Algorithmic Coloniality? The Case of Chinese Artificial Intelligence Technology and Zimbabwean Surveillance

L. Travers

Abstract: This paper examines the development and deployment of Chinese Artificial Intelligence (AI) surveillance technology in Zimbabwe through the lens of algorithmic coloniality. Focusing particularly on facial recognition technology, this research primarily draws upon concepts developed by Mohamed et al. (2020) to establish a novel analytical method. It traces questions of *algorithmic oppression*, *algorithmic exploitation*, and *algorithmic dispossession* using data collected through semi-structured interviews and surveys conducted with Zimbabwean experts and desk research. The study reveals that the adoption of Chinese AI surveillance technology in Zimbabwe is driven by the ruling party's aim to consolidate political power using oppressive facial recognition systems. This technology reinforces systems of repression, resulting in the subordination of different social groups including members of the ZANU-PF. Turning from algorithmic oppression to exploitation, ethical concerns arise as Chinese companies establish opaque agreements with the Zimbabwean government, leading to the illicit transfer and misuse of citizen data for their own benefit. The acquisition and extraction of biometric data replicate historical patterns of colonial exploitation, positioning Zimbabwe as a testing ground for Chinese technological advancements. Labour exploitation worsens as Zimbabwean workers face low wages, long hours, and limited agency. Examining policies related to algorithmic dispossession, the paper posits the finding that the importation of Chinese AI technology hampers the development of a thriving domestic AI industry, deepening Zimbabwe's dependence on China. Insufficient legal policies and oversight mechanisms further exacerbate the situation. By employing the concept of *algorithmic coloniality*, this paper provides a comprehensive analysis of the risks, power dynamics, and inequalities associated with Chinese AI surveillance technology in Zimbabwe. Ultimately, it emphasises the importance of responsible and ethical AI development and deployment that protects individual rights and works to remedy existing inequalities.

Introduction

There has been a rising global interest in the dissemination of AI surveillance technology. According to Feldstein (2022), at least ninety-seven countries globally are actively using AI and big data technology for public surveillance purposes within smart city initiatives, or as part of standalone facial recognition systems and smart policing operations (Saheb, 2022).

Recognised as the world leader in the exportation of facial recognition AI technology, China is largely responsible for the proliferation of AI-powered surveillance technology worldwide (Beraja et al., 2023). More specifically, the Chinese companies of Huawei Technologies Co., Ltd. (Huawei), Hangzhou Hikvision Digital Technology Co., Ltd. (Hikvision), and CloudWalk Technology Co. Ltd. (CloudWalk), are significant players in this domination. Notably, Huawei supplies AI surveillance technology to at least 50 nations, surpassing any other organisation (Feldstein, 2019).

The increased prominence of Chinese state-linked technology companies in many African markets has sparked widely reported concerns about the geopolitics of digital surveillance. The dual expansion of the technical means to conduct mass surveillance alongside contractions in democratic space has raised concerns about what Freedom House (2018) has named a descent into 'digital authoritarianism', as well as the possible emergence of 'digital colonialism' (Gravett, 2020). This article aims to ground such a debate in the empirical reality of Zimbabwe.

In the spring of 2018, state-backed CloudWalk of Guangzhou signed a deal with the Zimbabwean government to construct an AI facial recognition system to be used by national security and police forces (Feldstein, 2021). This was a watershed moment; the first time that a Chinese company had entered Africa with an AI surveillance technology (Gallagher, 2019). Whilst the question of Chinese interests on the African continent has long-interested scholars of geopolitics and global power structures, this shift represented a stark movement away from natural resources to data (Polykalova and Meserole, 2019).

The Zimbabwean government's *Smart Zimbabwe 2030 Master Plan* looks to harness the power of technology to transform the country (Ministry of ICT, Postal and Courier Services, 2019). Central to this proposal are smart cities in which surveillance capabilities are essential. The nation's long-standing relationship with China powers these surveillance ambitions through the provision of necessary technology via the companies of Huawei, CloudWalk, and Hikvision. Taken together, the importation of sensors, network infrastructure, and cloud facilities makes the surveillance of Zimbabwean citizens possible.

Rashweat Mukundu, the International Media Support's sub-Saharan Africa advisor, described sophisticated surveillance in Zimbabwe as "a dark spot in which the state has not pronounced its intentions clearly and yet it is secretly growing its capacity" (Ndlela, 2020a). Through interrogating Sino-Zimbabwean surveillance technology relations, it is hoped that this paper will shine light on this dark spot as well as trace the elements of domination embedded within the development and deployment of Chinese AI technology in Zimbabwe.

The central research question this paper seeks to address is:

> To what extent is the case of Chinese AI technology in Zimbabwean surveillance illustrative of algorithmic coloniality?

Effectively interrogating this central question requires an examination of the concepts of algorithmic oppression, algorithmic exploitation, and algorithmic dispossession. These areas will be analysed through an exploration into the effects of the development and deployment of Chinese AI technology on social actors.

It has become critical to "track the ways in which data are generated, curated, and how they permeate and exert power on all manner of forms of life" (Iliadis and Russo, 2016:23). Given the potential for AI surveillance systems to reproduce and perpetuate colonial power structures, biases, and forms of discrimination, it is essential to adopt frameworks that interrogate the institutional politics of data and the top-down effects of surveillance. Such frameworks can help in understanding the landscape of AI development and deployment, as well as the relations that give space to its rollout (Beraldo and Milan, 2019). In line with such an assertion, this paper will critically analyse to what extent the creation, introduction and policies surrounding Chinese AI surveillance technology in Zimbabwe exacerbate existing inequalities or create new forms of domination and control (Layton, 2020).

Background

China's wide-scale domestic deployment of sophisticated surveillance technology has made the nation's framework for ICT integration aspirational (Freedom House, 2022; Ndlela, 2020a). According to reports (Ndlela, 2020b), Zimbabwe is aiming to follow the Chinese model to create a massive surveillance network, "underpinned by the use of artificial intelligence to boost security in cities" (Ndlela, 2020a). As part of this, a senior government official confirmed that the Zimbabwean government was building an "artificial intelligence database" using Chinese technologies (ibid.; Burt, 2018). This has been corroborated by former presidential advisor and ZANU-PF spokesperson Christopher Mutsvangwa, who revealed that Chinese firms were playing an integral role in the *Smart Zimbabwe 2030 Master Plan*, after being approached to "spearhead [an] AI revolution in Zimbabwe" (Sharma, 2020).

The following paragraphs aim to elucidate how Chinese companies are supporting facial recognition initiatives across the layers of sensors, networks, and platforms within Zimbabwe (Hove, 2012; Hawkins, 2018). It should be noted that these outlines are a synthesis of public disclosures regarding facial recognition developments, and that it is highly likely that support from Chinese actors extends to a greater breadth and depth than the following summaries suggest.

Central to the functioning of facial recognition systems is the use of sensors such as surveillance or facial recognition cameras. The Zimbabwean government signed strategic agreements with the Chinese AI technology companies, CloudWalk and Hikvision in 2018, to introduce facial recognition cameras into selected urban and strategic spaces. Both the CloudWalk and Hikvision deals were completed without public consultation or parliamentary approval (AdVox, 2022).

As confirmed by Mutsvangwa, Zimbabwe has received facial recognition sensors from CloudWalk (Masau, 2018). In July 2018, it was reported by South Africa's Daily Maverick newspaper that the Zimbabwean government, through the Zimbabwe Defence Force (ZDF), had reached an agreement with Hikvision - a technology company that is 42% owned by the Chinese government via the Chinese Electronic Technology Company - for the supply of similar technology (Munoriyarwa, 2021). It is understood that the chairman of Hikvision, Zongnian Chen, signed a memorandum of understanding with Mutsvangwa, and the Office of the President released a statement stating that President Mnangagwa and then Chinese Ambassador to Zimbabwe Huang Ping were present.

Using facial recognition cameras with deep learning capacity donated by these companies, Zimbabwean investigative journalist Dumisani Ndlela (2020a) reports that the government has been harvesting data at the country's airports, state facilities, and border points. The cameras were also deployed in the eastern border town of Mutare, where the government launched the city's smart city initiative in January 2020 (Ndlela, 2020b). In addition, for the pilot smart city projects in the cities of Harare and Bulawayo, Hikvision and Huawei have rolled out further facial recognition cameras (Advox, 2023). Further, it was reported in March 2020 that the company had received US$20 million to start the installation of a grid of facial recognition surveillance cameras across the country, with a budget of US$100 million provided over the next five years, although this has been contested by Huawei (Mabaya and Motsi, 2020).

The rollout of facial recognition camera systems depends on reliable internet protocols. Yao Zhiqiang, strategic director of CloudWalk's research and development in Chongqing Municipality, told the Global Times - in a now deleted article - that CloudWalk demanded strong and stable networks as the next step in its cooperation with Zimbabwe (Hongpei, 2018).

> The system vastly depends on internet protocols. It will, therefore, require a very reliable data communication network to function.
>
> *Yao Zhiqianq (ibid.)*

Huawei is reportedly driving the building of backbone infrastructure for the surveillance developments in Zimbabwe (Ndlela, 2020a). According to Albert Yang, managing director of Huawei Zimbabwe, "Huawei is dedicated to being a contributor of providing ICT access to people in Zimbabwe and to the whole continent of Africa, to bridge the digital divide by increasing network coverage and offering affordable devices" (The Financial Gazette, 2016). In 2019, the organisation completed a fibre optic project for state-owned TelOne linking Harare and Bulawayo, the country's two major cities, with South Africa (Dawn-Hiscox, 2017; Ndlela, 2020a).

The transfer of data from sensors using networks results in storage in platforms, also known as data centres. In 2017, two data centres with cloud facilities in Harare and Marzowe for the state-owned TelOne were launched (Ndlela, 2020c). The launch was part of the $98 million National Broadband initiative to upgrade Zimbabwean networks and was implemented by Huawei and funded by a loan from the Export-Import Bank of China (Dawn-Hiscox, 2017).

More controversially, however, is the construction of a National Data Centre (NDC) to which these two data centres are linked. On the 26th of February 2021, President Mnangagwa opened the NDC in Harare. The facility, which is in the process of being linked with databases covering information from key economic players and state institutions including data from surveillance technology, was completed in partnership with the Chinese government (Mudzingwa, 2020; Swinhoe, 2021).

> The establishment of the National Data Centre could not have been achieved without the well-meaning support of our comprehensive strategic partner - the People's Republic of China. Indeed, the government of the People's Republic of China assisted us in the process of appreciating the historic development of ICTs and their customization for use by government.
>
> *Vice President of Zimbabwe, Constantino Chiwenga (ibid.)*

Consultants from Huawei Technologies have reportedly advised the government on digitalising the national registration system for birth and identity documents. This ensures that citizens' details, such as their names, gender, date of birth, identification number, and photos, can be linked with the NDC. Through the ability of the NDC to link this information to sophisticated facial recognition software, easy identification of individuals becomes possible (Ndlela, 2020b).

Whilst the cameras supplied by Hikvision and CloudWalk have the in-built capability of capturing faces, movements, actions and, depending on location, even voices and utterances (Media Policy and Democracy Project [MPDP], 2020), facial recognition is a software functionality that can be implemented within existing systems (such as cameras and image databases) (European Data Protection Board, 2022).

