Journal of Education and Practice
ISSN 2222-1735 (Paper) ISSN 2222-288X (Online)
Vol.16, No.13, 2025

An Assessment of Data Colonialism Awareness and Proposed Remedial actions: The case of Zambia

Billy C Sichone*
Central Africa Baptist University
*bsichone@cabuniversity.com

Abstract
The study aimed at assessing final digital data destiny awareness and management among stakeholders in Zambia. It sought to establish where and how data was stored, used and whether patrons were aware where their data finally ended up. Using a cross-sectional qualitative study design, the enquiry elicited thoughts, opinions and ideas from patrons from a cross section of Zambians drawn from HEIs, Government, ICT experts and users that voluntarily offered valuable data. The enquiry relied on two theories: Stakeholder and Surveillance Capitalism respectively. To arrive at the initial sample, stakeholder mapping was conducted followed by purposive sampling at each site. A final sample of responsive entities of 28 emerged that were then interviewed using open ended questions. The Research found that the majority of respondents were unaware where their generated digital data finally ended up nor did they know who else had access to it. The study also found that Zambia was perceived largely dependent on external entities for cloud data storage. The study concludes that Zambia is vulnerable. Its data is neither secure nor protected from third party privacy abuse like global tech giants. The enquiry recommends that Zambia heavily invests in locally owned digital infrastructure (e.g. servers, cloud storage and computing, data centres etc.) so that it could assert total control and locally manage this data for citizen identity protection and growth of contextual AI. The study also recommends that the government invests in on going sensitization, training and enacting relevant objectively equitably strong cyber laws to protect citizens rather than digital for democracy inhibiting ends, narrative control or only enhancing foreign conglomerate interests.
Key words: Data; Digital Colonialism; Storage; Artificial Intelligence (AI); Higher Education Institution (HEI); Surveillance capitalism; Control
DOI: 10.7176/JEP/16-13-06
Publication date: December 30th 2025

Introduction and background

The word ‘colonialism’ differently affects all of us, triggering high emotions in some minds than others. To the latter cohort, the word appears a remote reality not worth discussing today. In their minds, the idea of colonialism appears to belong to a by-gone-era, forever thrust into the dustbin of history. However, despite the fact that the practice of physical imperial territorial occupation largely is past, it is back in another form, and sadly, not many are aware or care. Manzar (2017) correctly observes that “colonizing a country no longer requires its physical invasion…” This study reviews this concept and proposes corresponding remedial actions for a Global South Nation in a digital age. Specifically, this enquiry examines the local Zambian scene since there is much going on in the world today where the globe has literary shrunk into a village in terms of connectedness, is technology propelled and integrated (Steger, 2003). In the contemporary world and at the click of a button, decisions are disseminated right across the world in record time thus accelerating life pace. Although this is an extremely good thing, it equally presents challenges (Ohara-Deveraux & Johansen, 1994; Hill, 2003; Rowntree et al., 2015; Greenwood, 2020). In this enquiry, we discuss the situation presented by the digital age; both opportunities and challenges. Despite all these potentials offered by technology, Zambia lags behind on infrastructure for data security and thus susceptible to foreign agents meddling with or profiting off its data.

Statement of the problem

Given the scenario painted above, Zambia is at a bad place. Whilst benefiting from these emerging technologies, a number of concerns arise. First, the integrity or country’s data sovereignty stands in peril[1]. Second, privacy of individuals is compromised and so is data security is no longer assured. Third, this leads to dependence on other

[1] An example is the recent development where Starlink has increasing global potency to connect or disconnect a country or group of them. In 2025 (9th April), the tech giant rolled out direct connectivity to any cell phone on the planet. The full report is accessible at: https://jasondeegan.com/elon-musk-enables-satellite-calls-on-iphones-and-androids-worldwide/, accessed on 12th April, 2025. With this coverage comes even greater power, reach and threat to other industry competitors. While this is good for the larger global citizenry, it is not ideal to concentrate power in one entity. To partly mitigate this, strong cyber laws need to come into play for equitable functioning by all players.

wealthier nations' digital and data storage infrastructure. Granted, connecting and synching to the world wide web (www) is a given but not everything must be on the internet for more reasons than one. This study evaluates the status quo, identifies gaps while offering proposed potential solutions into the future.

Research Objectives

To execute this exploration, a number of study objectives are listed below.

1. Establish the perceived status of data storage awareness in Zambia today.
2. Identify mandated key data storage facilities, protecting agencies in Zambia and their intentions.
3. Suggest content relevant solutions for Zambia.

Research Questions

The objectives are buttressed by corresponding Research Questions stated at length:

1. What is the perceived status of data storage awareness in Zambia today?
2. What data storage facilities, data protecting agencies exist in Zambia and what are their intentions?
3. What suggested context relevant solutions could aid the situation in Zambia?

The study sought to establish awareness levels and what mandated data protection institutions were doing to mitigate data breaches. It also established what study informants knew about AI use and management.

Research Significance and contributions

A study of this nature is important. What difference does the enquiry make? For one thing, it answers the 'so what?' question.

First, it triggers discussion in Zambia, because during preliminary literature review, it was evident that limited published documentation existed, urging caution, circumspection, prudence to determine how data was stored or managed. It was further observed that not much history was available. Thus, this study should animate discussion and documentation.

Secondly, the study provides empirical data for the Zambian scenario, filling a data dearth and should offer ready information for planners, stakeholders or interested parties, in Academic circles and otherwise.

Thirdly, strategic decision makers, should use this report for efficient strategic allocation of scarce national resources. Armed with data, they will not only focus on the positive sides, but mind the downside as well. For example, the Starlink Global Satellite advent appears (and in fact it is) a great idea. Data access is fast, efficient, cheaper and cost effective but what is it doing to country sovereignty? How secure is data? Suppose Starlink decided to abruptly terminate the contract and walked away, what would Zambia do?[1] These are sorts of questions that this study explores and contributes to national body of knowledge. Sichone (2023) expressed similar concerns when he opined that the multinationals, whilst investing impressive amounts of cash and infrastructure, had a subtly hidden agenda of maximizing profits in any context they dominated. By that token, the study makes massive contribution to existing body of knowledge in Zambia, one of them being that is it generates ongoing discussion about data integrity in our country. Second, the enquiry raises strategic cautions around how and who has access to national data and secondarily, how citizens use digital devices. The Research encourages prudent and cautious use of digital networks, where data is stored or secured. The fourth contribution is that this study triggers thought around harvesting, storing contextual local national data and resultant control. Armed with that power, Zambia could then harvest, manipulate and use indigenous data for correct purposes e.g. training local AI experts. There is need to be extremely cautious as a nation, not rushing into things because '*…everybody else is doing it…even us let us also go along…*' This mentality is prevalent among politicians whose sole goal in life is short term political mileage acquisition.

