices or state practices with surveillant

potential. This diversity complicates oversight as it requires anti-surveillance activists to do more work than they ordinarily would need to, to explain why the public should be concerned. In this regard, the author examined the potential for a centralised, smart, biometrically based ID card to become a tool for digital surveillance, and used a mixed-theory approach to examine the factors that allowed the campaign against the smart-ID-card system to achieve at least partial victory. She concluded that organised political forces or policy entrepreneurs in Mauritius exhibited a high degree of consensus that led to successful public oversight, and a change in government also played a role in the amendment of the biometric ID card. Their mobilisation strategies included being able to frame a government initiative to improve citizen-identification services that would, on the surface of things, have little to do with intelligence-led surveillance, as one with surveillant potential and a potential danger to citizen privacy. They were also able to mobilise a broad cross-section of society through popular campaigns that extended to the political opposition who took the campaign up as part of an electoral platform. The author attributed successful mobilisation to a combination of specific historical factors, notably the international context of heightened sensitivity to the dangers of surveillance that coincided with the Snowden revelations, as well as public sensitivity to the potential for government surveillance before an election. There were also deeper factors peculiar to Mauritius as a society that contributed to this success story, such as a deep concern for privacy and enmity towards government initiatives that smacked of surveillant colonial practices, a mobilised and deep-rooted culture of organising and political opportunities to ensure that activism had an effect, although there is more recent evidence of democratic backsliding. There is much to be learnt from how the campaign against the smart-ID-card system was organised, as these lessons can be applied elsewhere in the hope of achieving similar successes. However, the structural conditions that made Mauritius receptive to the activism were peculiar to Mauritius and were unlikely to be replicated in other countries with different histories and social structures.

Mozambique presents a much bleaker picture, in that it showed

deep continuity between Portuguese colonial and postcolonial intelligence practices, and the fact that Mozambique fuses democratic and authoritarian characteristics facilitated this continuity. The Portuguese International State Defence Police were involved in the maintenance of colonial rule until the popular uprising in Portugal itself, but this colonial tradition of using intelligence for political policing was embraced by Frelimo, and they used the civil war as a pretext to maintain these problematic surveillance practices. They also militarised state intelligence under the party's control, initially through a one-party system, and then through a nominally democratic political system with the appearance of electoral competition and institutionalised, professionalised intelligence services, but with very little substantial democratic content. This lack of a democratic culture accounts for the failures of civil society to mobilise successfully against the government's centralised, expansive intelligence and surveillance powers, as government has promoted an uncritical citizenry. The government has made the abuse of these powers more likely by keeping the legal remit and accountability of postcolonial intelligence deliberately unclear, and collapsing the separation of powers between the executive, legislature and judiciary on the basis that it has the moral authority to lead all aspects of society.

South Africa, on the other hand, offers a mixed picture of tremendous success in activist mobilisation and strategic litigation against state secrecy and the excessive power of state intelligence services under former president Jacob Zuma, followed by an inability to sustain a campaigning style for public oversight. The author examined how an attempt to establish a popular campaign that attempted to combine the best traditions of non-governmental organizations (NGOs) and social movement organising led to a campaign that broadened out from a focus on a Protection of State Information Bill to include intelligence and surveillance abuses that appeared to be taking place under the guise of intelligence secrecy. The campaign was able to generalise intelligence and surveillance abuses across society by relating them to popular struggles against exploitation and oppression, thereby making them relevant to affected interests. The lack of definition of the campaign's popular base proved to be

the campaign's undoing, though, with anti-surveillance work having to shift gear and focus on strategic litigation and culminating in a blockbuster victory against South Africa's main surveillance law, Rica, in the Constitutional Court. However, strategic litigation lacked a popular base and was unable to maintain public pressure after the Constitutional Court case. Ultimately, anti-surveillance activism in South Africa was a victim of broader demobilisation of social movements in the wake of the 2008 global recession and underscored the need to use litigation without sacrificing a popular base and social-justice focus.

In the case of the semi-authoritarian Zimbabwe, intelligence services have been highly partisan from the colonial and pre-independence periods, with no real period of professionalisation after independence. The author examined how the first post-independence leader, President Robert Mugabe, set about designing Zimbabwe along deliberately authoritarian lines. The civilian intelligence agency, the CIO, which was absorbed wholesale into the government from the colonial era and which was responsible for the maintenance of British imperial interests in then-Rhodesia, followed by white minority interests, was central to his designs. This longstanding problem of intelligence partisanship has led to mission creep, where the country's military intelligence where the country's military intelligence have meddled in civilian matters, as the CIO could not be trusted even within the ruling ZANU-PF government due to its alignment with Mugabe. ZANU-PF became factionalised, which ironically, created greater potential for activism around surveillance abuses as these concerns reached right up to the highest levels of the political establishment as different factions feared being spied on by other factions. Nevertheless, there was no real public outcry when prominent Zimbabweans were put under surveillance, echoing the finding of the DRC chapter about the lack of affected interests. However, the fact that intelligence services in Zimbabwe have discredited themselves through partisanship, especially the CIO, has created scope for reform, as has the limited scope for parliamentary and judicial oversight given the lack of independence of these institutions. In view of these challenges, the author proposes a multivariate model of oversight that involves the key actors into an institutional mech-

anism that locks the official actors into a civilian-led oversight mechanism, rather than relying on them to perform oversight of their own initiative, and forces greater transparency and accountability in how state intelligence conducts surveillance.