As such, software supplied by companies such as Huawei, Hikvision, and CloudWalk is available to be used in these data centres to facilitate the conversion of public space into private data. Here, computer vision algorithms detect and analyse facial features from images or video footage. These algorithms extract unique facial landmarks, such as the position of the eyes, nose, and mouth, and create a mathematical representation called a face template or face print. These face templates are compared to a database of known faces - such as those from national facial databases - and used to identify individuals in real-time when the network connection allows it (Norman, 2017). Frequently, machine learning algorithms are employed to train the system by providing it with a large dataset of labelled faces. This data allows the system to learn patterns and features that are characteristic of different individuals and improves the system's ability to accurately match and recognise faces.

Taken together, it is clear to see that collaboration between Chinese technology companies and the Zimbabwean state across the domains of sensors, networks, and platforms is rife, and drives the use of facial recognition technology across Zimbabwe.

Research Design and Methodology

This paper is fundamentally about the power surrounding this selected case study: who wins, who loses, and how. As Mohamed et al. (2020) explain, harnessing elements of decolonial theory offers a framework to interrogate the power imbalances in the design, development, and deployment of computational technologies, and interrogate the unequal distribution of risks and economic benefits.

In their paper, *Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence*, they highlight the significance of decolonial thinking in understanding and influencing current developments in AI. Central to their paper is the decolonial approach to coloniality, which interrogates the power dynamics between those advantaged and disadvantaged by processes of dispossession, appropriation, and extraction that were central to the emergence of the modern world (Bhambra, 2020).

Specifically, the authors argue that there is a failure to identify and address the asymmetrical power dynamics that underlie both AI technology and the actors to which it is linked. Citing a number of examples ranging from health care diagnostics to predictive policing, the authors argue that the harms AI technologies can produce with regard to inequality do not emerge by chance. They "result from long-term, systematic mistreatment and inadequate legal and economic protections rooted in the colonial project" (Mohamed et al., 2021). Even though formal colonialism has ended, its negative effects continue through the persistence of its logic, institutions, and practices. Through exploring AI as both object (the application its products and predictions) and as subject (the structure of data, networks and policies that support it), the authors present the argument that structures related to datafication can become sites of domination, and thus sites of coloniality, algorithmic coloniality.

Their novel concept of algorithmic coloniality describes how such domination can feature in the development and deployment of algorithmic technologies. To dissect this phenomenon, the authors introduce the following taxonomy of decolonial foresight to describe its components: *algorithmic oppression*, *algorithmic exploitation*, and *algorithmic dispossession.*

Building on this, this paper aims to use decoloniality as a framework through which power relations between two countries are re-contextualised and further deconstructed to reveal an emerging imbalance. It thus takes forth Mohamed et al.'s (ibid.) work as not simply a theoretical lens, but as a practical tool for structuring and systematically analysing the terrain over which questions of power surrounding computational development and deployment emerge. The adaptation of Mohamed et al.'s (ibid.) three forms of decolonial foresight into an analytical method means that the questions of how power operates in the context of algorithmic technologies can be centred, opening up deeply contemporary avenues to explore and address power imbalances both in the case study at hand as well as in other localities. Indeed, whilst this paper is grounded in the China and Zimbabwe case, this is just one landscape where technology is posited to act as a vehicle for perpetuating inequity.

In sum, the concept of algorithmic coloniality and the constituent components defined below, offer a novel structure to rigorously examine the power centres and peripheries emerging within this case study in a manner that pays particular credence to how such contours may intersect with the logics of colonial practices.

Algorithmic oppression can be defined as the unjust subordination of one social group and the privileging of another through the deployment of AI. This paper will thus, in the first place, explore the impacts of **the deployment** of Chinese AI surveillance technology on various social actors. The first section of analysis will thus answer the question:

> To what extent does the deployment of Chinese AI surveillance technology in Zimbabwe extend the unjust subordination of a social group and the privileging of another?

Algorithmic exploitation and dispossession, on the other hand, surround the structures (data, networks, and policies) that support AI, conceptualising it as subject rather than object. As Mohamed et al. (2020) explain, this development can be divided into two sections: the actual production of AI surveillance technology through the human activities that underpin it, and the wider economic and legal policies that provide space for the development and deployment of AI surveillance technology.

Algorithmic exploitation can be defined as actors and industries involved in AI surveillance technology taking advantage of people by unfair or unethical means, for the asymmetrical benefit of these groups. This paper will thus explore the impacts of **the development** of AI surveillance technology on various social actors, focusing particularly on questions of data exportation and labour. The second section of analysis will thus answer the question:

> To what extent does the development of Chinese AI surveillance technology in Zimbabwe involve actors and industries taking advantage of people by unfair or unethical means, for the asymmetrical benefit of these actors?

Algorithmic dispossession can be defined as the way in which policies related to AI technology result in a centralisation of power, assets, or rights in the hands of a minority and the deprivation of power, assets, or rights from a disempowered majority within AI surveillance technology. This paper will thus explore **the economic and legal policies** that provide space for the rise of Chinese AI surveillance technology in Zimbabwe. The final section of analysis will thus answer the question:

> To what extent do policies related to Chinese AI surveillance technology in Zimbabwe facilitate the centralisation of power, assets, or rights in the hands of a minority and the deprivation of power, assets, or rights from a disempowered majority?

These will be the questions utilised to analyse material collected to interrogate whether the case of Chinese AI surveillance technology in Zimbabwe is emblematic of algorithmic coloniality.

The approach taken to investigate this case study is qualitative, for it allows one to understand phenomena from the perspective of social actors (Babbie and Mouton, 2001). A combination of primary and secondary data was collected to form the foundation for analysis. This involved:

1. **Desk research** Collection of relevant material including legal and policy documents, secondary literature, newspaper reports, and publications on the internet.
2. **Semi-structured Interviews** and **Surveys** Original data has been collected from experts using semi-structured qualitative interviews and surveys. These experts were Zimbabwean professionals working across relevant industries such as academia, human rights law and advocacy, engineering, and artificial intelligence development.

Much of this paper depends on secondary data such as academic texts, newspaper articles, policy papers, and research data on Zimbabwe's surveillance infrastructure. Where possible, locally produced academic texts and reports have been used to root the research in Zimbabwean perspectives. The study thus focused on gathering materials from Zimbabwean investigative journalists and utilized online archives like the Wayback Machine for inaccessible documents. The research also analyzed documents from NGOs, CSOs, and government sources to understand Chinese AI surveillance technology's impact in Zimbabwe.

Table 1: Information regarding informants

Informant	**Profession**	**Involvement**
1	Human Rights Lawyer	Interview (17/2/23)
2	International Relations Researcher	Survey (20/2/23)
3	Data Protection Professional	Survey (1/3/23)
4	Social Justice Advocate	Interview (6/3/23)
5	Smart Technologies Engineer	Survey (6/3/23)
6	Media and Surveillance Researcher	Interview (11/3/23)
7	Human Rights Professional	Survey (16/3/23)
8	Human and Digital Rights Advocate	Interview (20/3/23)
9	Innovation Engineer	Interview (21/3/23)
10	Machine Learning Professional	Interview (22/3/23)

Noting the sensitive nature of this topic and potential issues with data interception, comprehensive consideration was given to protect informants. To protect informants due to potential data risks, encrypted communication platforms were used. Informants were informed about the research purpose and assured they could withdraw their responses if the study was published. While many chose not to be anonymous, some emphasized the need for confidentiality due to potential monitoring. To maintain anonymity, each informant was assigned a number, but their general professional domain was disclosed for context.

The data was manually coded for thoroughness with coding done in two cycles, initially focusing on three areas: AI surveillance technology deployment, development, and related policies in Zimbabwe. The second cycle grouped related content, revealing patterns used to answer research questions. These patterns were supplemented by documents from desk research, with a focus on power dynamics and potential future impacts of AI technology (Saldaña, 2021).

Analysis and Interpretation

Deployment: Analysing Algorithmic Oppression

To what extent does the deployment of Chinese AI surveillance technology in Zimbabwe extend the unjust subordination of a social group and the privileging of another?

Motivations: The Drive for Datafication

Emerging strongly from both the desk research and comments from informants is a marked political desire for the ruling Zimbabwean government to deploy sophisticated systems of public space surveillance. As Informant 9 remarked, "knowing our government and how they like to control people, the need to maintain power is driving the deployment of these systems".

As Informant 1 revealed, "[the Zimbabwean government] have long wanted to perfect the infrastructure of surveillance", and the importation of sophisticated systems marks a strong step in this direction. The use of facial recognition systems speaks directly to the "need of the [political elite] to hold on to power and to keep citizens, especially dissenting voices, in check" (Informant 7). While the particularities of how this is made possible will be outlined shortly, it is clear from conversations with informants that the central motivation for surveillance is to pre-empt opposition-induced civil unrest by gathering data on opposition leaders and other opponents and taking proactive actions such as making arrests and disrupting plans using knowledge of citizen movement.

One further possible understanding for the new impetus in this acquisition of surveillance technology can be traced to the growing involvement of security forces in Zimbabwe's governance. Indeed, it has been theorised that diplomatic and strategic exchanges between the CCP and the ZANU-PF have led to the latter's governance approach becoming more aligned with that of the former, particularly in terms of the increasing role of the ZDF in party decision-making.

Within the context of Zimbabwe, the military's role in President Mnangagwa's ascent to power and toppling of Robert Mugabe resulted in the removal of constitutional order and an increased prominence in intelligence gathering (Noyes, 2020). Indeed, the removal of Mugabe from office emphasised the military's importance in Zimbabwean politics and their dominance in decision-making, with those generals who staged the coup assuming both administrative and political power. In this way, the ruling party's survival is linked to the use of military-driven digital surveillance that seeks to prevent the very coups that they benefitted from (Rupiya, 2013).

This understanding strongly diverges from one of the key stated goals behind the creation of smart city projects and the implementation of AI surveillance technology: safety.

> Every time the government has commented on the use of new surveillance tools in Zimbabwe, the justification has been for the prevention of crime and maintenance of law and order.
>
> *Informant 3*

From an analysis of the geographic deployment of facial recognition surveillance cameras, a misalignment between the locations of deployment and areas with high crime rates strongly emerges. In those areas where facial recognition cameras have been deployed - such as in the city centres of Bulawayo and Harare - crime rates were not statistically more pronounced than other areas of the nation at the time of their introduction (Munoriyarwa, 2021).

According to Informant 1, in those areas where crime is at an elevated and serious magnitude, the level of illegal activity is at a point where there is a “need to deploy actual boots on the ground” rather than relying on a digital network of cameras. Furthermore, in these locations, “the cold underlining infrastructure that is required” such as the power supply and internet connection needed to facilitate the use of these technologies, is lacking. Thus, the claim that these cameras are solely for preventing crime are hollowed when we consider the lack of targeting of those geographies that are most affected.

Furthermore, according to Zimbabwean court records, there has not been one public conviction of a criminal based on these cameras even though they have been installed for a number of years (MPDP, 2020). This fact, in combination with insights from informants, strongly points to the deployment of AI surveillance for authoritarian purposes.