Finally, this study contributes to raising awareness about the possibility of profiting from our locally generated

[1] Starlink is far more potent today than yesterday. Refer to an earlier link to get an illustration of what we mean to say: https://jasondeegan.com/elon-musk-enables-satellite-calls-on-iphones-and-androids-worldwide/, accessed on 14th April, 2025.

data harvested for sale to help develop the nation. Currently Zambia is dishing out data for free while somebody profits over the same.

Literature Review

A sensitive study of this nature and magnitude is critical, demanding urgent attention. The parties publishing on it must have access to the right data and execute good literature review lest they mislead masses. *Literature Review* is basically an evaluation of what other Scholars, thought leaders and Researchers have opined or published about a given subject directly or indirectly, what they found or concluded about it. As such, Researchers need to demonstrate that they have done their homework, observe and correctly interpret what actually is on the ground. From the outset, it is evident that a number of people now increasingly are beginning to realize that a few multinational corporations and individuals are in control of and thus benefiting from data mining that the world generates.

For us to better appreciate this enquiry, we need to define basic terms like *colonialism* in the contemporary setting. While acknowledging that various definitions, connotations, imports or descriptions of the concept exist, we select two definitions and then craft a working definition for ourselves. Later, we also distinguish between 'digital' and 'data' colonialism for clarity. Manzar (2017) describes 'colonialism' or attendant words as "…process by which a central system of power dominates the surrounding land and its components." Gregory (1951)[1] defines this same idea as "…the control over one territory and its peoples by another, often accompanied by ideologies of superiority and racism, and may involve formal political and legal rule". From the forgoing, we constructed a working definition as "the physical, geographical or digital domination of a given sphere or territory, means of production for self-benefit of one entity over another whether country or not". Admittedly, this definition is a hybrid of historical and contemporary descriptions. This constructed definition highlights the geographical domination by a foreign power over another perceived 'inferior' territory but at the same time it captures emerging digital technologies dominion not limited by physical border controls or boundaries. This idea includes possessing control and power over the means of operations or production such as digital infrastructure.

But for the purposes of this study, we need to further define existing terminology and thus transition to make the distinction between 'digital' and 'data' colonialism. This distinction is important because it then helps us to know what exactly we reference in this enquiry. Simply stated, the distinction between data and digital colonialism lies in the control of the means of data generation or the data itself. In other words, 'digital colonialism' refers to the control of the means of data generation such as digital infrastructure used like servers, storage, software etc., that third party clients exploit while 'data colonialism' refers to the control of the data itself as generated by users (Pinto, 2018). While the former (i.e. digital colonialism) leads to the latter, it can be said that the rights to the data generated initially belong to the individuals but lost to infrastructure owners and controllers of the systems (means) by virtue of using their structural ecosystem and signing prior agreements passing on the right to the more powerful (usually multinational) entities. Dahmm and Moutrie (2021) make this distinction well when they state that "The term 'data colonialism' has been used to describe the appropriation of big data throughout the Global South, particularly by the major international powers in the data space, the United States and China…[while] The process of "digital colonialism" — whereby the Global North monopolizes the digital technology supply — can impede Southern economies, particularly in Africa, to develop their own digital economies, manufacturing capabilities, and other domestic industries"[2] relating to Data Sovereignty.

[1] Accessible at: https://www.google.com/search?q=definition+of+colonialism+by+different+authors&sca_esv=6292aac01ea52d81&rlz=1C1GCEU_enZM945ZM945&ei=-Rf1Z7vUC6Krxc8P0daN6Ak&oq=Definition+of+colonialism&gs_lp=Egxnd3Mtd2l6LXNlcnAiGURlZmluaXRpb24gb2YgY29sb25pYWxpc20qAggBMhAQABiABBiRAhiKBRhGGPkBMgsQABiABBiRAhiKBTILEAAYgAQYkQIYigUyBRAAGIAEMgsQABiABBiRAhiKBTILEAAYgAQYkQIYigUyBRAAGIAEMgUQABiABDIFEAAYgAQyBRAAGIAESL1VUI0HWOE4cAF4AJABAJgB3AKgAZgZqgEFMi0zLje4AQHIAQD4AQGYAgegAucnwgIOEAAYgAQYsAMYhgMYigXCAgsQABiABBiwAxiiBMICCBAAGLADGO8FwgIHECEYoAEYCsICBBAhGBXCAgcQABiABBgNwgIMEAAYgAQYDRhGGPkBwgImEAAYgAQYDRhGGPkBGJcFGIwFGN0EGEYY-QEY9AMY9QMY9gPYAQHCAioQABiABBiRAhiKBRhGGPkBGJcFGIwFGN0EGEYY-QEY9AMY9QMY9gPYAQGYAwDiAwUSATEgQIgGAZAGB7oGBggBEAEYE5IHCTEuMy01LjktMaAHiWGyBwczLTUuOS0xuAfiJw&sclient=gws-wiz-serp, accessed on 8th April, 2025.

[2] Refer to: https://www.data4sdgs.org/blog/avoiding-data-colonialism-trap, accessed on 9th April, 2025.

Technological developments[1] have progressively evolved over millennia, expressed in different forms and modes. Long before the ancient cuneiform or papyrus existed, technological advancements had long commenced. The successive industrial revolutions[2] have basically largely been around sea change technological shifts. This particular one (i.e. 4IR connected to AI) dates back to the 1950s or earlier and has progressively evolved until today, AI performs feats once thought impossible. Though this revolution has known seasonal halts and progress in the intervening period (to about 2021), it's advent has spawned massive changes, causing some traditional processes and ways of doing business seem obsolete (Bolon-Canedo & Moran-Fernandez, 2023). More is yet to unravel but humans need to keep growing as well by that token. Zambia stands at crossroads of 3rd and 4th Industrial revolutions needing to churn out relevantly equipped, skilled human capital to drive shifting future development goal posts. No longer will slow bureaucratic, red taped methods of doing business thrive in the contemporary and emerging context.

Rationale for study

Why should we spend time examining 'data' or 'digital' colonization' awareness? After all, digital technologies are increasingly mundane and a fact-of-life today. A number of important reasons for this consideration are advanced.

Firstly, it is the implications that come with this 'colonization'. If anyone has free access to and control of private records, then that entity is potentially in charge of the records, can use the said data without permission, or even alter it. Additionally, spying, surveillance tracking becomes a reality. Zuboff (2019) calls this 'Surveillance Capitalism'. This, alone should trigger concerns. Further, we should be asking who is profiting from our data? Who is using it? Do they have our permission?

Secondly, this 'control' has been perceived as a return to ancient colonialism, though in a different dress (Kwet, 2019; Pinto 2018; Greenwood, 2020). Some even call it a 'neo-colonialism', because only a few entities and countries in the global north control these systems, software, infrastructure, data sets, analytics and even generated information itself.

Thirdly, is the blatant disregard of ethics and human rights. By 'disregard' is meant the fact that unauthorized and unethical parties can easily invade private or even national datasets, hack into individual privacy, use their information, manipulate, benefit from, sell, and data mine from entire nations. It should be remembered that there are only a few leading global tech giants (i.e. Microsoft, Google, etc.) can do things without asking permission in reality. That violates human rights to privacy and expression (Azaroual, 2023; Greenwood, 2020).