Bringing the findings together: Assessing the state of public oversight

The chapter findings provided data to attempt answers to the research questions posed in the introduction. The Angolan 15+2 case, the Botswana campaign around the Criminal Procedures and Evidence Bill, the campaigns in the DRC against the RAM tax and the release of journalist Stanislas Bujakera despite his conviction, the campaign against the smart-ID-card system in Mauritius, the case involving reportage by *The Patriot* newspaper on corruption in the Namibian NCIS's and the Agency's failed attempt to prevent publication, and the anti-surveillance and anti-secrecy campaigning, culminating in strategic litigation against Rica in South Africa, are some of the stand-out moments discussed in the chapters. They were examples of successful public oversight, in that these democratic victories against extant or potential digital surveillance abuses extracted costs from the respective governments and were won through public action. The Botswana and South African cases had lasting impact in that laws were changed in ways that reduced the scope for surveillance abuses beyond the scandals that brought the issues to public attention. Actions taken ranged from strategic litigation to lobbying of policymakers and legislators, public education, pickets and protests, investigative journalism and media publicity. The indicators of success were that these public oversight interventions led to individuals who had been convicted wrongly, being released or not being imprisoned, the abandonment or partial abandonment of government initiatives with surveillance potential and the redrafting of laws allowing for surveillance overreach.

All these countries had differing opportunities for formal oversight, with South Africa offering the most opportunities. Nevertheless, the formal oversight mechanism barely features in the successful

case studies as having contributed to meaningful oversight, except for the judiciary. Interventions were more likely to succeed when public interventions could appeal to a responsive court system willing to act independently from the government on national security matters, when intelligence agencies respected court decisions, when campaigns had an international element, and when established civil society actors adopted a popular campaigning element combined with technical expertise on digital surveillance. Journalists and journalists' organisations could also play a decisive role with their ability to mobilise resources, provide publicity and explain the dangers of digital surveillance to the public.

The ineffectiveness of formal oversight institutions provided opportunities for public oversight. During economic downturns, voters tend to withdraw from the electoral system, and this trend is pronounced across Africa (Halfdan and Coma, 2022). The decline in electoral participation has implications for formal oversight, especially parliamentary oversight, as it can lead to a loss of confidence in electoral politics that provide state institutions with the legitimacy to perform oversight on behalf of the public. If more governments are governing with smaller voter mandates, then the edifice on which state institutions, including intelligence oversight institutions, is built becomes fragile indeed and open to question. On the other hand, the citizenry, including disaffected non-voters, could become activated for public oversight, allowing for deeper citizen participation in how intelligence agencies are held to account.

There is evidence of capacity to sustain oversight having been built to different extents in Namibia, Mauritius, Botswana and South Africa, and this capacity includes the technical knowledge needed to engage with official actors on what may be technically complex laws, policies and practices. This capacity is domestically based, with much of it being based in sectors of society that are relatively resource rich, such as NGOs, churches, investigative journalism organisations and editors' associations. South Africa and Mauritius also have traditions of popular organising and mass movements, and remain, relatively speaking, highly mobilised societies, and these traditions of organising provided a social base for anti-surveillance activism. The Mauritian, DRC and South African cases contained

more elements of popular campaigns with broader social bases, but these have proved to be the most difficult to sustain given the resource poor nature of many of the social groups engaged in these campaigns and the difficulties of sustaining social movements in this historical period. These challenges are important to grapple with, as these broad-based campaigns have proved to be highly successful in performing public oversight as they can exercise considerable social power and cannot be marginalised easily.

With regards to failed public oversight, responses to mass surveillance and SIM-card registration in Mozambique and the surveillance of some prominent individuals in Zimbabwe and DRC, and the failure to prevent enactment of part six of the Communications Act in Namibia that provides for the monitoring of communications and SIM-card registration, are some of the standout failures. However, the Namibian government took many years to enact the relevant section, suggesting that they were sensitive to criticism, but not enough to stop the enactment.

The most difficult environments for effective public oversight are Mozambique and Zimbabwe, where no real breakthroughs in reining in digital surveillance abuses, are evident. While many countries show signs of continuities between colonial era surveillance practices involving political policing of the then-liberation movements, continuities are particularly pronounced in these countries. In the case of Zimbabwe, the CIO was literally a colonial invention and was absorbed into the post-independence presidency as is, rather than being shut down and a new intelligence agency being established in its place. As a result, it is hardly surprising that surveillance of dissent remains central to what the CIO does, as that is what it was set up to do. Mozambique's situation is slightly more complicated as it is more difficult to draw straight lines between colonial and post-colonial surveillance practices as the SNASP and SISE were post-colonial institutions. However, post-colonial Mozambique did adopt the lack of intelligence oversight, coupled with excessive centralised control and political policing of dissent, from the colonial Portuguese regime. The ruling parties of these countries also exercise strong control over the levers of society, making it extremely difficult for the public to organise effectively.

In contrast, Angola, which shares a similar colonial history to Mozambique's, is much more unstable, and the ruling MPLA's grip on society is weaker, creating space for more contestation around digital surveillance.