Capabilities: Facial Recognition Cameras and Digital Authoritarianism

For informants, the central actor who has subsequently emerged as the ‘winner’ from the deployment of Hikvision and CloudWalk sensors has been the Zimbabwean government who use facial recognition cameras for purposes that range from directly profiling and targeting members of opposition parties, to establishing threats to the wider public in order to maintain the status quo.

In the first place, these sensors allow for the ZANU-PF party to specifically target individuals and selected groups. A number of the categories of externally surveilled groups developed by Munoriyarwa (2021) were corroborated by informants. These covered opposition party members, civil society leaders, and citizens who use social media for political expression. In the case of the former, Informant 6 revealed that “the whole surveillance practice is no longer tailored at legitimate targets like foreign enemies ... but it’s targeted at opposition leaders who might actually push ZANU-PF out of power”. Turning to the surveillance of NGOs and CSOs, a number of informants testified that they themselves had been targets of either communication interception, or warnings that the state was watching them. Such a reality falls in line with the narrative the Zimbabwean regime has pushed that diabolizes civil society actors as regime change agents (ibid., Sachikonye, 2011).

The analytical aspects of facial recognition technology facilitate a reverse search capability, allowing users to conduct searches based on facial images or specific parameters such as name, biometric data, or time. Furthermore, the system offers advanced search functionality, enabling users to obtain information regarding the whereabouts of individuals of interest within a designated time period, their interactions with others, and the duration of their presence at specific addresses. These parameters can also serve as triggers for notifications, wherein the system promptly alerts users upon the detection of a chosen parameter, such as a specific individual. It is this capability that facilitates the targeting of certain individuals (Dauvergne, 2022).

The purpose of collecting and analysing information about the population in the context of surveillance is driven by the desire of repressive administrations to govern people's activities (Haggerty and Ericson, 2006). Within Zimbabwe, the ability to influence citizen behaviour and reduce the possibility of dissent operates through two distinct mechanisms.

The first is *direct action.* The deployment of facial recognition cameras in the country means that Mnangagwa's regime can quickly identify those individuals and groups who are thought to pose a risk to his political establishment (Woodhams, 2019). This is done through the use of algorithms to compare the data points captured by sensors to those stored in data centre files. With this information, a sophisticated understanding of the movement and activities of those individuals that pose a threat to the status quo is built, and activities to curtail their actions are implemented.

In 2019 alone, 49 cases of abductions and torture were reported in Zimbabwe without investigations leading to perpetrators being held to account (Office of the United Nations High Commissioner for Human Rights [OHCHR], 2020). One of the most high-profile of these occurred in May 2020 after three female opposition activists - Member of Parliament (MP) Joanna Mamombe, and activists Cecilia Chimbiri and Netsai Marova - were arrested for attending a peaceful protest organised by the Alliance Youth Assembly of the main opposition party, Movement for Democratic Change (ibid.). On the same day, they were forcibly disappeared from police custody, and sexually assaulted and tortured during their abduction reportedly by state security personnel (Amnesty International, 2020). After being released, the trio were further charged with violating COVID-19 regulations on public gatherings and for purportedly intending to promote public violence. The women have even been accused by ZANU-PF politicians such as the then Zimbabwean Deputy Information Minister, Energy Mutodi, of "stage-managing" the abduction and attacks in order to oust the ruling ZANU-PF government (Dube, 2020). This type of direct military-driven digital surveillance "is the major weapon in the arsenal of the ruling party for forestalling civil unrest and dissent" (Munoriyarwa, 2022:467). The use of such technology to collect information means that the government has "an advantage over dissenting voices, [and] this may lead to authoritarianism" (Informant 7).

This advantage, however, does not always need to be palpable for it to be influential. As Gravett (2020:8) explains, facial recognition technology "can fundamentally change the relationship between people and the police, and even alter the very meaning of public space". In this way, opponents to the ZANU-PF regime are immobilised by *indirect action* and the mere threat of being monitored in their activities, particularly when individuals recall the experiences of Mamombe, Chimbiri, and Marova.

The degree to which these sophisticated surveillance networks are operational is subject to conflicting reports. Despite this, the government has been keen to promote the idea that it is all seeing, and the aforementioned example involving opposition MP Joana Mamombe and activists

Cecilia Chimbiri and Netsai Marova is testament to this ambition. President Mnangagwa refuted their claims of abduction and justified such a position by maintaining that the government "was able to trace where they walked, slept and who they talked to" (Ndoro, 2020). The irony of this disclosure is obvious. The very existence of a sophisticated network of surveillance and hence the ability to monitor movement has been cited by the president as reasons why the abductions were not possible, when, in reality, it is beyond all likelihood that this very network was harnessed to target the opposition members. More significantly, Nompilo Simanje of the Media Institute of Southern Africa Zimbabwe has asserted that Mnangagwa's claims are "a clear example that the government has the necessary tools and the capacity to monitor people" (Hawkins, 2022). The impacts of this possibility contribute to the chilling effect outlined in detail in the section below.

Consequences: The Emergence of the 'Chilling Effect'

Although some informants cited the potential benefits of transparently introducing facial recognition technology for "combatting crime and bringing perpetrators to book" (Informant 2) as well as "making communities safer" (Informant 4), the dominant theme identified from the interviews and surveys was a chilling effect that involves the deterrence of people from exercising their freedoms because of state surveillance.

> The losers [from the deployment of AI surveillance technology] are the targeted people who are unable to exercise their fundamental rights out of a fear of being surveilled by state security agents working to promote the ruling party's interests. The use of these technologies chills the enjoyment of fundamental rights which are key to the building and maintenance of democratic processes, for example, the right to free expression, information rights, the right to privacy and the rights of freedom of assembly and association.
>
> *Informant 3*

Numerous reports illustrate the shrinking civic space that exists in Zimbabwe (OHCHR, 2023; Karekwaivanane and Msonza, 2021). Almost all informants of this paper pointed out the potential or material effects of the deployment of the government's Chinese AI surveillance technology for discouraging activists and opponents from mobilising against the state.

> One of the ministers was saying, look, be careful how you criticise our president because we will visit your bedrooms.
>
> *Informant 1*

In this way, it becomes clear that surveillance is becoming the selected mechanism for silencing critical voices (Lyon, 2001). The cost of action for civil society and opposition members increases because of surveillance and has led to the ongoing decline of organisations and movements in opposition to the state and a move toward more fragmented forms of resistance (Tarrow, 1998; Davenport, 2005).

As such, the proliferation of sophisticated surveillance technologies is a potent tool for policing and subsequently streamlining the ZANU-PF's regime of truth. Such a regime of truth is strengthened by the power-knowledge dynamic implicit within systems of AI surveillance; with citizens turned into objects of power whilst new knowledge is simultaneously created about them (Foucault, 1980). Simply put, these surveillance systems are designed to render citizens and their behaviour more legible, within the orbit of the state. In line with the work of James S. Scott, it can be noted that “legibility is a condition for manipulation” which nullifies the resistance of opposition members (Scott, 1998:183).

Beyond working to prevent opposition party members from protesting or organising, the roll-out of these sensors also impedes the privacy of the ‘normal’ citizen.

As the complete picture of active facial recognition cameras is not publicly disclosed, citizens are unaware whether these may be operating in only strategic locations or all-over urban areas. According to informants, those citizens with even a basic awareness of the roll-out of Chinese AI surveillance technology, tend to assume the latter. In this way, we see a type of presupposed liquid surveillance emerge, a supposition that dynamic and pervasive surveillance is being undertaken despite ambiguity over whether or not this may be happening. As Informant 1 aptly points out, “the net effect of all this surveillance infrastructure is not whether you prove its existence or otherwise, but whether it’s contributing to a chilling of the environment, in political participation because everyone thinks, okay, if I’m being watched, why should I bother?” This revelation is supported by Informant 4, who asserts that it’s “not secure for one to enjoy their privacy because you don’t know who is following, you don’t know what is happening.”

These behavioural effects - namely immobilisation - fall in line with the words of Greenwald (2014:177) that “mass surveillance kills dissent in a deeper and more important place as well: in the mind”, and that these systems of AI surveillance force citizens to interiorise new rules regarding how they occupy and engage with public space (Cabestan, 2020). A strong trend emerging across responses from informants surrounds the impossibility of overcoming this phenomenon. The entrenchment of such a chilling effect, and by extension digital authoritarianism, is extended by two primary mechanisms. For those actors working to expose the practices of the Zimbabwean government - a number of whom have contributed to this paper - there are significant difficulties in obtaining a comprehensive picture of the deployment of Chinese AI surveillance technology.

> There’s no clarity in terms of the procurement processes, number one, and number two, there is no clarity with regards to the specific purpose for which that technology is being deployed. As a result, human rights defenders run the risk of being surveilled.
>
> *Informant 8*

> We only receive information from these investigative journalists who sometimes leak information. Otherwise, it’s all secrets and secrets. The press is only given an overview, but not the actual details.
>
> *Informant 9*

By extension, the public faces the same issues in terms of acquiring accurate information. As Informant 8 - a human and digital rights advocate - explained, there is no level of consultation with local people with regard to surveillance developments in public spaces.

> The information gap is most concerning. When you are deploying any smart city initiative, at the top of the list should be making sure that you consult all the relevant groups including those who are likely to suffer from discrimination or to be marginalised because of certain technologies or those who are at risk of certain kind of violations so that they are part of this conversation before rolling out any use of smart city initiatives.
>
> *Informant 8*

When individuals do receive information, either through the media or community channels, it is often conflicting. As an international relations researcher revealed:

> Some may say Zimbabwe is attempting to build a surveillance state while others may say they are trying to keep everyone safe.
>
> *Informant 2*

These conflicting sources of information are compounded by a lack of knowledge regarding surveillance technology.

> The rolling out of such technologies coupled with sometimes a low level of literacy sort of muzzles the general public and those people who actually don't have a voice.
>
> *Informant 8*

> There is not yet knowledge about it; awareness has not yet percolated to the grassroots. So that is one the saddest parts of surveillance, we still need to mobilise people to understand its implications, to understand that when one is surveilled, the danger lies to everyone, not only to an elite.
>
> *Informant 6*

Taken together, challenges in accessing information, filtering this research into fact or falsehood, and then integrating these new findings into an existing knowledge about surveillance systems that may not be sufficient, explain how a large information gap in Zimbabwe has grown. Consequently, the opposition to the implementation of facial recognition infrastructure remains subdued because only a small fraction of the population is aware of its widespread deployment and the associated risks it poses.

With the deployment of technology established through public-private partnerships with Hikvision and CloudWalk, there is no independent body available for citizens to report their concerns regarding the use of facial recognition systems in public spaces. According to a Zimbabwean data protection expert, Informant 3, this means "people do not know where to submit data protection related complaints". When complaints are voiced to journalists, the results are rarely published. Not only do the leading outlets in Zimbabwe have links to the ruling party (Tshabangu and Salawu, 2022), but the government also owns and controls approximately 60% of the nation's newspapers, radio, television, printing, and online platforms (Media Monitors, 2020). For those outlets existing outside of this nexus, the threat of being muted or targeted by the state makes it difficult for them to challenge state narratives, bear witness, and represent the public interest, particularly when the safety of their sources cannot be guaranteed (York, 2014).