Further, colossal financial losses result in contributing nations, individuals or companies originating this data. Daily, as humans transact, chat, debate, talk, express opinions, research, study, or interact, large swathes of data are consistently being generated. This is harvested and traded for huge sums of cash. If an individual can generate that much data, what more an entire community, nation or continent? All that data is captured, collated and analyzed using algorithms, neural networks etc., for various ends, including trade and business marketing, among others. Sadly, individuals generating (originating) this data are never consulted or rewarded, while unknown others profit from this same data without client knowledge, consent or benefit. That leaves data originators completely vulnerable. For these and other reasons, this consideration is critical.

When considering opportunities, we are referencing things like seamless data sharing, expanded digital democracy, access and the world can generate much valuable information in record time. In terms of the challenges, it is observable that less technologically advanced nations are now vulnerable and susceptible to surveillance or being spied upon as they do not have assured privacy because the data they generate is tracked, harvested, ripped-off and thus the data integrity is questionable and finally, issues of control or manipulation by a few powerful entities around the world. National sovereignty is lost in the process. This is a critical issue affecting entire nations. The few potent dominant multinationals control global data and decide what they use it for. These mega global conglomerates are able to do whatever they please sometimes tampering with or selling the data thus raking in colossal sums of money. Yet primary data originators languish in poverty and never prosper.

[1] In different forms.
[2] Now in the fourth (Moloi and Mhlanga (2021) accessible at: https://www.etdpseta.org.za/education/sites/default/files/2021-09/Key-features-of-the-fourth-industrial-revolution-in-South-Africas-basic-education-system.pdf, Accessed on 26th September, 2022.

The ideal scenario

In an ideal world, with everything functioning normally and everyone correctly executing their part, the concept of interconnectivity across the world using digital means is a most plausible idea.

First, the motivations, original intentions and aims are good in that it helps to shrink the world in the sense that within a split of a second, a decision made could be disseminated right across the globe for immediate attention, action and collaboration.

Second, if correctly used, digital democracy should be enhanced. In that world, everybody having access to information at low or no cost at all. But also, there is safety and connection among global citizens, knowing that their data is securely encrypted, protected and not exploited for unintended purposes. This could further enhance world's integration.

In third place, this connectivity could foster research and development (R&D). In that scenario, people easily share information, interact, collaborate and discover new things they previously did not know. Thus, when discussing research, technologies are an integral part without which work significantly slows down. AI, like ChatGPT, Google Gemini, DeepSeek or any other emerging software is currently all over the net with incredible potencies and capabilities. It is available for anyone with the means, possessing a link, know how to search for information only a click away. Then there is also the social development aspect. Nations can develop when they possess the right, timely, strategic information, skills, expertise and resources resulting in advanced countries.

Fourthly, as earlier hinted at, collaboration, harmony, information exchange fostering well-being through this interconnection in profound ways. Clearly, AI is a great concept demanding much digital data to operate efficiently and well (Bolon-Canedo & Moran-Fernendez, 2023).

Actual situation on the ground

Currently, Zambia is a major recipient and user of various forms of technology but hardly generates its own (in a major way). Even that which reaches Zambia (i.e. Technology) is hardly holistically scrutinized to establish both the pros and cons of these perceived helpful technologies. Generally, what is highlighted and focused on by opinion leaders are the immediate plausible perceived potential immense benefits resulting from technology adoption and exploitation to maximize national benefit. Clearly, physical wellbeing in Zambia is the main agenda item and scarcely any one objectively thinks of examining both sides of the coin before accepting things. An example will do. South Africa appears slightly different in that while applauding and accepting cutting edge digital technologies, the nation takes time to meticulously scrutinize emerging trends before committing. Starlink hit the world technology scene with blistering force, potentially offering superior direct connectivity or data access to nations of all stripes but for some reason, South Africa is yet to officially whole heartedly embrace this innovative star entity offering (as at December, 2024). For all intents and purposes, there could be a reason for this reluctance worth pondering over. One possibility could be the data security piece, the way it (data) is stored, accessed, safety-net features in place and data integrity issues appear paramount[1]. Granted, a mode or system may be flawless, offering superior service and yet unsafe for safe strategic data hosting. That entity may not be the ideal primary platform of choice for long, unless it urgently fixes the flaws. Advanced nations jealously guard their data, knowing what to share or not. Can it be said that a third world Global South country like Zambia has the ability to protect or dictate where its data goes and how it is used? Does the nation yield any profits and benefits from the data locally generated data stored offshore? If it does, is this profit maximized? These are the sorts of questions worth exploring. Let us pursue this consideration further by stating that the actual situation on the ground is not encouraging because like many Global South Nations, Zambia is open and vulnerable to all sorts of international exploiting entities including vultures likely having access to our information. Zambia cannot protect it and these invasive entities can, at will, use it to profit while data source generators remain in squalor.

Secondly, imbalances exist where a few global north corporations control our data. Imagine originating intellectual property but somebody else takes it away, gains control and sometimes even sells that very data back to you despite the fact that that you were the originating party.

[1] South Africa has rejected Starlink offer to provide services in South Africa as at 17th February, 2025, This stems from different motivations including SA's uncomfortability with and hostile relations between SA government and entrepreneur, Elon Musk. This was reported by iharare.com at the following link: accessed on 18th February, 2025. SA's rejection is instructive and other emerging economies must take stock of their choices. While all of us applaud Starlink and other tech giants, there is need equally to prudently evaluate options and their long term implications.

In the third place, data is used at will disregarding ethics, human rights and vulnerability. This data is freely used by hawkers and nobody can tell these corporations to stop abusing the same. Fourthly, most of the data in Zambia or Zambian data daily generated from the financial institutions (e.g. banks), government, individuals or HEIs is likely stored offshore in cloud servers, probably in places like Singapore or some other far-flung places. These cloud servers are controlled by a few corporations harvesting and using this data. We have no control and that is why the situation is concerning.

Who should be concerned and why?

The next question that begs answering could be, 'who should be concerned and why?' We have partly demonstrated the 'why' of this consideration by advancing a number of reasons, but now we are asking the question, 'who should be concerned?' Is it only private individuals? Is it only nations?

In this study, we argue and assert that all planet citizens without exception must be concerned because their data is being accessed, harvested, exploited, manipulated and traded for (Azaroual, 2023).

Secondly, respective governments should be concerned about where their sensitive data is stored, or ends up, how used, third party access, security and who does what to it. Responsible progressive governments have a duty to protect, safeguard and ensure the safety of their citizens', identities and that the generated data is secure. Thus, ethical governments should be concerned where and how they encrypt state secrets as well as the safety of its own citizens (Liywalii, 2024). The Zambia National Digital Transformation Strategy has a small but critical section highlighting these concerns (#2.1) This acknowledgement is key. However, it hardly shows the full deleterious effects of colonization beyond highlighting a few troubling indicators (e.g. crippling creativity).