Mozambique faces the added problem of a culture of uncritical citizenship. While this problem is particularly pronounced in Mozambique, it is a problem shared by countries where former liberation movements became governing parties, as they face the risk of these parties overtrading on their liberation credentials, claiming to be the sole and authentic custodians of transformation values and limiting dissenting voices on the basis that they are counter-revolutionary. The fact that Mozambique had transitioned through a civil war and was battling instability in the Cabo Delgado region, also led to a lingering culture of fear coupled with a militarisation of civil functions, including intelligence. The government had little difficulty in justifying this militarisation on the basis that the country could lapse back into full-blown civil war if security institutions failed to maintain heightened vigilance.

With regards to public oversight with mixed outcomes, even the successful cases were episodic, ultimately leading to mixed outcomes in the longer term, where the pressure for reform subsided somewhat once the surveillance scandal died down. Namibian civil society has developed capacity to sustain work on surveillance oversight, but it is difficult to see what significant and lasting democratic gains have been made beyond the legal precedent set by *The Patriot* case. The disintegration of anti-surveillance activism in South Africa meant that the legal victory achieved through the Constitutional Court case was tempered somewhat by a Parliament and government intent on adopting the most conservative interpretation of the judgement possible. International NGOs and the international media have also emerged as strategic and, in some cases, problematic, oversight actors. The Botswana, DRC and Angolan governments have been sensitive to international criticism, and these cases raise complicated questions about who governments take seriously as oversight actors. However, in the case of the international NGO interventions, there is no evidence of them engaging in local capacity building, and it is at the domestic level where public oversight is

likely to be sustained. As a result, once the scandal dies down and they turn their attention elsewhere, local organisations still lack the capacity to continue the oversight (Angola being a case in point). If lasting impacts on oversight are going to be achieved, then international NGOs need to change how they work on surveillance abuses in Southern African countries.

As the case studies show, the domestic capacity needed to sustain public oversight includes the policy capacity needed to understand and engage in areas that may be technically complex: the surveillance potential of Mauritius's smart-ID-card system, Namibia's SIM-card registration or DRC's IMEI registration, for example, require technical knowledge to explain. However, technical knowledge on its own is unlikely to be enough to convince policymakers to depart from unhealthy digital surveillance practices: activists would also need to bring public pressure to bear through direct actions within the confines of what is possible within countries where there are significant democratic limitations. These actions may include organising, public education and meetings, lobbying, picketing and pamphleteering, protests and strikes, to ensure that their arguments are taken seriously. Organising on a more popular basis could avoid the kind of statis that is evident in Angola, but without falling into the trap of over-inclusivity that South African anti-surveillance activists fell into.

It has also proved to be difficult to take up surveillance cases involving individuals, as activists face the challenge of reframing an individual injustice as a collective injustice. This has been easier to achieve in the case of journalists, who can be framed as 'worthy victims' whose surveillance cannot be justified and is likely to indicate a broader attack on media freedom and society's right to know. Surveillance of politicians, on the other hand, such as the ones subjected to surveillance in Zimbabwe, may be more difficult to frame as an injustice in situations where there are already low levels of trust in political institutions and the integrity of politicians. Despite the central role of the media in performing public oversight, as the Botswana case showed, media professionalisation, or the lack of it, can be a significant brake on its ability to perform public oversight that enjoys widespread legitimacy. Media systems may not be struc-

tured in ways that enable public oversight, particularly those with large state and weak private and community ownership and control (Zimbabwe being a case in point). As the Angolan 15+2 case has shown, social media can become an alternative outlet. One possibility is for journalists to collaborate internationally and, in this regard, global collaborative investigative journalism has become a major factor in the media being able to perform successful public oversight by exposing surveillance abuses. This form of journalism is allowing the burden of interpreting leaked documents to be shared across various newsrooms and has spread the risks of official reprisals across various media actors.

Some elements of effective oversight

So, what makes for effective oversight of intelligence-driven surveillance? There are no easy answers to this question, considering what the different chapters in this book, which delve into specific cases of oversight in various contexts, raise. Each chapter raised its own concerns, and every context raises its opportunities and challenges (Van Brakel, 2021). It is also difficult to anticipate changes – especially political – that are likely to take place and that may have a bearing on oversight. For example, changes in surveillance laws often affect how oversight will likely evolve in the future. In some contexts, these changes arise out of legislative initiatives, highlighting the need for constant vigilance and adaptability in the oversight process. An elected parliament may pass a law that (partially) overhauls surveillance and impacts on oversight. In other contexts, surveillance oversight may be midwifed by judicial pronouncements. For example, a higher court may strike down certain surveillance provisions, like what happened in South Africa in 2019 and 2021 (see Duncan in this book), and, in the process, overhaul surveillance oversight practices.