As Informant 1 remarks, this disjuncture between the ability of the state to access security technologies and for citizens to resist these developments "continues from the colonial era", with Zimbabwean citizens "at no point ... having sufficient oversight on security arms of the state and their operations." In the context of Zimbabwe, under colonial rule the British employed surveillance methods to monitor the activities of the indigenous population, particularly those who were seen as potential threats to colonial rule. After gaining independence in 1980, the ZANU-PF government, led by Robert Mugabe, inherited this legacy of surveillance and established institutions such as the Central Intelligence Organization and the Joint Operations Command, which were responsible for intelligence gathering and maintaining internal security. These agencies employed surveillance tactics to monitor political opponents, activists, and journalists critical of the government. As has been explored in this chapter, surveillance practices in Zimbabwe have continued under the current administration, evolving alongside complex shifts in power, culture, and the political economy, to absorb further targets including human rights lawyers and social activists (Munoriyarwa and Chiumbu, 2022).

Caveats: Surveillance as a Double-Edged Sword

Whilst a clear picture emerges of digital authoritarian practices enacted against dissenters and the public at large, it is inaccurate to assess this pattern as simply unidirectional.

> I want to call it fractionalisation, or factionalism. Within the military and the ruling party itself, there has been a lot of dissenters, elite dissenters in the party since the fall of Robert Mugabe. So, the whole idea is now surveillance is a double-edged sword, one tailored against opposition of ZANU-PF, but also against opposition within the ZANU-PF, opposition to the ruling clique within ZANU-PF. So that's why you'll find that as much as the state might be surveilling on the opposition, it is also the same technologies used to surveil against opponents within the ruling party itself, those who might institute a coup against the current system.
>
> *Informant 6*

As such, there is seemingly a 'surveillance paradox' at play (Munoriyarwa, 2022). That is, whilst these surveillance practices primarily benefit the ruling party, the ZANU-PF's escalating political fragmentation has led to some individuals becoming targets of the very same strategies initially designed to serve their interests. In the Zimbabwean context, there is an observed levelling effect, whereby surveillance is in some cases extended to internal groups (Haggerty and Ericson, 2000). At the heart of the deployment of surveillance technologies in Zimbabwe is thus a steadfast political allegiance to ZANU-PF, which takes precedence over any practical concerns, as it ensures the party's continued existence. This argument is corroborated in the literature, with Munoriyarwa and Mare (2022) citing that surveillance activity is driven by the desire to ensure that power remains within ZANU-PF rather than being transferred to other institutions in Zimbabwe.

Development: Analysing Algorithmic Exploitation

To what extent does the development of Chinese AI surveillance technology in Zimbabwe involve actors and industries taking advantage of people by unfair or unethical means, for the asymmetrical benefit of these actors?

Data Exportation: CloudWalk and Beta-Testing

As Mohamed et al. (2020) explain, the development of AI systems frequently involves the testing of technology by companies in countries outside of their own due to the lack of regulations and safeguards around data use in these 'testing grounds'. Each informant was questioned regarding what happens to the data accumulated by sophisticated facial recognition systems in Zimbabwe. Once a face is detected and travels between sensors and data centres, who might have access to it?

In the first place, a number of informants cited the marked difficulty in acquiring information regarding which actors have access to data collected by facial recognition cameras across the urban landscape.

> [The general public] actually don't know what happens with that information when it's been collected or whatever happens with the government.
>
> *Informant 8*

Such opacity is compounded by the fact that the line between the military and the ZANU-PF party is hard to distinguish. These assertions support the findings of MPDP (2019), who reveal that it is often not clear who harvests the data collected by cameras, with claims of joint ownership between city councils and security forces. However, it is in this clandestineness that space is provided for the illicit transfer of data beyond those that citizens are aware of.

> The opacity of these agreements allows these [Chinese AI] companies to move data back and forth. And we don't have very clear or strong regulations around, you know, transfer of personal data. And of course, we now have the data protection act that talks about that, you know, that if you want to be moving data out of the country, but it's highly unlikely that it would be enforced against China. They will not reinforce it against China.
>
> *Informant 1*

The legal loopholes that permit the possibility of this reality are detailed at length in the next section.

Despite this cloud of ambiguity, it has been revealed through a combination of leaks and now deleted Chinese newspaper articles, that the public-private partnership signed with CloudWalk in May 2018 has involved the Zimbabwean government turning over data to the organisation (Jie, 2018). Whilst there is ambiguity over the current status of the CloudWalk agreement - Musodza et al. (2022) suggest that the arrangement stalled after the Zimbabwean government asked the company for a discount - it has been confirmed in domestic and international media that the Zimbabwean government has turned over huge amounts of biometric data to the Chinese firm (Ndlela, 2022; MISA Zimbabwe, 2019; Hawkins, 2018).

This paper also owes a debt of gratitude to Informants 3 and 6 who alerted to this particular development.

> China is actually making use of that data to sharpen their surveillance technologies. It has been speculation, but there is now evidence coming out that [CloudWalk] use this data, to train their technology on black skins, to sharpen it.
>
> *Informant 6*

> The export of facial recognition technology gives the Chinese an opportunity to collect useful biometric data which can be used to train future AI technologies. For example, when the Zimbabwean government approached CloudWalk to acquire facial recognition technologies, part of the deal was that Zimbabwe would turn over biometric data to the Chinese company for purposes of training its AI and machine learning platforms which were usually trained on data that did not include African biometric data.
>
> *Informant 3*

The terms of the agreement signed between CloudWalk and Zimbabwe required the Zimbabwean government to send collected biometric data to the former's Chinese offices (Okolo et al., 2023; Andersen, 2020). It is this condition that has allowed Zimbabwean leaders to access "technology and tools that they would never be able to afford on the open market if they didn't have a currency other than the data of their own people to leverage against that" (Hawkins, 2018).

A MISA Zimbabwe (2019) letter to the UN Special Rapporteur report revealed that this agreement is particularly valuable to CloudWalk as it allows the company to read and differentiate between African faces through the acquisition of huge amounts of biometric data. Such datasets are important because facial recognition software today largely struggles with differentiating faces that are not white since existing AI facial recognition technologies are principally trained on white and East Asian datasets (Okolo et al., 2023).

In a now deleted article from China's Global Times outlet, Yao Zhiqiang, strategic director of CloudWalk's research and development centre in Chongqing Municipality, revealed that to make a breakthrough in facial recognition technology, deep learning was being used to exploit the data supplied by Zimbabwe.

> The differences between technologies tailored to an Asian face and those to a black one are relatively large, not only in terms of colour, but also facial bones and features.
>
> *Yao Zhiqiang (Hongpei, 2018)*

In a written statement submitted to the House Committee on Oversight and Government Reform, Cook (2018) elucidated that by utilising datasets containing millions of sub-Saharan African faces, Chinese developers were able to rectify widespread, race-related software inaccuracies. Noting that Zimbabwe has absorbed migration flows from across sub-Saharan Africa, the Zimbabwean case represents a particularly rich data set (Okolo et al., 2023). For CloudWalk, this development provides an opportunity to gain a significant market advantage over their competitors. This subsequent technological capability, when implemented in predominantly black populations such as Zimbabwe, provides an algorithmic advantage over American and European developers (Sharma, 2020).

Although present cases of data exportation at the hands of Hikvision and Huawei organisations are unclear, its fruition looks increasingly possible with "the Zimbabwean government largely strapped for cash and the Chinese ready to take advantage of this. Unless the government owns full rights to the data, this may yet be another avenue of manipulation" (Informant 2). For data protection professional Informant 3, any data collected by facial recognition cameras "is likely to be exported to China or accessible to the manufacturers of facial recognition technology."

Labour Importation: Workplace Relations and Displacement Effects

As much as one might situate the development of AI within an imagination detached from human influence, AI is neither artificial nor intelligent but rather a product of planetary properties, concepts, and entities including physical and intellectual labour (Crawford, 2021). Advancements in AI depend to a large extent on the material labour of workers to either label or annotate large volumes of data or oversee the maintenance and construction of relevant infrastructure that is situated in the built environment (Gray and Suri, 2019). This section will thus trace the interplay of labour and Chinese facial recognition technology in Zimbabwe.

Informant 6 revealed that he knew of "many incidents that have happened in Zimbabwe where people who work in Chinese companies have not been paid for a long time. Sometimes they work ... for months, they get dismissed without receiving their salaries and wages ... spare a thought for the workers who are involved in the assembling of the technology, the harvesting of the data and processing of it. They suffer from low wages, long working hours, and more importantly, sometimes they walk away without even their wages."

Despite protestations from the Chinese Ambassador to Zimbabwe, Guo Shaochun, over accusations that Chinese companies mistreat workers in Zimbabwe (Masau, 2022), a number of informants spoke directly to contradict this assertion.

> The Chinese [companies] are not transparent in their activities and ... people who have worked in these industries say that the Chinese are harsh in their working conditions to the extent that there is little time to rest and there are language barriers since the Chinese don't prefer to learn the local language but prefer you to learn theirs or working with an interpreter.
>
> *Informant 5*

Such insight has been bolstered by Informant 7 who confirms that "at Chinese owned companies, there are reports of rampant human rights and labour abuses". This has been to such an extent that the human rights professional has himself received numerous reports from workers and confirmed that some cases of 'labour exploitation' have even spilled over into the courts. These cases, however, tend to be a rarity. "The lack of formal structures for registering complaints [means] it is only those extraordinary moments that are captured on camera ... when the government pretends to act" (Informant 6). The result is that "fairness is closed against these workers", as is their agency to situate themselves in the ecosystem in which they form the foundations (ibid.)

Further instances of exploitation within AI development emerge when we consider the possible displacement effects for Zimbabwean employment. Although questions of economic dependency will be addressed in the following section, it is worth noting here the impact of importing qualified labour on trained citizens.

> These [digital] workers are also supervised by the Chinese. China brings their own labour, especially at managerial level - they don't take on locals, they bring their own labour. Zimbabwean universities are producing IT gurus. Have you ever thought where they will exercise their abilities to also to start their own stuff, technologies if they cannot even benefit from the local market? That's the idea here. So, it's not like the Chinese are assembling their technology in Zimbabwe and creating jobs ... that's another form of exploitation.
>
> *Informant 6*

In this way then, actors such as CloudWalk take advantage of not only the facial data they are able to extract without consent, but also, to albeit to a lesser extent, Zimbabwean labour to accelerate their own development to the detriment of the local ecosystem.

Policies: Analysing Algorithmic Dispossession

To what extent do policies related to Chinese AI surveillance technology in Zimbabwe facilitate the centralisation of power, assets, or rights in the hands of a minority and the deprivation of power, assets, or rights from a disempowered majority?

Economic Policies: Dependency and Agency

The exportation of Chinese technology to the Zimbabwean government is based on a bank-led business cycle that has been extended across the continent. Chinese financial institutions provide loans to African administrations, enabling them to acquire advanced surveillance technology from corporations within China (Hemmings, 2020; Hawkins, 2022).