Thirdly, decision makers of all sorts, stripes and strata should be concerned because they make decisions eventually affecting entire nations, communities and a wide spectrum of HEIs etc. Large swathes of data is daily locally generated and if not meticulously managed, countries remain in perpetual squalor when they could have been better off. Unless holistic mitigations are in place, manipulation, abuse and blatant human rights violations will perpetuate, as the unfettered multinationals exploit data sometimes against pauper nations. At other times colonizers use the same data to lure unsuspecting entities into things they initially did not intend doing or subscribing to. Thanks to AI, this data abuse can go in either direction. It could be for positive developmental ends or for negative purposes, given that the script is written (and controlled) based on the information that servers collect. For these and other reasons, everyone should be concerned and rightly so.

To execute this study, a number of relevant sources were consulted. One of them is Kwet (2019) that pursued a PhD study on digital colonialism and highlighted several interesting findings. For instance, he found that a few corporations had total unfettered access and control of this global data. These entities accessed private and public data which they used at will. What was troubling was that these entities were profiting from and were able to manipulate, control and literally break all data privacy protocols with practically no consequences. Additionally, they could use the data without permission and for their own intended ends. Kwet (2019) made a big issue of this matter. Few from Zambia have written or published on this troubling matter. Sichone (2023: 105) opined that "For example, Coleman (2019) and Pinto (2018) found that the large mega corporations repeatedly violated and breached country laws (e.g. privacy, engaged in unethical data surveillance for profit etc.) at will, since they potently had the influence and capacity to settle litigation battles while continuing to break others. They further found that these large conglomerates had the capacity to offer free cutting edge infrastructure to weak countries for exchange of information." That is a bugging problem facing pauper nations. For some reason, everybody thinks, "…well, this is a great idea that we are able to have information right across the globe. People can see us. We are visible. We feel powerful and important. 'Our voice is heard'", but really, who is benefitting or using this data and to what ends? There is need for research to establish exactly what is being said and having done all that, to offer possible solutions to this scenario, Suggestions include the building of a local servers to house data on Zambian turf in the unlikely event somebody wishes to lock Zambia down. With own infrastructure, we simply just switch to our local servers and access data while life continues. Said differently, there is need to enhance, expand, enlarge, update, upgrade, harness data, computing power, security and strengthen the National Data Center built several years ago[1]. But Zambia needs to strengthen or expand its capacity so that national data is safe and secure in case of any eventuality. As things stand, anything is possible.

Theoretical Framework

What theoretical framework was used to use to execute this kind of investigation in the Zambian context? To

[1] 2017 or earlier

execute the study, two adopted primary theories undergirded the enquiry, one of them was the Stakeholder theory, where we mapped and identified relevant entities mandated to control and manage data in this country. Institutions like ZICTA and Ministry of Technology and Science (MOTS) or such entities in this country. This could extend to mobile companies like MTN, Airtel or Zamtel. These are important to interview to gain insights. The Stakeholder theory posits that a stakeholder is anyone with vested interest in what is going on (Eskerod, 2020). If something goes wrong, they will react and if something goes well, they equally react. Further, stakeholders could be classified as primary and secondary. Primary stakeholders are those immediately impacted by the decision taken. Secondary stakeholders, on the other hand, are probably those not directly involved in the project or event. This theory is relevant to this study because it helps in the identification and later data collection from relevant parties.

The second adopted theory is the 'Surveillance Capitalism' originally postulated by Shoshana Zuboff (Kavenna, nd)[1] in her 2019 book *The age of surveillance capitalism* in which she argues that with the advent of AI, a number of things result including people's data being used for marketing purposes without consent. The theory argues that surveillance is a very present issue needing attention because individual rights are violated by the incessant rise of data analytics and big data feeding AI models in the quest to predict or influence human behaviour. Zuboff (2019) raises a relevant issue of protecting and defending people's rights daily violated by marketing corporations in collaboration with the perceived unaccountable global tech giants (Kevanna, nd; Avila, nd). This theory is equally relevant to this enquiry because it highlights the very ethical issues raised in this study. This study takes a 'behind the scenes' look and goes further to find out whether the average person on the street in Zambia is aware of what finally happens to their data and whether they are aware that their every move and digital life is meticulously monitored, tracked and surveyed.

Methodology

Methodology has to do with the approaches used to execute the study. Here, the design, data collection tools, analysis tools, rationale, sample size, criteria, and a number of elements are in view. In short, the methodology answers the 'how' question, in executing the study. For these purposes, a cross-sectional qualitative design approach was adopted. The reason for this is that the study elicited opinions, data points and thoughts from individuals in a limited time frame. This yielded data sought in relation to the Zambian scene. Creswell (2012), Berg (2009) and Patton (2002), all opine that qualitative designs are best for such kind of studies. In this way, we found out whether people were aware that 'data colonization' existed at all, and whether they knew that their data was being exploited for purposes they may not have been aware about. The tools used were interview guides via open ended questions with limited quantitative trace elements. The sample was drawn from a cross section of informants involved in and had been party to making data storage related decisions or opening up the Zambia to the outside world, such as Starlink or other digital service providers. Table 1 is a sample description.

Table 1: Sample description

	Entity	Type of inst.	Public or Private	Role
1	HEA		Gov	QA & Accred.
2	ZAQA		Gov	QF, cred mobility
3	MOTS		Gov	Digital environ. Enabler
4	MoE		Gov	National Education standards
5	ZICTA		Gov	ICT National Regulator
6	NU	HEI	Pvt	Research & Dev
7	EU	HEI		Research &

[1] Refer to this link for full write up: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy, accessed on 9th April, 2025.

				Dev
8	UNZA	HEI	P	Research & Dev
9	CBU	HEI	P	Research & Dev
10	UCZU	HEI	Pvt	Research & Dev
11	Mukuba University	HEI	P	Research & Dev.
12	KMU	HEI	P	Research & Dev
13	MU	HEI	P	Research & Dev
14	BTS	HEI	Pvt	Research & Dev
15	Exp 1			Exp.
16	Exp 2			Exp.
17	CBU	HEI		Research & Dev.
18	ARU	HEI	P	Research & Dev.
	Users			Experience
19	Mobile Phone provider	ISP		Mobile Phone company

Source: Research Data (2025)

Another layer of respondents were regular day to day users of connective digital devices. This enabled diversity as well as some level of in-built triangulation. The initial proposed sample size was small consisting of 19 informants. This is consistent with non-representative samples found in qualitative studies. The criteria used observed the following essential attributes:

1. Decision makers (Presently within or once in relevant Institution esp. HEI)
2. Lay regular digital device users
3. Mandated institutions (e.g. Gov: ZICTA; HEA, MOTS, MoE etc.)
4. Mobile companies (ISPs)
5. HEIs
6. Experts in the field of data security or related ICT sphere.