All of the above are realistic possibilities that militate against a one-size-fits-all approach to oversight. Furthermore, the countries researched are different politically. South Africa and Botswana have a tradition of constitutionalism. The same cannot be said about Zimbabwe, however, which actually has a reasonably strong consti-

tutional basis for democratic oversight. Nevertheless, the country has drifted into a hardened authoritarian regime that maintains a façade of democracy (for example, through periodic elections) but dissolves the substance (for example, through prohibiting free and fair elections and maintaining captured and coercive state apparatuses). In the other countries discussed, there is less appreciation of inclusive institution-making. Thus, it is very difficult to say what an effective oversight model would look like. Two issues of agreement are, however, important to highlight. The first one is that every model currently known – judicial, legislative and executive – has strengths and weaknesses. For example, the judicial model may provide independent oversight (McIntyre, 2016), but it can be slow, cumbersome and costly. It can also be captured in (semi-)authoritarian regimes, as Munoriyarwa has demonstrated in this book. Conversely, the executive model may be more agile, but it can be prone to political influence. But, in all the cases we have examined here, there is very little evidence that any of them are working consistently, especially legislative and executive oversight. Increasing both transparency and accountability are the broader objectives of oversight (Butler, 2013; Newell, 2014).

However, public oversight is not guaranteed to be effective in detecting and preventing surveillance abuse, either. The cases we have documented in this book, for example, the DRC Heri Kalemaza case, show that while public oversight can detect arbitrary behaviour and illegal and unconstitutional conduct by surveillance agencies and speak back to these agencies' unfettered powers wherever they are exercised, it can still fail. When exercised, public oversight can still name and shame individuals within institutions who abuse surveillance powers. Where it has been attempted, as in some cases in this book, the objectives of public oversight, while clear, have been narrowly defined. The core objectives of public oversight have been protecting individual and citizens' rights and liberties (Murray et al. 2020) from arbitrary surveillance that lacks transparency and accountability and to protect human rights (Malgieri and De Hert, 2017). Broadly speaking, it means public oversight has consistently attempted to guard against state and surveillance agencies' excesses and hold them accountable for their powers.

Public oversight objectives can and should go beyond these narrow confines, though. Following the South African approach, the objectives of public surveillance oversight can expand (see Duncan's chapter). In South Africa, attempts at public oversight have been more holistic than in other countries whose experiences are chronicled in this book. They have included oversight over intelligence budgets and its (ab)use. Except for the South African case, the several cases that form this book do not often include this kind of oversight. Yet, it can be argued that surveillance agencies can only be as powerful (as well as abusive) as their budget permits them to be. Thus, whatever public oversight might end up being, one of the objectives should include ensuring that surveillance institutions do not waste taxpayers' money and operate functional machinery that serves the public interest within a stipulated budget. The South African and Zimbabwean cases in this book remain stark examples of why the fiduciary oversight responsibility is pertinent to any existing forms of public oversight envisaged. In South Africa, the State SSA agency budget was looted by highly (politically) connected individuals. It became a self-enrichment 'cookie jar' by organised criminal networks that had invaded and paralysed the agency and rogue SSA officials.[1] In Zimbabwe, the CIO budget had on several occasions been reported to be looted[2] by highly (politically connected individuals. The agency had been used to sustain a 'jobs-for-pals' culture where ZANU-PF officials' relatives are hired. Yet, in the cases constituting this book, there is very little evidence that attempts at public oversight in the different countries, except South Africa, have prioritised financial oversight within these intelligence agencies. This mechanism should protect rights and monitor the financial health of intelligence agencies, which is necessary for these agencies' long-term survival and integrity. We underscore the urgency and importance of a holistic public oversight mechanism

1 More details can be found here: https://www.news24.com/news24/investigations/ssa-declassified-i-networks-which-looted-r15bn-from-spy-agency-still-in-place-as-investigations-collapse-20220221.

2 The Zimbabwe case has been investigated and documented here: https://thenewshawks.com/financial-looting-exposed-at-cio/.

that not only protects rights but also monitors the financial health of intelligence agencies, which is necessary for these agencies' long-term survival and integrity.

As we have traced in its different forms of practice in this book, public oversight is a very complicated and ambiguous phenomenon. The term 'oversight' itself means looking over. It does not mean 'touching' as an example (being involved in the day-to-day management of intelligence agencies). By merely 'looking over', there are limited objectives that oversight can achieve. Some may not be easily achieved by 'looking over'. This does not mean to devalue it. It is merely highlighting its potential pitfalls as an alternative to formal intelligence oversight, which may be able to compel remedial action when abuses occur. This raises the second question: what kind of oversight can achieve most of the ideals – protection of individual liberties and privacy, financial oversight of state security agencies, transparency, accountability, as well contributing to more just and equal societies - without being involved in the day-to-day management of intelligence institutions, or without the level of involvement that can easily lead to accusations of interference? This is a very difficult question considering the disparate cases, scenarios, contexts and circumstances of each case study in this book.

Unpacking the key terms in public oversight of intelligence-driven surveillance

In order to move towards identifying a set of theoretical propositions about public oversight and the conditions under which it is likely to succeed, it is necessary to break the terms down into its different concepts, using the insights provided by the chapters, and then move onto the optimal combination of these concepts to achieve effective oversight.