> Loans from China are usually given as economic rather than concessional terms as such the nature of Zimbabwe's relations with China is most likely going to perpetuate a vicious cycle of economic dependency.
>
> *Informant 2*

> The acquisition of AI surveillance and telecommunications equipment from China is based on the extension of credit lines to Zimbabwe which keeps the country economically dependent on China until such debts are paid.
>
> *Informant 3*

The result of such predatory lending is an extension of the patterns of dependency that emerged during the Chinese scramble for Zimbabwean mineral wealth (Birhane, 2020). Framed within China's 'non-interference policy', these loans are justified from the Chinese perspective under a discourse that stresses non-interference, framing these developments as neutral and non-political projects (Aidoo and Hess, 2015). An examination of this 'debt-trap' diplomacy, however, negates the view that these interventions are purely project-based, technical business, negotiated bilaterally at eye level (Al-Fadhat and Prasetio, 2022).

Indeed, anthropological scholarship has illustrated how reliance on external finance extends the power that multinational organisations - and by extension the states they are attached to - hold over regions (Ferguson, 2006; Sanusi, 2011; Du Toit, 2017). The accumulation of significant debt by Zimbabwe to finance imports of Chinese facial recognition technology creates economic dependence on China, as a considerable portion of Zimbabwe's economic activity becomes tied to repaying those loans and honouring trade obligations.

Although the exact volume of Chinese external debt has been contested in the Zimbabwean Parliament (The Zimbabwe Mail, 2022), most estimates have it at least above the US$ 1 billion mark. Furthermore, the Zimbabwe Coalition on Debt and Development (2020) has revealed that the ZDF has significant amounts of undisclosed debt to China. Through these technology companies and the economic arrangement that facilitates their penetration in Zimbabwe (which also includes loans from Chinese state banks to domestic technology companies), China is able to position itself as an indispensable economic force in the region. In addition, the import of Chinese facial recognition technology necessitates ongoing maintenance, support, and updates, concretising China's involvement in Zimbabwe's technological systems and stifles local industry.

Regarding the latter point, Informant 10, a machine learning professional, disclosed that domestic AI development within Zimbabwe is "still at its infancy stage". The question that subsequently arises is what the implications are for this industry as reliance on Chinese companies grows. The previous section has already illustrated Chinese patterns of importing skilled labour, with the result that "[the Chinese] do not impart the skills to Zimbabweans to empower them to develop their own AI resources" (Informant 2). In this way, "Zimbabwe's own development trajectory for AI resources is being pre-empted ... Zimbabwe will just be a consumer of Chinese goods" (Informant 7)

> It is just like the old colonialism led by the British and Europeans, it extends old forms of colonialism and dependency because what it means now is the technology industry of Zimbabwe cannot grow because it is it is under the shoulders and heavily put into oblivion by Chinese data companies. The importing of these technologies means that we forever depend on the Chinese technology because we cannot give room to our own entrepreneurs to start their own companies to drive the technological development of the country.
>
> *Informant 6*

Evidence is mounting that such arrangements ensure the persistence of Zimbabwean dependence on Chinese technology for economic prosperity, but also for policy formation (Feldstein, 2019; Dahir, 2019; Elmi, 2020). With policymakers increasingly reliant upon the information that facial recognition technology provides for infrastructure, transport, and security solutions, the roll-out of smart city initiatives across the nation may further entrench dependence on Chinese technologies. As Lee (2017) points out, unless developing countries "wish to plunge their people into poverty, they will be forced to negotiate with whichever country supplies most of their AI software—China or the United States—to essentially become that country's economic dependent".

All the while, these Chinese technology firms - such as CloudWalk - leverage the data amassed from the private citizens of Africa, including facial information, to enhance their artificial intelligence-based facial recognition systems, whilst "[making] a lot of money out of selling their technology" (Informant 6) in a "market with serious demands their products" (Informant 7). Subsequently, the refined or updated facial recognition technology can be marketed to African governments as an improvement or substitute for their existing systems. Under the guise of seemingly mutualistic economic relations, the nation is able to position itself favourably to accumulate data to pull further ahead in the race for AI dominance.

Despite a landscape indicative of dependency, reports have emerged that the Zimbabwean state granted Huawei significant income tax exemptions. According to a 2019 Zimbabwean Government Gazette:

> With effect from the 25th [of] August 2014, the receipts and accruals of Huawei Technologies Co ... are approved ... as being exempt from income tax on any receipts and accruals.
>
> *Government of Zimbabwe (2019)*

This was then backdated to 2009, resulting in the repayment of income tax to Huawei between 2009 and 2014 under Statutory Instrument 25 of 2020 (Karombo, 2020). Such a disclosure reveals the desire of the ruling party to maintain favourable relations with its Chinese counterparts. Noting the fact that international and domestic media outlets have raised questions on the topic of the Zimbabwean government's dealing with Chinese banks and technology companies, it is important to further unpack why these engagements persist despite the structural dependencies outlined above.

Contextually, the Zimbabwean economy is facing a weakening currency, hyperinflation, and plummeting living standards (Muronzi, 2022). As a way to ensure the penetration of their AI dragons, the Chinese government, its banks, and telecommunication companies have built infrastructure and are investing across the Zimbabwean economy.

Between 2019 and 2022, China has invested over $2 billion in Zimbabwe and is now the Southern African country's largest foreign investor (van Staden, 2022). According to Guo Shaochun (2022), China has provided financing support for projects such as "the National Pharmaceutical Warehouse ... the Kariba South Hydro Power Station Expansion ... and upgrading of the Robert Gabriel Mugabe International Airport".

Critically, the aesthetics of these investments provide space for the ZANU-PF to purchase the surveillance technology at the heart of this paper. In the first place, this outcome is made possible by the lack of scrutiny from Zimbabwean citizens, whose priorities sit at a distance from the possibility that they may or not be surveilled.

> For [the government], in their policies they say they want to move towards economic growth. Their partnerships [in surveillance technologies] . . . can always be sanitised under the banner of economic development, economic growth.
>
> *Informant 8*

> I think the current political leadership, you know, if I can describe it, it's a very predatory leadership. So, they are not that concerned with the slower development with regards to the Smart Zimbabwe 2030 Master Plan, as long as China is making other investments in things that are visible. So, your parliament is built, your road is built. These I think are the things that [citizens] are more worried about.
>
> *Informant 1*

The ruling elite subsequently play on the abject poverty experienced by many of its citizens, using visible investments from Chinese enterprises to nullify resistance to the extension of Zimbabwean surveillance infrastructure.

> So, these guys [the Zimbabwean state], they know it and they can sort of underplay the investments and the surveillance, but then overplay the other side of what China is doing. So, in the in the grand scheme of things you are caught in between comparing the deployment of surveillance infrastructure and the deployment of health humanitarian related support. So, you end up just saying forget the surveillance at least they're doing this.
>
> *Informant 1*

As previously discussed, national security has also been used as the pretext for the importation of sophisticated surveillance technology, with such interests cited in the Zimbabwean government's justification for engaging with CloudWalk (Musodza et al., 2022). For a citizen not party to the intricacies of these surveillance developments and the use of the collected data, it is hard to contest arguments - legitimate or linguistic - surrounding safety and economic development.

The government's intention to leverage technology for Zimbabwe's advancement into an upper-middle economy is not inherently problematic. However, the concern lies in how the media and other influential observers have permitted the authorities to obscure the potential detrimental impact of their project on the liberties and opportunities of citizens, under the guise of the *Smart Zimbabwe 2030 Master Plan.* This situation is made more alarming through the manner in which it grants the government the freedom to infringe upon the constitutional rights of Zimbabweans without proper oversight or accountability (Ngwenya, 2021). Indeed, what often gets obscured in this narrative of technological solutionism is the fact that automation and the pervasive collection of data in society provide opportunities for the government to advance intrusive surveillance practices and foster a culture that normalizes them (Munoriyarwa and Mare, 2022). In this way, "the fetishization of smart city projects has the net effect of normalising surveillance tendencies" (ibid:38). As Hecht (2011) explains, there is a need to be conscious of how new forms of technopolitics and technopower can be cloaked in a rhetoric of neutrality and innovation as progress.

A discussion of the predatory leadership of Zimbabwe provides an important segue into questions of agency. There has been a tendency for Western scholars to blame the exporters of digital surveillance technology for the rise in authoritarianism in some geographies. This blanket perspective ignores the ability of the ruling elite to (dis)engage with such actors. Indeed, there have been instances within this surveillance relationship of Zimbabwe reportedly forging its own role as a commercial client that seeks out and purchases China's technologies (The Herald, 2019).

Further, there is the argument that the Zimbabwean government would still be able to surveil without this relationship. This perspective is further reinforced by the implementation of a surveillance system in the city centre of Bulawayo in 2021. The contract for this project was awarded to the local company Tendy Three, which reportedly made a significant investment of $2.2 million (Munhende, 2021). As such, Zimbabwe still has domestic surveillance initiatives that sit outside of this relationship. However, it is unlikely that Zimbabwe would be able to internally develop world-renowned facial recognition technology, and that "without Chinese involvement this surveillance would not be as developed as [it is] in the country" (Informant 6).

Legal Policies: Issues of Operation and Oversight

Zimbabwe has only a few laws and statutory instruments that speak to the question of surveillance. The majority of these legal instruments do not measure up to regional and international benchmarks, and fall short in satisfying criteria related to legality, necessity, proportionality, and user notification.

Metropolitan areas like Harare and Bulawayo operate under the Urban Councils Act (2015) (Chapter 29:15) (Government of Zimbabwe, 2015). This legislation clearly states that local governing bodies, including municipal and town councils, are responsible for managing local boards and municipalities. As a result, the implementation of security camera systems should primarily fall under the jurisdiction of these local organisations. The Media Policy and Democracy Project, however, has found evidence that shows that in most instances the city authorities have had no say in the installation of these surveillance operations in areas where they, legally should have jurisdiction (MPDP, 2020). In some cases, members of the military have issued instructions regarding these rollouts without consulting the relevant stakeholders (ibid.). In this way, the legislation is purely semantic, with the deployment of cameras around cities and towns a national security issue that "requires presidential permission, not anyone else's" (MPDP, 2020:61).

As MISA Zimbabwe (2021a) have written, Zimbabwe's Interception of Communications Act (2007) (ICA) "legitimises surveillance". The legislation, which is not aligned with the constitution, regulates the interception of communications, including telephonic communications, postal telecommunications as well as internet-based communications (MISA Zimbabwe, 2021b). Although questions of communications interceptions sit beyond the remit of this paper, crucially, the "Act does not have any oversight mechanisms that prevent over-surveillance and extra-judicial surveillance" (ibid.). More specifically, the ICA does not address public space surveillance.

As such, there has been a critical absence of legislation governing the installation and application of surveillance technologies in public spaces. The ICA - the major surveillance legislation in existence in the country - falls far short of addressing this subject. According to military commander Edzayi Chimono, the official Zimbabwean narrative regarding surveillance is to "fight hostile foreign forces and internal dissidents led by western sponsored opposition parties" (Munoriyarwa, 2021:8). In practice, this leads to ministerial oversight in place of judicial oversight, with surveillance authorised by a government minister.

> The law says that, you know, at the end of the year, the Attorney-General and the Minister responsible should, should discuss the nature of surveillance that has been done. But it's still very confined to the executive. The Attorney-General constitutes part of the executive, the Minister is part of the executive. So, there's no parliamentary oversight at all whatsoever.
>
> *Informant 1*

As discussed, this gives rise to well-founded fears of political surveillance against opponents and citizens more broadly. The result of these legislative gaps and the absence of a legal framework to comprehensively address public space surveillance in Zimbabwe is the possibility for public-private partnerships - such as those established with CloudWalk and Hikvision - which lead to the installation of surveillance cameras without sufficient regulatory oversight.