To be included, a respondent needed to at least any three of the above listed elements.

The criteria used to arrive at the final sample size was inclusion and exclusion responsive entities. Non-responsive entities were excluded. Purposive and convenience sampling were then employed to identify relevant study participants. Convinience and snowballing sampling enabled inclusion of additional respondents. For validity, everything was recorded, stored and transcribed. This was followed by review, coding, sorting, placing in predetermined categories concluding with content analysis, interpretation and report generation. Final triangulation ensuring validity and trustworthiness was achieved by comparing feedback from various sources including experts.

Findings

From collated data, the study synthesized a number of data points and presents them.

Data is not stored here in Zambia, but off shore at another part of the world, rather than at the local Zambian Data Center (Infratel)[1] since storage there is not mandatory. Granted, some of it might be stored in the Data Center, but most of it is likely offshore.

Third, data integrity or user confidentiality is not assured because anyone including has access to it, particularly the multinationals, and they can use it in ways they please, including selling the data.

Fourth, the multinationals reign in Zambia. More recently, included is Starlink, (i.e. direct satellite to cell project)

[1] Refer to their site at: https://infratel.co.zm/ accessed on 11th April, 2025.

to the list composed of Microsoft, Google, among other tech giants.
Fifth, users appeared largely unaware where their data finally ended up. 43% either had a vague idea or did not know at all. Figure 1 illustrates informants awareness of the final destiny of digital data.

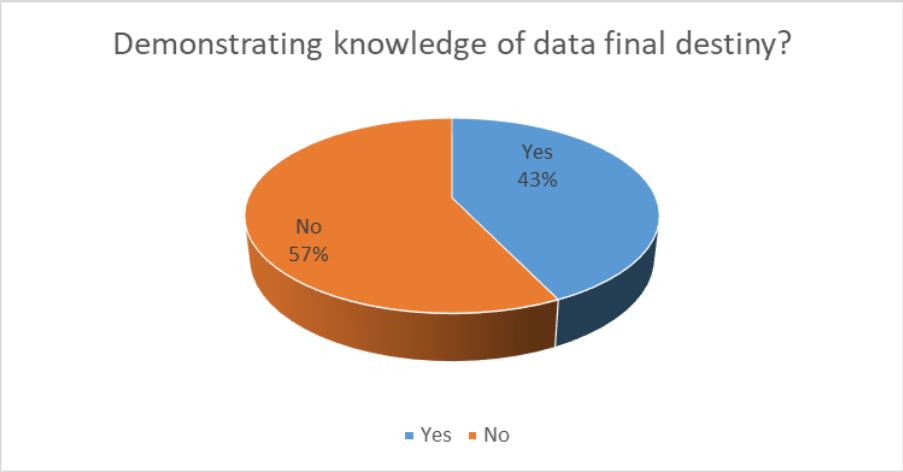

Figure 1: Knowledge of where data finally ended up
Source: Research Data (2025)

Sixth, Informants appeared unaware that their rights were being violated and others profiting off their data. Their knowledge of 'Data or Digital colonialism' distinction was low at 36%. Figure 2 summarizes awareness levels (proxy) of data/digital colonialism or its import.

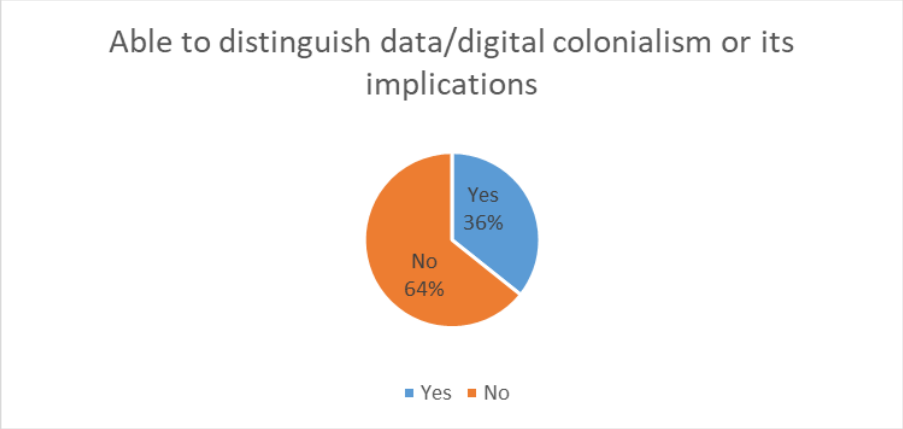

Figure 2: Summary of informant awareness levels of digital/data colonialism
Source: Research Data (2025)

Seventh, majority favored Zambia owing its own infrastructure (61%) for benefits including control and data security.
Eighth, Respondents comfort with not knowing final destiny: 93% expressed discomfort with this scenario. Table 2 shows a summary of what was found in the entire study

Table 2: Summary of study findings

	A	B	C	D	E	F	G	H	I
					1	2	3	4	5
		Entity	Type	Public or P	Knows fin	Knows fin	Comfortal	Able to di	At home v
1		MOTS	Gov		0				
2		HEA	Gov						
3		ZAQA	Gov						
4		Exp 9 (MM	HEI		1	1	0	1	0
5		NU (Sik)	HEI	Pvt	1	1	0	1	0
6		CABU	HEI	Pvt					
7		CBU (MS)	HEI	P	0	1	0	1	0
8		MU (CK)	HEI	P	1	1	0	0	0
9		Exp 8 (PhC	HEI		0	0	0	1	0
10		UNZA (Kal	HEI		0	0	0	0	0
11		KMU	HEI	P	1	1	0	1	0
12		Exp 10 (PH	Expert	P	0	0	0	1	0
13		Exp 1 (Pat	Expert		1	1	0	1	1
14		Exp 2 (Mw	Expert		1	1	0	1	1
15		Exp 3 (KS)	Expert		1	1	0	1	0
16		Exp 4 (DK)	Expert						
17		Exp 5 (Bar	Expert						
18		Exp 6 (Ma	Expert		1	1	1	1	0

Source: Research Data (2025)

Discussion

Having highlighted the key findings and, in a sense, hinted at the implications of data found, we will now proceed to discuss this data. Only a few key points are emphasized.

First of all, data integrity is essential to any nation, security, integrity, and esteem, because once data is safe and nobody's tampering with it, few litigation or rights violations arise. If this is not assured, it will trigger other problems, including ethical issues, data losses, human rights violations etc. This concern is consistent with what the National Digital Transformation Strategy (2022) observed.