PUBLIC

The different cases in this book show that defining the public is difficult, but there are a few points of convergence. The cases show

that the public is not a neutral and democratic space that everyone has equal access to. It is a space for deliberation and action that is shaped by the deep inequalities persisting in the countries under discussion, leading to a fractured public sphere into multiple publics or even counterpublics (Fraser, 1992, pp. 109–42), which complicates the formation of the publics available to perform oversight. What is clear from the chapters, though, is that publics in the respective countries are constituted by outsiders to the intelligence community and, if there is a sufficiently clear common interest and a well-considered organising strategy and political space execute it, then it is entirely possible to transcend these divisions. Although there has been evidence of whistleblowers stepping forward to report abuses, notably in South Africa and Botswana, unlike the case of Edward Snowden, there is no real evidence in the chapters of ex-spies taking up the cudgels on behalf of the public to fight openly against surveillance abuses. This has meant that these publics lack the deep knowledge that insiders would bring to oversight and, without consistent contact with whistleblowers, they find it difficult to prove the existence of surveillance abuses, and even if they do, to act on this knowledge. Encouraging an environment where sympathetic insiders or former insiders, or spies of principles, step forward and blow the whistle on abusive practices is key, and the factionalised nature of intelligence agencies, even in more authoritarian countries, makes this possible.

Journalists are in a strong position to expose surveillance abuses, as they (except for insiders) are more likely than other sections of the publics to have access to sources in the intelligence community. However, the media is highly uneven across Southern Africa, with a strong state-owned and controlled component and relatively weak commercial and community sectors that may be risk adverse owing to their financial instability. Editors, however, enjoy social capital and can make a big difference when they act collectively against surveillance abuses, as Botswana has showed, or when the media find ways of insulating themselves somewhat from commercial pressures, by operating on a non-profit basis, opening themselves up to more public conceptions of journalism and collaborating internationally to spread the risks of reporting on surveillance abuses.

Global collaborations can also help build more democratic relationships between foreign and domestic media, particularly in former colonial countries, and prevent the kind of demobilisation evident in Angola once the immediate crisis around the 15+2 case died down. These collaborations should aim to ensure that domestic media are taken more seriously by governments, while leveraging domestic political elite's sensitivity to adverse publicity in the former colonies.

With respect to the non-media components of the public, the DRC, Mauritius and South Africa suggest that public interventions are likely to be effective if they have been constituted for a range of other purposes that bring subaltern publics into the public sphere and create space for their voices, and that allows them to relate actual or extant surveillance abuses to broader social ills. In the case of Botswana, Namibia and South Africa, where publics have been constituted in more specialist ways as networks of collaborations that share intelligence accountability and transparency as valency issues, these publics may be too narrow to exercise the social power necessary to make power-holders take them seriously. There is a clear need for civil society actors that specialise in intelligence and surveillance oversight, as the issues, and that may be constituted as NGOs with limited or no memberships. However, they are unlikely to sustain public oversight without more inclusive approach to who the affected public is and how they are constituted already for social action on diverse issues, and that generalises surveillance grievances as being part of broader problems of injustice, oppression and exploitation. As with journalism collaborations, there are clear benefits in forming more democratic international collaborations, to reshape how international organisations work in affected countries and to ensure that their interventions leave local capacity in their wake. However, as the South African case warns, an overinclusive approach towards building public oversight has its own dangers, and care needs to be taken to ensure that collaborations aim to 'get the right people in the right room with the right agenda', which is what the proposed Campaign Action Teams attempted to achieve (Right2Know Campaign 2018: 13).

OVERSIGHT

What are the tools available for public oversight? This, again, depends on the context. However, the first tool available for public oversight is space. Public oversight can utilise available media space, for example, to raise awareness about unwarranted surveillance and, in the process, mobilise communities. As Duncan states in this book, we have seen R2K in South Africa doing this. In the DRC, in South Kivu, Trésor Maheshe Musole notes that '. . . the organisation of civil society is based on the South Kivu Civil Society Charter and the internal regulations. According to Article 1er of the Charter, civil society is understood to be a grouping of structures and associations co-ordinated and organised at different levels of service to protect the vital interests of the population . . .' . Thus, public oversight mechanisms can utilise space to mobilise people and create an enduring narrative against intelligence agencies' abuse.

The Mauritius, DRC and South African case studies have shown that activists who intend to perform public oversight need to pay attention to how they frame the problem of intelligence-driven surveillance. In these cases, framings that tapped into deeper and shared social problems, and made it clear that surveillance exacerbated them, were more likely to be successful than ones that focused on individual wrongs, such as invasions of the right to privacy or violations of media freedom. Mobilisation strategies that allowed for collective responses by publics that may well have been mobilised around other constituencies and issues – for example, the churches in the case of the RAM tax in the DRC, social movements mobilised around issues as diverse as poor housing and unemployment in the case of South Africa, editors in the case of Botswana and political action, village level issues and data protection in the case of Mauritius – were more likely to win demands than those that relegated the problem to specialist groups. Nevertheless, these groups had an important role to play to explain the more technical issues around surveillance to potential publics.

What is also apparent from the successful cases is the diversity of oversight practices used. In more democratic contexts of the region, litigation is another tool for building public oversight, and

strategic litigation especially can ensure that successful cases had more general benefits. Research and documentation ensured that any policy activism, including lobbying formal oversight institutions, governments or political parties, was evidence-based and supported by, at the very least, circumstantial evidence strongly suggestive of surveillance. Investigative journalism and advocacy for the information rights necessary for such journalism also added to the evidence base, with the added advantage that journalists were more likely than other members of the public to have access to sources in the intelligence establishment. In Mauritius, Chiumbu has asserted the importance of the media as a tool used to mobilise CSO actors and pressure groups against the biometrification of IDs. The media was important for awakening dormant networks and mobilising them. However, the utilisation of media space was likely to be successful if it was combined with public education and mobilisation – including picketing and pamphleteering, marches, publicity, production of media, and parliamentary and policy submissions – as these tools helped to engage broader publics beyond specialist NGO communities focusing on privacy, freedom of expression, surveillance, intelligence and/or data protection.