Turning to the question of data protection, a prominent theme surrounding the inability of the state to adequately ensure the privacy of citizens was cited by a number of informants.

The right to privacy is enshrined in the Constitution of Zimbabwe. Section 57 of Zimbabwe's Constitution of 2013 states that "every person has the right to privacy" (Government of Zimbabwe, 2013:30), which assumes that every citizen has a right to have their data adequately protected from abuse and any form of misuse (MISA, 2018).

Whilst the constitutional framework has these "relevant guarantees for privacy in the country", insights from Informant 8 as well as the preceding analysis have shown that "there [have] been a number of tools that have been deployed by the government to kind of like crack down on human rights defenders, civil society actors and kind of like monitor their movements as well as political actors in the country". This gap between written disclosures and practice means that a certain regulatory silence can be identified.

Noting that monitoring via facial recognition cameras does happen, the questions that are subsequently raised are thus who has jurisdiction over the data collected by sophisticated surveillance systems, and what happens to this dataset.

The issue surrounding the government's utilisation of CloudWalk's facial recognition technology offers a valuable opportunity to explore the conflict between established laws and their implementation. As part of this agreement, the Zimbabwean government must provide a significant amount of photographic data to the Chinese firm, enabling CloudWalk to adapt its technology to recognise varying skin tones.

In the Access to Information and Protection of Privacy Act (AIPPA), Section 29 (b) states that public entities may collect personal information if it serves the purposes of national security, public order, and law enforcement (Government of Zimbabwe, 2002). However, the question arises whether this provision encompasses the international transfer of such data. The absence of specific data transfer regulations has to date made it impossible to hold both the government and foreign organisations responsible for their handling of Zimbabwean data.

Perhaps somewhat in response to growing pressure from civil society actors, the government established the DPA in late 2021, which also amends parts of the ICA (Government of Zimbabwe, 2021).

The DPA establishes guidelines and principles for the collection, use, and disclosure of personal data by both public and private entities, and according to Zimbabwean attorney Steve Munyaradzi Chikengezha, it was enacted as a means ”to increase data protection in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects” (MISA Zimbabwe, 2021c).

It also permits for the creation of a Cyber Security Centre and a Data Protection Authority involved in the collection of evidence of cybercrime and unauthorised data collection and breaches. A number of informants spoke directly to questions surrounding its functionality, stressing the need to interrogate who oversees its implementation and who is accountable for its results, as well as the two separate spheres of data security and cybersecurity it combines.

The DPA document shows that the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) will be the Data Protection Authority for the purposes of the law (ibid.). POTRAZ has been widely accused of partisanship and making politicised decisions as evidenced by reports by Freedom House (Sanja and Truong, 2012) and the following disclosure:

> The collection of biometric data is regulated by the Cyber Security Centre and Data Protection Act, but the implementation of this Act is compromised by a partisan Data Protection Authority. This leaves opportunities for the misuse of collected biometric data as well as the repurposing of biometric data databases for purposes outside of why such databases were originally established.
>
> *Informant 3*

The location of the new centre has also raised questions:

> [The centre] is vested in the Office of the President, which is state security. So, the Ministry of Information and Communication Technologies has to report to this centre. We’ve got state security sort of like over everything that happens with data. So, the central question is what’s going to happen as well to that data that is collected by the state? What about this smart city initiative? What is going to happen to that data?
>
> *Informant 8*

A Cybersecurity Committee has been established, with members chosen on a temporary basis by the Minister of Information and Communication Technologies. Consequently, it is essential to raise questions about the party responsible for enforcing this data protection legislation and whether the presidential office and political committees can be held accountable.

Turning to the exportation of data, the updated legislation explicitly mentions that “personal data cannot be transferred outside Zimbabwe unless an adequate level of protection is ensured in the destination country” (Securiti, 2022). Nevertheless, there are certain areas within the Act that remain unclear, leaving room for the Data Protection Authority to define the conditions or cases where transferring data to foreign countries is permitted. As stated, "[the transfer of data] will be determined by the regulatory authority keeping in mind what data is being transferred" (ibid.).

In a similar vein, the Act mentions that citizens can report issues regarding their data protection. However, where there exists a genuine avenue for accountability is unclear. In Zimbabwe, the contentious Amendment No. 2 has granted the president the authority to personally select judges, which has effectively undermined the judiciary's independence. In such legal contexts, it is rare that these mechanisms for accountability stand up if the justice system effectively serves partisan interests (Munirorywa and Mare, 2022). There is already evidence in Zimbabwe of the judiciary functioning as a mere instrument of the ruling elite. For instance, High Court Judge George Chiweshe declared the coup that ousted Mugabe as legal (Mutsaka and Torchia, 2017).

Despite not being mentioned by informants, additional objections to the Act have emerged from civic groups like the Zimbabwe Human Rights Lawyers' Association. These organisations contend that data access guidelines and cybersecurity regulations ought to be addressed separately. They believe that combining these matters leads to the conflation of distinct issues, which in turn, hinders stakeholders from contesting specific aspects of the legislation (such as opposing data retention laws without disputing the cybersecurity provisions included in the same law). MISA Zimbabwe (2022:7) agrees, stating that these provisions make it clear that "the government is operating under a very misled presumption that cybersecurity equals national security".

Taken together, the outlined legal provisions allow for "executive powers with no oversight mechanisms, of any remedial mechanisms, and lack end-to-end safeguards" (Saki, forthcoming: 14). This paper thus asserts that both surveillance and data protection regulations in Zimbabwe highlight the conflict between political interests and legal values, with the former increasingly influencing the exercise of the latter. In this way, "Modern Zimbabwe has maintained and perfected an arsenal of obnoxious security laws reminiscent of the colonial era" (ibid.: 2). The presence of law makes a difference, but when there are gaps and questions are raised about oversight mechanisms, the law ceases to be just law.

Informants, however, did not just stress issues surrounding Zimbabwean regulatory and legal frameworks. A number of informants covered the absence of global frameworks surrounding the exportation of sophisticated surveillance technology.

> Globally there is no there's no regulation of the selling off of this software. We know that all these potentially harmful tools require a regulatory framework. You know, they can't just be stored just like that like open market. So, the global absence of a regulatory framework makes this [phenomenon] inevitable.
>
> *Informant 1*

The lack of transparency in this domain makes arrangements such as those with CloudWalk and Hikvision possible, and makes it difficult for actors to be held responsible. Demand is increasing for worldwide oversight of monitoring technology as it is essential to ensure that such software upholds human rights standards. This has included UN human rights experts calling "on all states to impose a global moratorium on the sale and transfer of surveillance technology" until robust regulations are introduced that guarantee "compliance with international human rights standards" (OHCHR, 2021).

The need to examine these deals more closely is further compounded when we consider the implications of the exportation of biometric data to sharpen algorithmic technologies. Algorithmically intelligent surveillance systems - as discussed - are deeply embedded in the global capitalist race for economic dominance. In this way, a small number of companies - many of which are intimately entangled with state relations - will be at the forefront of the roll-out of these technologies. If the development of a domestic AI system is beyond Zimbabwe's capabilities, it seems necessary to initiate a global endeavour that taps into the "ethical foresight and the multiplicity of intellectual perspectives available to us" to prevent the replication of existing societal inequalities in roll-out of sophisticated surveillance technologies (Mohamed et al. 2020:28).

Conclusion

This paper has examined the case of Chinese AI technology in Zimbabwean surveillance through the lens of algorithmic coloniality, addressing three central research questions derived from the work of Mohamed et al. (2020).

The research demonstrates that the deployment of Chinese AI surveillance technology in Zimbabwe is primarily motivated by the ruling party's desire to maintain political power. Examining algorithmic oppression, the analysis found that facial recognition systems enable the government to silence political opponents, curtail rights to association and assembly, and create a climate of intimidation. However, it is argued that the adoption of sophisticated surveillance tools has sharpened the capabilities of existing surveillance practices rather than generating entirely new ones. The case study also revealed a dual level of subordination, where the ruling elite can surveil both the wider public and individuals within its own party, effectively subordinating multiple social groups.

Regarding algorithmic exploitation, the research highlighted ethical concerns related to the exploitation of resources and people. Chinese companies, such as CloudWalk and Hikvision, and their opaque agreements with the Zimbabwean government have allowed for the potential illicit transfer and use of citizen data for the asymmetrical benefit of these actors. It is asserted that the acquisition and non-consensual extraction of biometric data resembles historical colonial exploitation, with Zimbabwe serving as a testing ground and data source for Chinese technological advancements. Labour exploitation and displacement further contributes to algorithmic exploitation, as workers involved in the production and management of these systems face low wages, long working hours, and limited agency.

The paper also examined algorithmic dispossession, focusing on economic and legal policies. Chinese investment in Zimbabwe extends beyond digital surveillance and leads to a deepening economic dependency on China. The bank-led business cycle perpetuates a vicious cycle of economic dependence, consolidating China's power in the region, stifling the development of a domestic AI industry. It is argued that the importation of Chinese technology also hinders the empowerment and growth of local entrepreneurs, reinforcing Zimbabwe's role as a consumer of Chinese goods and solutions. Legal policies related to surveillance technology exhibit gaps and inadequate oversight mechanisms, making the configuration of outcomes this paper has analysed possible.

In sum, the analysis revealed that the deployment of Chinese AI surveillance technology in Zimbabwe extends the unjust subordination of social groups and the privileging of the ruling party, illustrating algorithmic oppression. The development of Chinese AI surveillance technology involves the exploitation of data and labour, reflecting algorithmic exploitation. Furthermore, policies related to the importation of Chinese AI surveillance technology facilitate the centralisation of Chinese economic power, lubricated by an inadequate domestic legal framework and relaxed global picture, resulting in outcomes indicative of algorithmic dispossession. Cumulatively, this paper can confidently assert that this case study exhibits strong elements of the algorithmic coloniality conceptualised by Mohamed et al. (2020).

It is hoped that other scholars will take up the analytical method deployed and apply it to other case studies such as those outside of the African continent. Not only will this endeavour help understand the similarities and differences in outcomes between separate geographies, but it will also help to fine tune the application of algorithmic coloniality as a tool for academic research.

Further, it is hoped that the topic of this paper is explored beyond academia, with policymakers taking heed from experts such as the informants of this paper. The findings highlight the need for comprehensive legislation, independent oversight, and international collaboration to address the gaps, loopholes, and inadequate regulations surrounding AI surveillance technology. This paper makes the case that global frameworks for regulating the exportation of surveillance technology should be developed to ensure the protection of rights and nullify the high degree of risk they can pose to already marginalised people (Vernon, 2019).

References

AdVox. 2022. ”Unfreedom Monitor Report: Zimbabwe.” *Global Voices.* September 8. Accessed January 2024. https://globalvoices.org/2022/09/08/unfreedom-monitor-report-zimbabwe/.

AdVox. 2023. ”How Zimbabwe is Building a Big Brother Surveillance State.” *Global Voices*, January 10. Accessed January 24, 2023. https://globalvoices.org/2023/01/10/how-zimbabwe-is-building-a-big-brother-surveillance-state/.