Second, digital democracy needs to be enhanced and if not done, digital exclusion results where people not having access to data are systematically excluded. This is a form of digital divide (Trepels, 2012; Mukosa & Mweemba, 2019). In a thriving healthy democracy, information is freely accessible and available, but if this is lacking, only a few people, and because of these individuals who are using and sometimes abusing it, it may erode the very foundations of democracy and digital democracy, in particular, that is sought to be enhanced. If this is not urgently attended to and data is insecure, nations are ripped off by data miners (MOTS, 2024). These mongers, initially appearing with a big powerful corporate image, are in effect self-serving, ripping off pauper nations and abandoning them to chronic poverty. And in fact, the value of this generated data is extremely high probably with potential to outstrip all the copper mines income in Zambia combined. These conglomerates own the digital infrastructure and thus control the parameters of use and access (MOTS, 2024). In short, they do as they please. Such entities are the de facto rulers and colonizers, that can do what they wish, when, where and no one can successfully challenge them. To regain control, nations need to build or procure their own full house local ground and cloud servers with upgradeable capabilities able to seamlessly connect to the internet. This is consistent with what thought leaders like Greenwood (2020) have opined. Once connected, syncing should periodically, seamlessly take place updating both ground and cloud servers sync. There is need to sync, with this powerful network, without which the entity is deemed redundant. Said differently, Connectivity is essential to access the good things that come with it, but we must ensure that data integrity is safeguarded by the nation. Sichone (2023:142) observed the following: "Cyber security and integrity features. If the system is unreliable, occasionally loses data or porous, then users flee from it like a plague (Kwet, 2019; Scasserra & Elebi, 2021; Keevy et al., 2022). If anyone can easily hack into a system, destroy information or tamper without a trace, then the institution does well to rethink whether to proceed with the proposed purchase (Coleman, 2019; Kwet, 2019). Imagine for a moment that students could easily hack (ethically or not) into a system storing their grades or final course results, how reliable (trustworthy) would those grades be? This point scarcely needs further be-labouring because of the ghastly consequences." Sichone (2023:103) further opines: "Unknown to each user, all the data spawned on the net is collated (i.e. digital footprint) thus creating a picture through algorithms that can be analyzed and processed into useful information (Coleman, 2019; Kwet, 2019; Jandric & Kuzmanic, nd.;

Scasserra & Elebi, 2021). Baz (2018: 4) gives a helpful overview by stating that: "Recent developments in database technologies have made it possible to accumulate and maintain large and complex amounts of data from many forms and from multiple sources. In addition, this complex data is meaningful, and there are analytical tools that can transform the mold. These tools are called big data…," Baz further argues that teachers and researchers must be aware of the critical nature of their work and what they help generate over time. Although this fact may and should unsettle highly private individuals, given the potential security data breach and privacy violation concerns, this big data is spawned from all over the net and professionally used to create data for useful purposes as Baz (2018), and Kimmons and Rosenberg (2022) have ably attempted to explain. Coleman (2019), Kwet (2019), Pinto (2018), Mouton and Burns (2021), among others have carried out detailed penetrating analysis around what digital colonization is or entails with deeply concerning results. They found that national and individual sovereignty or control over data (which they perceive as an asset like any other) is lost to the tech giants in the gig ecosystem. They argued that a few selected Silicon Valley companies like Facebook (*Meta*), Google, [Microsoft], Project Aires or Starlink, for instance, have control of almost all the data generated around the globe, especially infrastructure poor (and thus vulnerable) Africa which they exploit to engender a new kind of imperialism. A detailed exploration of this phenomenon is outside the scope of this study but suffice it to say that data daily generated by educational institutions [and outside] lands in hands they cannot control, especially if they store data on the cloud (thus enabling unethical data surveillance or fostering even digital colonialism) or are connected to the web, for that matter. Kwet (2019) devoted an entire PhD study to that end which this study recommends [for] readers to acquaint themselves. Oyedotum (2020: 3) further deliberates on the data security concerns thus: "with computers and other portable technological devices being entrenched in our daily educational and teaching lives driven by the migration of traditional learning to online mode, there abounds various kinds of breaches, exposure to viruses, hacking potentials, and other cybersecurity threats (Nam, 2019)." Although this comment may arguably be directed towards learning digital platforms, the concern [is] universally true around internet use. That said, big data is equally used in other sound areas such as for Marketing purposes (Kimmons & Rosenberg, 2022). Present trends point to a scaling up of this in future." This scenario is concerning indeed.

While celebrating these tech giants once they enter a given country, what really they are coming to do is to colonize the nation afresh. Therefore, they ultimately are in full control of all country data. Fifth there is evidently little intention to ensure data security by our country. Ideally, our government was supposed to protect us but they are celebrating, in fact, because all they are thinking is the dollars flowing in, but forgetting the sovereignty, they are (deliberately?) forgetting other things in the name of being one world, and so on? So laws are aimed at controlling citizens and not data integrity. We see the laws that are being churned out. They are supposed to be targeted at helping citizens, the nation, or national sovereignty to secure the information for data integrity. The laws crafted often are designed to protect those in political power and to push down people who are using these means. Even those executing a genuine research effort, are doing the right thing, they too are affected.

Conclusion

We wrap up this entire study by re-echoing that data colonization impacts Zambia. This enquiry generates several conclusions based on available data. Having explored this sensitively important subject of 'data' and 'digital' colonization and how it affects our nation, we can safely opine that:

i. Zambians' identity, privacy etc., are currently vulnerable because no firm safety nets or full house digital infrastructure (updated) exist to guarantee from third party access protection for citizen's data. Additionally, sensitive data is stored offshore on global digital servers. By that token, Zambia and Zambians are further currently vulnerable because of these absent key safety nets. In the event there is a problem, Zambia likely stands to lose its valuable data. Another possibility is that, in the event of disagreements, with these ISPs or cloud server providers, the country could be squeezed by these providers much like Starlink did during the Russia/Ukraine war. Starlink provided direct internet access when all imaginable national digital infrastructure was demolished. By the same token, the same company could have unilaterally chosen to 'switch off' the country at will. A further ramification is that such entities have access to state and individual secrets, strategies, plans etc., and can do whatever they please with such confidential data. This gives them strategic competitive advantage over others and most likely will always be a step ahead. That is the first conclusion arrived at.

ii. As a country, Zambia likely lacks adequate digital safeguards in terms of infrastructure. Granted, the National Data Center [Infratel] exists (since 2017) but how advanced and adequate is it? Despite

several touted upgrades and the impressive security protocols, generally Zambia is ill equipped and lags behind, potentially relying on external facilities. Digital device users daily expose their information and should be made aware that their data is up for grabs by anyone and everyone with access or control to data storage sites. Few people realize this that pundits can twerk, tilt their data in directions different ways. Most of the profit makers concentrate on maximizing income at the expense of ethical practice or data security. A further consideration; Suppose something undesirable were to happen, say, a disagreement with digital infrastructure providers, we are all instantly affected for lack of Zambian owned infrastructure.

iii. This study further concludes that the lack of dedicated funds and investment into state of the art digital infrastructure impedes progress leading to the current vulnerability. There is need to invest in knowledge management, capacity, skills and Computing power.

iv. Sensitization and awareness is lacking in the country. Ignorance of digital technologies and implications of their use was evident from the study. Many digital device patrons seem unaware nor do they care what finally happens to their precious data.