Where do we place parliament in this regard, as supposed elected representatives of the people and that therefore should straddle public oversight and formal oversight? The answer to this question is still not straightforward. This is because, in countries like South Africa, Mauritius and Botswana, robust debates on intelligence oversight have ensued due to an enduring culture of robust deliberative and often agonistic debates in the public sphere, and at times these debates have placed pressure on elected representatives in ways that they could not ignore as they risked losing electoral support. Mauritius, especially, is an excellent example of how surveillance can be turned into an electoral issue when the political opportunity However, parliaments that have been captured by governments or ruling parties have often ignored intelligence agency excesses. This signifies the failure of parliament as a public oversight mechanism. Yet, parliament would, one could expect, have said, 'We are the elected officials who account for the public. We should, therefore, do our job to watch over any institution with the potential to violate

citizens' rights' (Former Opposition Member of Parliament in Zimbabwe, interview in Harare, 3 January 2024). In many instances, this opportunity has been missed. The failure of parliament means the failure of such an important oversight mechanism closely linked to the public.

What are the expectations of public oversight actors? In the previous sections, we have noted these expectations. For example, we have noted that oversight is meant to bring transparency and accountability to a surveillance. We have also added the need to exercise oversight of the intelligence budget, noting that, as Duncan and Munoriyarwa note in this book, failure to exercise oversight of this issue can lead to a 'Frankenstein' type of intelligence institution from which powerful individuals emerge and feed. Intelligence agencies' capabilities are defined by the technologies at their disposal. One purpose of public oversight would be to monitor the trade in surveillance technologies within specific jurisdictions. This is going to be difficult, considering the black-box nature of trade in surveillance technologies. The danger of not exercising such oversight is that some intelligence agencies may acquire technologies that may not necessarily assist with national security intelligence gathering but can be trained against legitimate political opponents at home or communities of practice like journalists. This, in turn, will protect people from arbitrary surveillance practices and the abuse of power by intelligence agencies. In some cases, though, expectations of public oversight actors have moved beyond transparency and accountability and into broader transformational objectives of ending systems of oppression and exploitation that routinely deny basic democratic rights to already socially excluded and exploited publics.

INTELLIGENCE-DRIVEN SURVEILLANCE

However, the chapters have also made it clear that in a situation where more areas of life are being digitised, the potential for digital systems to be used for surveillance purposes has grown. Therefore, what is needed is a form of public oversight that takes the diversity of surveillance practices, or practices with surveillant potential, into

account. The research project on which this edited volume is based focuses on how digitisation has provided intelligence agencies with the capabilities to conduct surveillance on an unprecedented scale, and the role of public oversight in limiting the potential for abuse in circumstances where official oversight may be limited or ineffective. We have adopted this focus for the simple reason that, if misused, then these capabilities can have a massive, direct impact on the lives of citizens through, for example, repression, subversion of democratic processes and so on. At the same time, intelligence mandates have become expansive, covering a range of national security threats and interests, and which has also expanded the scope of surveillance.

As the primary focus is on intelligence-driven digital surveillance – and particularly national security intelligence where the potential for abuse is so high – it has been outside the focus of this project to examine the entire spread of public and private surveillance practices. There is one key aspect of surveillance capitalism that is relevant to this edited volume, though, namely what Shoshana Zuboff has referred to as the elective affinity between public and private missions after the September 11, 2001 terrorist attacks on the US (Zuboff, 2019, p. 116). This elective affinity arose after the attacks – and the intelligence failures that preceded them – because the intelligence community had a vested interest in collecting as much data as possible, ostensibly to prevent further failures. This convergence of interests led to unprecedented collaborations between intelligence agencies and the private sector, and to conditions for what Zuboff refers to, with reference to Giorgio Agamben's states of exception, as surveillance exceptionalism, or a situation where secret public–private intelligence collaborations are stitched together that greatly expand intelligence powers for social control purposes, while making oversight even more difficult than it was. This state of exception played out in Southern Africa too, despite being somewhat removed from the immediate aftermath of September 11, saw governments seizing on the war on terror to expand surveillance powers, although mainly in response to domestic factors.

Unprecedented public–private collaborations have greatly expanded

the capabilities of intelligence agencies to collect, store and analyse data for intelligence purposes. The chapters detail the public–private interface on which so much of the surveillance architecture in Southern Africa rests. For example, SIM-card registration and data exploitation would not be possible without mobile phone cooperation with the state. Data exploitation on a massive scale in South Africa would not have been possible without compelling the involvement of the phone companies that have, on occasion, been critical of this compulsion. In this regard, China has played a key role in providing surveillance capabilities. There is a temptation for intelligence agencies to outsource or privatise more of their functions to evade scrutiny, as access to information rights tend to be weaker in relation to the private actors than the public actors. At the same time and, if pushed far enough, private companies may switch sides and defend consumer privacy if it is in their business interests to do so.