Aidoo, Richard, and Steve Hess. 2015. ”Non-interference 2.0: China’s Evolving Foreign Policy Towards a Changing Africa.” *Journal of Current Chinese Affairs* 44 (1): 107-139.

Al-Fadhat, Faris, and Hari Prasetio. 2022. ”How China’s Debt-Trap Diplomacy Works in African Countries: Evidence from Zimbabwe, Cameroon, and Djibouti.” *Journal of Asian and African Studies.* https://doi.org/10.1177/00219096221137673.

Amnesty International. 2020. ”Zimbabwe: Persecution of Tortured Female Opposition Leaders Continues as They Are Denied Bail.” *Amnesty International.* June 2020. Accessed January 22 2023. https://www.amnesty.org/en/latest/news/2020/06/zimbabwe-persecution-of-tortured-female-opposition-leaders-continues-as-they-are-denied-bail/.

Andersen, Ross. 2020. “The Panopticon is already here.” *The Atlantic.* Atlantic Media Company. September 2020. Accessed Febuary 6, 2023. https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

Babbie, Earl, and Johann Mouton. 2001. *The Practice of Social Research: South African Edition.* Cape Town: Oxford University Press Southern Africa.

Beraja, Martin, Albert Kao, David Y. Yang, and Noam Yuchtman. 2023. “Exporting the Surveillance State via Trade in AI.” *The Brookings Institution.* January 2023. Accessed January 13, 2023. https://www.brookings.edu/research/exporting-the-surveillance-state-via-trade-in-ai/.

Beraldo, Davide, and Stefania Milan. 2019. “From Data Politics to the Contentious Politics of Data.” *Big Data & Society* 6, no. 2: 2053951719885967.

Bhambra, Gurminder K. 2020. ”Colonial global economy: towards a theoretical reorientation of political economy.” *Review of International Political Economy* 28, no. 2: 307-322.

Burt, Chris. 2018. “Zimbabwe to use Hikvision facial recognition technology for Border Control.” *Biometric Update.* June 2018. Accessed March 8, 2023. https://www.biometricupdate.com/201806/zimbabwe-to-use-hikvision-facial-recognition-technology-for-border-control.

Cabestan, Jean-Pierre. 2020. “The State and Digital Society in China: Big Brother Xi is Watching You!” *Issues & Studies* 56, no. 01.

Cook, Sarah. 2018. “China’s Cyber Superpower Strategy: Implementation, Internet Freedom Implications, and US Responses.” *Freedom House.* Report 28.

Crawford, Kate. 2021. *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence.* New Haven: Yale University Press.

Dahir, Abdi Latif. 2019. “Chinese Firms are Driving the Rise of AI Surveillance across Africa.” *Quartz.* September 2019. Accessed March 24, 2023. https://qz.com/africa/1711109/chinas-huawei-is-driving-ai-surveillance-tools-in-africa.

Dauvergne, Peter. 2022. “Facial Recognition Technology for Policing and Surveillance in the Global South: A Call for Bans.” *Third World Quarterly* 43, no. 9: 2325-2335.

Davenport, Christian. 2005. “Understanding Covert Repressive Action: The Case of the US Government Against the Republic of New Africa.” *Journal of Conflict Resolution* 49, no. 1: 120-140.

Dawn-Hiscox, Tanwen. 2017. “Zimbabwe Launches Two Data Centers in Partnership with Huawei.” *Data Center Dynamics.* February 2017. Accessed January 24, 2023. https://www.datacenterdynamics.com/en/news/zimbabwe-launches-two-data-centers-in-partnership-with-huawei/.

Du Toit, André. 2017. “Hyper-Political Anti-Politics.” *openDemocracy.* April 2017. Accessed March 24, 2023. https://www.opendemocracy.net/en/hyper-political-anti-politics/.

Dube, Gibbs. 2020. “MDC Breathes Fire as Zimbabwe Deputy Minister Says Joanna Mamombe, 2 Others Are Faking Abductions.” *VOA.* June 2020. Accessed

January 27, 2023. https://www.voazimbabwe.com/a/zimbabwe-deputy-minister-faking-abductions/5424121.html.

Elmi, Najla. 2020. "Is Big Tech Setting Africa Back?" *Foreign Policy.* November 2020. Accessed January 21, 2023. https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back/.

European Data Protection Board. 2022. "Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement." May 2022. https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

Feldstein, Steven. 2019. *The Global Expansion of AI Surveillance. Vol. 17.* Washington, DC: Carnegie Endowment for International Peace.

Feldstein, Steven. 2021. *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance.* Oxford: Oxford University Press.

Feldstein, Steven. 2022. "AI & Big Data Global Surveillance Index (2022 updated)", *Mendeley Data*, V4.

Ferguson, James. 2006. *Global Shadows: Africa in the Neoliberal World Order.* Durham: Duke University Press.

Foucault, Michel. 1980. *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977.* New York: Vintage.

Freedom House. 2018. "The Rise of Digital Authoritarianism." October 2018. Accessed March 8, 2023. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

Freedom House. 2022. "Zimbabwe: Freedom on the Net 2022 Country Report." Accessed January 24, 2023. https://freedomhouse.org/country/zimbabwe/freedom-net/2022.

Gallagher, Ryan. 2019. "Export Laws: China is Selling on Surveillance Technology to the Rest of the World." *Index on Censorship* 48, no. 3: 35-37.

Guo, Shaochun. 2022. "Promoting China-Zimbabwe Ties to a New Height." Accessed February 12, 2023. http://zw.china-embassy.gov.cn/eng/xwdt/202210/t20221002_10776874.htm.

Government of Zimbabwe. 2002. *Access to Information and Protection of Privacy Act.* [Chapter 10: 27].

Government of Zimbabwe. 2013. *Constitution of Zimbabwe.* Amendment (No 20). Act 2013.

Government of Zimbabwe. 2015. *Urban Councils Act* [Chapter 29:15].

Government of Zimbabwe. 2019. "Income Tax (Exemption from Income Tax) (Huawei Technologies Co., Ltd.) Notice, 2019." Accessed February 7, 2023. https://www.veritaszim.net/sites/veritas_d/files/SI\%202019-227\%20Income\%2

0Tax\%20(Exemption\%20from\%20Income\%20Tax)\%20(Huawei\%20Technologies\%20Co.,\%20Ltd.)\%20Notice,\%202019.pdf.

Government of Zimbabwe. 2021. *Data Protection Act* [Chapter 11:12].

Gravett, Willem H. 2020. "Digital Coloniser? China and Artificial Intelligence in Africa." *Survival* 62, no. 6: 153-178.

Gray, Mary L., and Siddharth Suri. 2019. *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*. New York: Eamon Dolan Books.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. London: Palgrave Macmillan.

Haggerty, Kevin D., and Richard V. Ericson. 2000. "The Surveillant Assemblage." *The British Journal of Sociology* 51, no. 4: 605-622.

Haggerty, Kevin D., and Richard V. Ericson. 2006. *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Hawkins, Amy. 2018. "Beijing's Big Brother Tech Needs African Faces." *Foreign Policy*. Accessed January 24, 2023. https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.

Hawkins, Amy. 2022. "China is Helping Zimbabwe to Build a Surveillance State." *The Economist*. Accessed January 24, 2023. https://www.economist.com/middle-east-and-africa/2022/12/15/china-is-helping-zimbabwe-to-build-a-surveillance-state.

Hecht, Gabrielle. 2011. *Entangled Geographies: Empire and Technopolitics in the Global Cold War*. Cambridge: MIT Press.

Hemmings, John. 2020. "Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road." *Asia Policy* 15, no. 1: 5-22.

Hove, Mediel. 2012. "The Debates and Impact of Sanctions: The Zimbabwean Experience." *International Journal of Business and Social Science* 3, no. 5.

Iliadis, Andrew, and Federica Russo. 2016. "Critical Data Studies: An Introduction." *Big Data & Society* 3, no. 2: 2053951716674238.

Karekwaivanane, George, and Natasha Msonza. 2021. "Zimbabwe Digital Rights Landscape Report." In *Digital Rights in Closing Civic Space: Lessons from Ten African Countries*, edited by Tony Roberts. Brighton: Institute of Development Studies.

Karombo, Tawanda. 2020. "Legal Experts Question Zim's Tax Exemptions for Huawei." *ITWeb Africa*. Accessed February 7, 2023. https://itweb.africa/content/Olx4zMknzG5756km.

Kelly, Sanja, Sarah Cook and Mai Truong. 2012. *Freedom of The Net: A Global Assessment of Internet and Digital Media*. Washington: Freedom House.

Layton, Peter. 2020. ”Artificial Intelligence, Big Data and Autonomous Systems Along the Belt and Road: Towards Private Security Companies with Chinese Characteristics?” *Small Wars & Insurgencies* 31, no. 4: 874-897.

Lee, Kai-Fu. 2017. ”The Real Threat of Artificial Intelligence.” *The New York Times.* Accessed February 19, 2023. https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html.

Lyon, David. 2001. *Surveillance Society.* Buckhimgam: Open University Press.

Mabaya, N. and M. Motsi. 2020 ”Spotlight Zimbabwe”. Accessed January 24, 2023. spotlight-z.com/news/zimbabwe-splurges-us20-million-huawei-mass-surveillance-grid-technology/.

Masau, Problem. 2018. ”Face of the Future”. *ChinaAfrica*, 2018. Accessed January 23, 2023. http://www.chinafrica.cn/Homepage/201808/t20180813_800138079.html.

Masau, Problem. 2022. ”Ambassador defends ‘abusive’ Chinese employer”. *Zimbabwe Situation.* Accessed February 09, 2023. https://www.zimbabwesituation.com/news/ambassador-defends-abusive-chinese-employers/.

Media Monitors. 2020. *A Media Landscape Study: Unpacking Ownership in Zimbabwe's Creation and Delivery of News Content.* Harare: Friedrich-Ebert-Stiftung.

Media Policy and Democracy Project. 2020. ”Video Surveillance in Southern Africa: Case Studies of Security Camera Systems in the Region.” https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf.

Ministry of ICT, Postal and Courier Services. 2019 ”SMART ZIMBABWE 2030 MASTER PLAN,” *Internal Government Report.* Unpublished.

MISA Zimbabwe. 2018. ”Digest: Facial recognition technology and privacy rights”. Accessed February 29, 2023. https://zimbabwe.misa.org/2018/05/29/digest-facial-recognition-technology-privacy-rights/.

MISA Zimbabwe. 2019. ”Letter to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/MISA_ZIMBABWE.pdf.

MISA Zimbabwe. 2021a. ”Concern over acquisition and use of surveillance tools in Zimbabwe,” https://misa.org/blog/concern-over-acquisition-and-use-of-surveillance-tools-in-zimbabwe/. Accessed March 12, 2023.

MISA Zimbabwe. 2021b. ”Surveillance and privacy,” Accessed March 11, 2023. https://zimbabwe.misa.org/issues-we-address/surveillance-and-privacy/#:~:text=In\%20Zimbabwe\%2C\%20the\%20Interception\%20of,well\%20as\%20Internet\%2Dbased\%20communications.

MISA Zimbabwe. 2021c. "Analysis of the Data Protection Act". Accessed March 10, 2023. https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/.