Given the above, we safely conclude that Zambia is at a very bad vulnerable place. It cannot argue or control these potent invading tech giants. If anything, Zambians look forward to accessing free things invested by international entities rather than supporting home grown initiatives. Even decision makers and leaders long for free things and thus gravitate towards options with unfavourable long term consequences. Granted, partnerships must be diligently sought after but these need to be equitable and mutually beneficial in the long run. As things stand, these are concerning conclusions but there is hope that the country could possibly make a difference in future, if intentionally alert.

Recommendations

From the foregoing conclusions, the following specific recommendations naturally flow targeting specific stakeholders for action.

1. Zambian government should invest in cyber security. Zambia has made progress on the cyber security index and the generation of the national cyber security strategy but more remains to be done (Mulenga, 2024). This means Zambia should possess and heavily invest in cutting edge, trending infrastructure, with updated software. All these things should ensure data integrity, storage forestalls data leaks[1] and assured access. Sichone (2023:142) rightly opined that “Security (i.e. data integrity, security, confidentiality, ethical aspects etc.) is another component to watch out for (Kwet, 2019; Keevy et al., 2022).”, suggesting this is a matter of urgency. Government (ZICTA) should foster this because they are the ultimate regulating body mandated with the primary task of protecting the data rights of citizens, valuable national data, sensitive information securely stored within their eco-system. Figure 1 is a model solution structure for Zambia proposed by Sichone in 2023:

[1] Prominent examples of massive data leaks or unethical data breaches/breaches include the famous 2014 Wiki leaks, Cambridge Analytic, among troubling others. However, the majority of these breaches go unreported, noticed or prosecuted. Avila (nd) has reported on these unethical and unbalanced practices. Refer to her undated paper found at: https://infratel.co.zm/, accessed on 11th April, 2025.

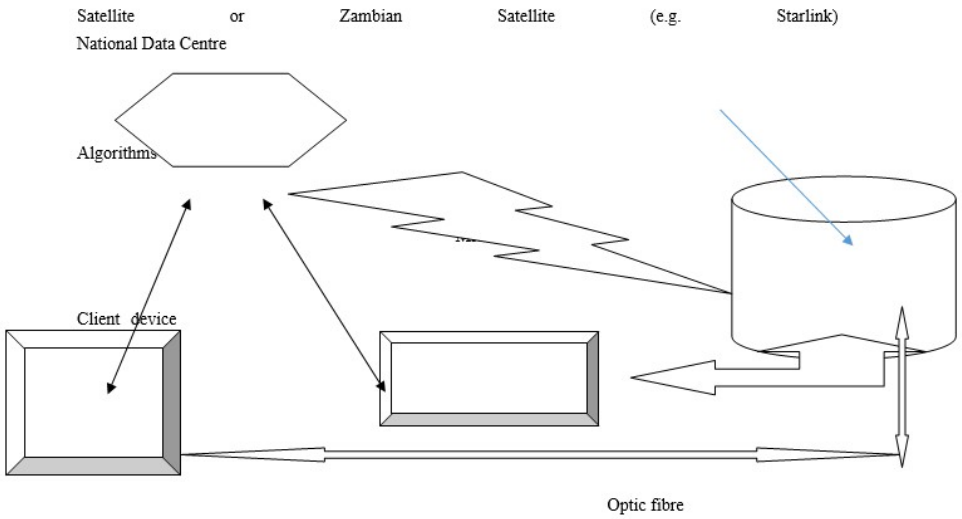

Figure 1: Proposed alternative model for country data security

Source: Research Data (2023); Generated by this Author

This alternative structure for data security infrastructure is the easier but riskier route. It assumes agreement, that the National Data Center ground server has 100% access to the provider satellite (cloud server) and automatically periodically seamlessly syncs. Said differently, Bolon-Canedo and Moran-Fernandez (2023:36) suggest a very helpful approach: the development of algorithms 'on the edge' with capabilities to sift sensitive information before data gets to the cloud. They suggest several other privacy protection options so that no rights are infringed or violated. They further state "one possible solution to privacy data collected on different devices is to develop algorithms on the edge (Shi et al., 2021)". Ideally, the system should also encrypt or have options to retain data through a phrase Bolon-Canedo and Moran-Fernandez (2023) call 'algorithm on edge'. Essentially, this keeps some sensitive information from third party (or cloud storage) access retaining it within the ground servers hence securing it. Generally, all other information should directly and seamlessly sync with the cloud but in the event that the cloud server locks down for any reason, the ground server immediately kicks in alleviating any potential data access delays or loss challenges. In that way, the country retains a record (hence secure data access) controls and ensures speedy connections.

Secondly, Zambia (Govt), NGOs etc., should train users on safer (data storage, management and use) practices and how they are to protect their data as well as what or what not to place on connective devices. Patrons should be made aware, sensitized because presently patrons use devices without much thought, knowledge that the information is being remotely collated, tracked or used by third parties somewhere who, in fact, are profiting from and getting richer (on private data) while the originators of this data remain poor. NGOs should be at work (such as advocacy groups), the government itself and private individuals should aggressively talk about this to guarantee safety.

Third, there is need for the government to create or expand the National Data Center. While one already exists (Infratel), something bigger, better and more secure to strengthen what is there is needed. A locally owned server with cloud computing capabilities and connections is strongly proposed. Government should take the lead in this venture, working along-side relevant stakeholders to secure national data.

Fourth, future Research should explore how Zambia could better harness and, if possible, generate its own data rather than merely selling it or giving out for free but using it for local marketing purposes. Before signing up, beware, "the devil is in the details" as an ancient adage rightly says. We need to take warning from previous tribal chiefs that lost large swathes of territory and mineral rights to deceitfully cunning colonizers only to painfully discover too late that they had been swindled with long term telling consequences to posterity (Ndulo, 1977; Greenwood, 2020; Keevy et al., 2022; Kukutai & Taylor, 2016; Scassera & Elebi, 2021; Avila, nd; Liywalii, 2024; Roberts & Montoya, 2022).

Fifth, Zambia needs to invest into awareness on how generated data is stored, used or where it finally ends up. This awareness will lead to better individual best practices so that people know how to safeguard their privacy

despite being connected to the tech giants control on their devices. There is need for people to be aware what is going on at the moment. From what was been observed during the study, not many people knew or cared exactly what is going on, what is at stake, who is gaining, who is winning, who is losing or whose rights are being violated. Such kind of things do not seem to be in the public domain. Only a few people that know can twerk, tilt their direction in different ways but most data miners are profit makers just wanting to make a killing and care little about ethics, data security or about whose rights were being violated. All they want is the extra buck.

Sixth, decision makers, technocrats, politicians, civil society etc., must make the right strategic calls ensuring that long term national interests are in view not mere short term political mileage goals taking precedence. Once the country's digital sovereignty is lost, out also goes its birth right, much like Esau gave up his right to Jacob (Genesis 25:29-34).

Seventh: Stronger equitable cyber laws around data. Remember, AI appeared way after current (obsolete?) laws and thus presents challenges. These laws must periodically be revised and new one generated. Robert and…speak to this issue, though in the South African context.