However, there is no real evidence in the chapters of private companies having played a significant public oversight role, despite the potential for them to do so, and neither is there evidence of public oversight having been brought to bear on the private sector when they strengthen unchecked state intelligence power. The fact that this is so, is unsurprising and a not entirely unjustifiable lacuna in public oversight. While these public–private surveillance collaborations have led to more distributed surveillance practices, in the cases under discussion and especially in Mozambique, Zimbabwe, Botswana and Namibia, ultimate control of these practices for intelligence purposes have also been highly centralised in presidencies and the ruling parties that control them. Therefore, oversight has focused on the legislation, policies and government practices enabling or even compelling these collaborations.

Towards a theoretical proposition on public oversight

In an attempt to develop strategies for theory-building from qualitative research, Saldana (2025) has identified six properties of theory, in that it: (1). expresses a patterned relationship between two or more concepts; (2). predicts and manages action through

propositional logic; (3). accounts for parameters of, or variation in, the empirical observations; (4). explains how and/or why something happens by stating its cause(s); (5). suggests generalisability and/or transferability to related social contexts; and (6). provides insights and guidance for improving social life. The above discussion and Saldana's suggestions provides us with the building blocks for the development of a set of theoretical propositions on effective public oversight.

Developing theory is complicated by the fact that such research is difficult to generalise, especially case studies. While the research that informs this edited volume has been designed to enable generalisability through building a comparative element into it, this publication confines itself to the case-study elements. However, some general propositions around successful public oversight can still be put forward, as there are patterns that are observable from the cases. These predictions can be generalised across time and space and thereby provide guidance for actions to learn from positive experiences, while avoiding negative experiences because theory allows people to predict what works and what does not when it comes to social action (Saldana 2025, pg. 2). These propositions can be logically interconnected and culminate in a 'consequently' or 'therefore' deductive statement made by the propositions (Saldana, 2025, p. 45).

The theoretical proposition is as follows: which attempts to incorporate Saldana's six properties as well the properties that must be present for public oversight to succeed, is as follows: if NGO's with specialist knowledge of surveillance conduct public oversight of intelligence-driven surveillance in nominally democratic or weak semi-authoritarian political systems, by collaborating internationally with publicly-driven investigative journalism organisations, while building clearly defined but broad-based local capacity capable of relating surveillance to existing grievances around the oppressive and exploitative root causes of surveillance overreach, and taking advantage of any prevailing crises of democracy and resulting divisions in the political elite around surveillance overreach, then they are more likely to succeed at sustaining public oversight and achieving intelligence accountability than those that don't.

The different elements of this proposition can be explained as follows: public oversight of digital surveillance for intelligence purposes is a poorly acknowledged but important, and at times, decisive factor in the success or failure of oversight as one condition for intelligence accountability. Such oversight can be a highly effective means of calling governments to account for how they use digital surveillance and, in more authoritarian contexts, potentially the only means of doing so. Public oversight is most likely to succeed in political systems with social contracts that have been weakened or made unsustainable by high levels of inequality, coupled with oppression and exploitation, and leading to a widespread suspicion of authority and delegitimisation of state institutions, including intelligence institutions. It is also more likely to succeed in nominally democratic contexts that do not prevent the right to organise, but that lack the political will to facilitate effective formal oversight or meaningful public participation and where intelligence agencies have scope to abuse their surveillance powers, and in semi-authoritarian contexts where surveillance abuses are likely to take place, but where political alignments are unstable, state institutions are weak, and where state oversight is limited in effectiveness or even set up for failure.

Public oversight is least likely to succeed in semi-authoritarian countries which exhibit some democratic trappings, such as regular elections, but where governments exercise strong control over the levers of society, including intelligence. Public oversight is also less likely to succeed in contexts where there is strong continuity between colonial-era surveillance practices and contemporary practices, and where there has been no democratic interregnum where attempts have been made to professionalise intelligence services following a political transition from authoritarianism to one with more democratic promise. In situations where a professional, civilianised intelligence culture has taken root, then it is more likely that whistleblowers may emerge to warn about surveillance abuses, as they are more likely to be aware of the normative values of professional intelligence.

Formal oversight mechanisms, such as ministers, parliamentary committees and ombuds offices, through default or design, typically

lack the resources, powers and even political will to perform oversight effectively. However, of all the formal mechanisms, the judiciary is more likely to exercise independence from the government on national security matters in situations where other official mechanisms fail and intelligence agencies are more likely to respect these decisions, particularly in nominally democratic contexts where the rule of law is more entrenched. Weak authoritarian systems may be pushed to concede demands for redress for surveillance abuses, in conditions where their survival is dependent on external relationships with international actors that are perceived to hold some kind of power over them. In strong authoritarian systems, on the other hand, they may have the opposite effect, strengthening their resolve to resist external interference. Parliaments and elected representatives may be pushed to perform oversight to limit surveillance overreach in moments when they face significant electoral competition and they fear being on the wrong side of public outrage at surveillance abuses, when political opposition commands a significant voice in political life, especially during election periods, when political competition may be heightened, or when international pressure from actors that they fear is brought to bear on them to respond to surveillance abuses, and when they fear international embarrassment.