MISA Zimbabwe. 2022. "The state of press freedom in Southern Africa 2020-2021". Accessed January 3, 2023. https://unesdoc.unesco.org/ark:/48223/pf0000381397.

Mohamed, Shakir, Marie-Therese Png, and William Isaac. 2020. "Decolonial AI: Decolonial theory as sociotechnical foresight in artificial intelligence." *Philosophy & Technology* 33, no. 4 (2020): 659-684.

Mohamed, Shakir, Marie-Therese Png, and William Isaac. 2021. "Decolonizing AI," *Boston Review*, May 20. Accessed January 19, 2023. https://www.bostonreview.net/forum_response/decolonizing-ai/.

Mudzingwa, Farai. 2018. "Government Acknowledges Facial Recognition System in the Works." *TechZim*, June. Accessed January 5, 2023. https://www.techzim.co.zw/2018/06/government-acknowledges-facial-recognition-system-in-the-works/.

Munhende, Lenin. 2021. "Government Approves Massive Surveillance for Bulawayo." *New Zimbabwe*, August 13. Accessed January 16, 2023. https://www.newzimbabwe.com/government-approves-massive-surveillance-for-bulawayo/.

Munoriyarwa, Admire. 2021. "The Growth of Military-Driven Surveillance in Post-2000 Zimbabwe." *Media Policy and Democracy Project.* https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/report_01_2021_military_driven_surveillance_zimbabwe_masterset.pdf.

Munoriyarwa, Admire. 2022. "The Militarization of Digital Surveillance in Post-Coup Zimbabwe: 'Just Don't Tell Them What We Do'." *Security Dialogue* 53, no. 5: 456-474.

Munoriyarwa, Admire, and Sarah Helen Chiumbu. 2022. "Powers, Interests and Actors 1: The Influence of China in Africa's Digital Surveillance Practices." In *Digital Dissidence and Social Media Censorship in Africa*, edited by Farooq A. Kperogi, 209-229. London: Routledge.

Munoriyarwa, Admire, and Admire Mare. 2022. *Digital Surveillance in Southern Africa: Policies, Politics, and Practices.* Berlin: Springer Nature.

Muronzi, Chris. 2022. "Analysts Predict Economic Struggles for Zimbabwe in 2023." *Al Jazeera*, DEcember 30. Accessed February 24, 2023. https://www.aljazeera.com/economy/2022/12/30/analysts-predict-economic-struggles-for-zimbabwe-in-2023.

Musodza, Chipo, Kholwani Hove, and Obediah Saki. 2022. "Surveillance to Consolidate Political Power." *The Zimbabwe Independent*, December 9. Accessed February 5, 2023. https://www.newsday.co.zw/theindependent/opinion/article/200004778/surveillance-to-consolidate-political-power.

Mutsaka, Farai, and Christopher Torchia. 2017. ”Zimbabwe Judge Says Military Action Against Mugabe Was Legal.” *Yahoo! Finance.* Accessed March 3, 2023. https://uk.finance.yahoo.com/news/zimbabwe-judge-says-military-action-133901288.html.

Ndlela, Dumisani. 2020a. ”Creating a Surveillance State: Ed Govt Zooms in for Critics with Chinese Help.” *The Standard*, March 1. Accessed January 23, 2023. https://thestandard.newsday.co.zw/2020/03/01/creating-surveillance-state-ed-govt-zooms-critics-chinese-help.

Ndlela, Dumisani. 2020b. ”Privacy Violations Fears Grow as Govt Sets Surveillance Cameras in Cities.” *The Standard*, June 21. Accessed January 23, 2023. https://www.newsday.co.zw/thestandard/2020/06/21/privacy-violations-fears-grow-govt-sets-surveillance-cameras-cities.

Ndlela, Dumisani. 2020c. ”’Zim’s Era of the State’ Could Herald Increased Repression.” *The Standard*, September 6. Accessed January 24, 2023. https://www.thestandard.co.zw/2020/09/06/zims-era-of-the-state-could-herald-increased-repression.

Ndlela, Dumisani. 2022. ”Zim in Danger of Sleepwalking into a Surveillance State.” *The Zimbabwe Independent.* Accessed January 23, 2023. https://www.newsday.co.zw/theindependent/tennis/article/15765/zim-in-danger-of-sleepwalking-into-a-surveillance-state.

Ndoro, Nyashadzashe. 2020. ”Misa Zimbabwe Bemoans Mnangagwa’s Use of Targeted Surveillance on Critics.” *Nehanda Radio*, October 14. Accessed February 2, 2023. https://nehandaradio.com/2020/10/14/misa-zimbabwe-bemoans-mnangagwas-use-of-targeted-surveillance-on-critics.

Ngwenya, Nhlanhla. 2021. ”Zimbabwe’s Vision 2030 Clouds Big Brother Technology.” *Research ICT Africa*, July 9. Accessed January 30, 2023. https://researchictafrica.net/2021/07/09/zimbabwes-vision-2030-clouds-big-brother-technology.

Norman, Thomas L. 2017. “Electronics Elements.” In *Effective Physical Security, 5th Edition*, edited by Lawrence J. Fennelly. Oxford: Butterworth-Heinemann. 95-137.

Noyes, Alexander H. 2020. *A New Zimbabwe: Assessing Continuity and Change After Mugabe.* Santa Monica: Rand Arroyo Center.

Office of the United Nations High Commissioner for Human Rights (OHCHR). 2020. ”Zimbabwe: UN Experts Demand an Immediate End to Abductions and Torture.” Accessed January 15, 2023. https://www.ohchr.org/en/news/2020/06/zimbabwe-un-experts-demand-immediate-end-abductions-and-torture.

Office of the United Nations High Commissioner for Human Rights (OHCHR). 2021. ”Spyware Scandal: UN Experts Call for Moratorium on Sale of ‘Life Threatening’ Surveillance Tech.” Accessed January 5, 2023. https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

Office of the United Nations High Commissioner for Human Rights (OHCHR). 2023. ”UN Experts Urge President of Zimbabwe to Reject Bill Restricting Civic Space.” Accessed February 16, 2023. https://www.ohchr.org/en/press-releases/2023/02/un-experts-urge-president-zimbabwe-reject-bill-restricting-civic-space.

Okolo, Chinasa T., Kehinde Aruleba, and George Obaido. 2023. ”Responsible AI in Africa—Challenges and Opportunities.” In *Responsible AI in Africa: Challenges and Opportunities*, edited by Damian Okaibedi Eke, Kutoma Wakunuma and Simisola Akintoye. Cham: Springer Nature. 35-64.

Polyakova, Alina, and Chris Meserole. 2019. ”Exporting Digital Authoritarianism: The Russian and Chinese Models.” *Policy Brief*, Democracy and Disorder Series, 1-22.

Rupiya, Martin R. 2013. *Zimbabwe's Military: Examining Its Veto Power in the Transition to Democracy, 2008-2013.* Berlin: The African Public Policy & Research Institute.

Sachikonye, Lloyd. 2011. *When a State Turns on Its Citizens: 60 Years of Institutionalised Violence in Zimbabwe.* Oxford: African Books Collective.

Saheb, Tahereh. 2022. ”Ethically Contentious Aspects of Artificial Intelligence Surveillance: A Social Science Perspective.” *AI and Ethics*, 1-11.

Saki, O. Forthcoming. “‘We Will Visit Your Bedrooms’: Testing the Adequacy of Safeguards in Interception of Communications in Zimbabwe through the Lens of the Ambhungane Case.”

Saldaña, Johnny. 2021. *The Coding Manual for Qualitative Researchers.* London: Sage. 1-440.

Sanusi, Lamido. 2011. ”Neither the Washington nor Beijing Consensus: Developmental Models to Fit African Realities and Cultures.” *CBN Journal of Applied Statistics* 2, no. 2: 101-113.

Scott, James C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.* New Haven: Yale University Press.

Securiti. 2022. ”Overview of Zimbabwe New Data Protection Act.” *Securiti.* Accessed March 2, 2023. https://securiti.ai/zimbabwe-new-data-protection-act/.

Shan, Jie. 2018. ”China Exports Facial ID Technology to Zimbabwe.” *Global Times.* Accessed January 24, 2023. https://web.archive.org/web/20191103210714/http://www.globaltimes.cn/content/1097747.shtml.

Sharma, Ishan. 2020. ”China's Neo-Colonialism in the Political Economy of AI Surveillance.” *Cornell International Affairs Review* 13, no. 2: 94-154.

Swinhoe, Dan. 2021. ”National Data Center in Zimbabwe Opens.” DCD. Accessed January 24, 2023. https://www.datacenterdynamics.com/en/news/national-data-center-zimbabwe-opens/.

Tarrow, Sidney G.. 1998. *Power in Movement: Social Movements and Contentious Politics*. Cambridge: Cambridge University Press.

Tarrow, Sidney G.. 2001. "Transnational Politics: Contention and Institutions in International Politics." *Annual Review of Political Science* 4.

The Financial Gazette. 2016. "Huawei Sees Growth in Zimbabwe." *The Financial Gazette*. Archived from the original on March 29, 2017. Accessed January 24, 2023. http://web.archive.org/web/20170329153056/http://financialgazette.co.zw/huawei-sees-growth-in-zimbabwe/.

The Herald. 2019. "Chinese Tech Revolution Comes to Zim." *The Herald*. Accessed March 8, 2023. https://www.herald.co.zw/chinese-tech-revolution-comes-to-zim/.

The Zimbabwe Mail. 2022. "Did Mthuli Ncube Lie to Parliament About How Much Zimbabwe Owes China?" *The Zimbabwe Mail*. Accessed March 24, 2023. https://www.thezimbabwemail.com/parliament-parliament/did-mthuli-ncube-lie-to-parliament-about-how-much-zimbabwe-owes-china/.

Tshabangu, Thulani, and Abiodun Salawu. 2022. "Alternative Media, Repression and the Crisis State: Towards a Political Economy of Alternative Media in Post-Mugabe Zimbabwe." *Journal of Asian and African Studies* 59(1).

Van Staden, Cobus. 2022. "China Is Now Zimbabwe's Biggest Investor." *China Global South*. Accessed January 23, 2023. https://chinaglobalsouth.com/2022/10/20/china-is-now-zimbabwes-biggest-investor/.

Vernon, David. 2019. "Robotics and Artificial Intelligence in Africa [regional]." *IEEE Robotics & Automation Magazine* 26, no. 4: 131-135.

Woodhams, Samuel. 2019. "How China Exports Repression to Africa." *The Diplomat*. Accessed February 4, 2023. https://thediplomat.com/2019/02/how-china-exports-repression-to-africa/.

York, J. 2014. "Communications Surveillance in the Digital Age: The Harms of Surveillance to Privacy, Expression, and Association." *Global Information Society Watch*.

Zimbabwe Coalition on Debt and Development. 2020. "Zimbabwe Coalition on Debt and Development: Second Quarter Report." Accessed February 12, 2023. https://zimcodd.org/wp-content/uploads/2020/03/ZIMCODD-2nd-Quarter-Report.pdf.

Zhang, Hongpei. 2018. "Chinese Facial ID Tech to Land in Africa." *Global Times*. Accessed January 24, 2023. https://web.archive.org/web/20180518215448/https://www.globaltimes.cn/content/1102797.shtml.

Notes