In terms of mobilisation factors in relation to public oversight and conflict settlement once it has been exercised, collective, organised responses to surveillance overreach are more likely to be effective than individual responses. Collective responses are more likely to be effective if there are divisions in the political elite, to the point where they too fear becoming surveillance targets. These fears may increase the potential for effective public oversight as elite consensus around the need for surveillance may be weaker. The presence of NGOs specialising in issues relating to surveillance, privacy and other data rights, is an important condition for sustained public oversight, as they help to keep a constant focus on surveillance powers and capabilities. They can also play an important role in translating what may be technically complex issues into understandable messages that could be used to mobilise broad sections of society for public oversight. However, their presence alone is not sufficient for effective public oversight. The presence of mass movements supported

by NGOs provides public-oversight actors with the best combination of specialist knowledge to frame digital-surveillance systems or digital systems with surveillance potential, as problems, develop informed strategies to mobilise around these problems and exercise the social power necessary to make power holders take these problems seriously and act on them. These movements do not have to be surveillance- or intelligence-focused, as they can play an important role in generalising grievances about surveillance overreach and relate them to broader societal grievances. International actors, such as international NGOs and investigative journalism organisations, can play an important and at times decisive role in forcing governments to relent on surveillance abuses but, for public oversight to be sustainable, then they need to take the building of local capacity seriously.

Other factors that may affect the success of public oversight may include a tradition of legal activism and strategic litigation in civil society, the presence of strong investigative journalism with a non-profit rather than commercial motive and an orientation towards public and collaborative, rather than competitive, journalism. At the same time, as media workers that often exercise considerable social power and that may have resources at their disposal, editors can play an important collective role in resisting surveillance abuses. The existence of surveillance victims to galvanise public support and build campaigns around, and a widespread and deeply rooted culture of activism, are additional factors and, in this regard, 'worthy victims', such as investigative journalists, are easier to organise around than victims whose occupational profiles may already be the object of suspicion, such as politicians.

Conclusion

As technologies change, actors mutate and interests shift, the question of a foolproof and totally effective oversight model of intelligence remains a far less settled question. Viitanen et al. (2012) have rightly noted how notoriously difficult it will be in the future to settle for an effective oversight model. However, by learning from the expe-

riences discussed in these chapters and what they tell us about how the problem of surveillance overreach has arisen, what has been done about it, its causes and what happens next, it is possible to develop a guide to action that builds on what has worked, while avoiding what hasn't. And that, ultimately, is what research that attempts to engage in theory building that seeks to change the world it observes and documents, should aspire to do.

References

Butler, A. 2013. Standing up to Clapper: How to increase transparency and oversight of FISA surveillance. *New England. Law. Review.* 48, p. 55.

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

Halfdan, L. and Martinez i Coma, F. 2022. The effect of economic downturns on voter turnout in Africa. *Electoral Studies*. 76. [Online]. Available from: https://doi.org/10.1016/j.electstud.2022.102456. 13 May 2024. Accessed 13 May 2024

Fraser, N. 1992. Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy. In: Calhoun, C.J. ed. *Habermas and the Public Sphere*. Cambridge: MIT Press, pp. 109–42.

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

Malgieri, G. and De Hert, P. 2017. European human rights, criminal surveillance, and intelligence surveillance: Towards 'good enough' oversight, preferably but not necessarily by Judges. In: Gray, D. and Henderson, S.E. eds. *Cambridge Handbook of Surveillance Law*. Cambridge: Cambridge University Press, pp. 509–32.

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.

McIntyre, T.J. 2016. Judicial oversight of surveillance: the case of Ireland in comparative perspective. In: Scheinin, M., Krunke, H. and Aksenova, M. eds. *Judges as guardians of constitutionalism and human rights*. Cheltenham: Edward Elgar Publishing, pp. 136–62).

Murray, D., Fussey, P., McGregor, L. and Sunkin, M. 2021. Effective Oversight

of Large-Scale Surveillance Activities: A Human Rights Perspective. *The Journal of National Security Law and Policy*. 11(3), pp. 743–70.

Newell, B.C. 2014. Technopolicing, surveillance and citizen oversight: A neorepublican theory of liberty and information control. *Government Information Quarterly*. 31(3), pp. 421–31.

Right2Know Campaign. 2018. *Second 2018 mid-term review* (report). [Online]. [Accessed 13 May 2024]. Available from: https://www.r2k.org.za/wp-content/uploads/MTR2-2018-report.pdf.

Saldana, J. 2025. *Developing theory through qualitative enquiry*. Los Angeles, California: Sage.

Van Brakel, R. 2021. How to watch the watchers? Democratic oversight of algorithmic police surveillance in Belgium. *Surveillance & Society*. 19(2), pp. 228–40.

Viitanen, P., Patama, P., Rajamäki, J.Y.R.I., Knuutila, J., Ruoslahti, H., Tuohimaa, T. and Tikanmäki, I. 2011. How to create oversight in intelligence surveillance. In: *Proceedings of the 10th WSEAS international conference on communications, electrical & computer engineering, and 9th WSEAS international conference on Applied electromagnetics, wireless and optical communications (ACELAE'11)*. World Scientific and Engineering Academy and Society, pp. 52–6.

Zuboff, S. 2019. *The Age of Surveillance Capitalism*. London: Profile Books.