Limitations

This study had limitations that could have impacted on the quality of the results. Here we highlight a number of areas that could have possibly affected the study.

1. Sample size. In a qualitative study, a sample is fine but this particular sample ( ) could have been more helpful if it was larger, potentially giving a fuller picture of what is going on, in a particular locality or space. Given the sample, it was difficult to arrive at a strong saturation point because then, there is assurance that all bases have been covered, and therefore no new data is emerging. This was a limitation in that sense.
2. The lack of or limited access to locally generated and published documents. In Zambia, not much information on digital or data colonization exists nor is there awareness of final destiny of generated data among informants in this country. The Researchers used only what was available, and the rest of it was basically drawn from international sources, apart from data generated during interviews. There evidently is limited local Research on this matter in this country, although decision makers are currently excited to welcome and have Starlink, Google, Microsoft, Meta (Facebook) and all these big multinationals service Zambia. In a sense, most Zambians perceive these conglomerates as the ultimate panacea for national development. In one sense, this is definitely true and to be celebrated, but there is a subtle high latent price tag to all this, including imperialistic data control agenda, where corporations can exploit this data in ways that they think best serves their interests. We need to be very mindful of all these things, or else Zambia stands to lose as a nation, individuals, and ultimately, as homesteads.
3. Three data collection methods were used including phone call, WhatsApp (written) and in-person interview. Each of these had their own challenges and could have affected the clarity of responses. It was observed that in person interviews or phone calls proved better because misunderstandings were immediately and easily clarified.
4. Data collection period (1st-8th April, 2025) was limited and resulted in potential key respondents being excluded. Their voice could have made a difference in the final study outcome.

Digital colonialism has lasting deleterious effects on a given country and its citizens for generations (Carr, 2010; Hoadley & Uttamchandani, 2021; Lanier, 2010; Avila, nd; Bolon-Canedo & Moran-Fernandez, 2023; Macra, 2021; Greenwood, 2020). Once entrenched, getting out of the trap attracts heavy penalties from controlling tech giants and thus, the earlier a country escapes, avoids or prudently manages (resists) the temptation to take in the enticing carrot, the better for posterity (Keevey et al, 2022; Kukutui & Taylor, 2016; Roberts & Montoya, 2002; Carr, 2010).

References

Avila, R. (nd). 'Against Digital Colonialism-Autonomy', Available at: https://autonomy.work/wp-

content/uploads/2020/09/Avila.pdf, Accessed on 5th October, 2022.

Azaroual, F. (2024). 'Artificial Intelligence in Africa: Challenges and Opportunities', Policy Brief (May), Available at: https://www.policycenter.ma/sites/default/files/2024-09/PB_23_24%20%28Azeroual%29%20%28EN%29.pdf, Accessed on 25th November, 2024.

Baz, C.F. (2018). 'New Trends in e-Learning', *IntechOpen*, Accessed on: 7th July, 2022. Available at: https://cdn.intechopen.com/pdfs/60282.pdf.

Berg, B.L. (2009). *Qualitative Research Methods: For The Social Sciences* 7*e*, Pearson Education.

Bolon-Canedo, V., and Moran-Fernandez, L. (2023). 'Artificial Intelligence: Past, Present and Future', RACSG, Volume 112 # 1; 28-39, Available at: https://rac.es/ficheros/doc/b05bb04f3283e5f4.pdf, Accessed on 30th January, 2025.

Carr, N. (2010). *The Shallows: What the Internet is doing to our brains*, New York: W.W. Norton. Available at: https://www.pdfdrive.com/the-shallows-what-the-internet-is-doing-to-our-brains-e178711310.html, Accessed on: 3rd October, 2022.

Coleman, M., and Glover, D. (2010). Educational Leadership and Management: Developing Insights and Skills, McGraw Hill (Open University Press), Available at: https://www.academia.edu/24824795/Educational_Leadership_and_Management_Educational_Leadership_and_Management?email_work_card=view-paper, Accessed on 9th November, 2022.

Creswell, J.W. (2012). *Educational Research*, 4e, Pearson. Available at: https://www.pdfdrive.com/educational-research-planning-conducting-and-evaluating-d16448388.html, Accessed on 3rd October, 2022.

Dahmm, H., and Moutrie, T. (2021). 'Avoiding the Data Colonialism Trap', *TReNDS* (online), Accessed on 31st March, 2023, available at: https://informatics.tuwien.ac.at/news/1991. Or https://www.data4sdgs.org/blog/avoiding-data-colonialism-trap, accessed on 9th April, 2025.

Eskerod, P. (2020). 'A Stakeholder Perspective: Origins and Core Concepts', Oxford Research Encyclopedias, Business and Management(online) Available at: https://oxfordre.com/business/display/10.1093/acrefore/9780190224851.001.0001/acrefore-9780190224851-e-3?d=%2F10.1093%2Facrefore%2F9780190224851.001.0001%2Facrefore-9780190224851-e-3&p=emailAQT4fxOzYyCr., Accessed on 14th February, 2024.

Greenwood, F.(2020). 'Data Colonialism, Surveillance Capitalism and Drones', in *Mapping Crisis*, University of London Press: 89-117, Available at: https://www.jstor.org/stable/pdf/j.ctv14rms6g.12.pdf?acceptTC=true&coverpage=false&addFooter=false,

Accessed on 4th March, 2023.

Gregory, D. (1951). "Colonialism", Oxford Reference, available at: https://www.google.com/search?q=definition+of+colonialism+by+different+authors&sca_esv=6292aac01ea52d81&rlz=1C1GCEU_enZM945ZM945&ei=-Rf1Z7vUC6Krxc8P0daN6Ak&oq=Definition+of+colonialism&gs_lp=Egxnd3Mtd2l6LXNlcnAiGURlZmluaXRpb24gb2YgY29sb25pYWxpc20qAggBMhAQABiABBiRAhiKBRhGGPkBMgsQABiABBiRAhiKBTILEAAYgAQYkQIYigUyBRAAGIAEMgsQABiABBiRAhiKBTILEAAYgAQYkQIYigUyBRAAGIAEMgsQABiABBiRAhiKBTILEAAYgAQYkQIYigUyBRAAGIAEMgUQABiABDIFEAAYgAQyBRAAGIAESL1VUI0HWOE4cAF4AJABAJgB3AKgAZgZqgEFMi0zLje4AQHIAQD4AQGYAgegAucnwgIOEAAYgAQYsAMYhgMYigXCAgsQABiABBiwAxiiBMICCBAAGLADGO8FwgIHECEYoAEYCsICBBAhGBXCAgcQABiABBgNwgIMEAAYgAQYDRhGGPkBwgImEAAYgAQYDRhGGPkBGJcFGIwFGN0EGEYY-QEY9AMY9QMY9gPYAQHCAioQABiABBiRAhiKBRhGGPkBGJcFGIwFGN0EGEYY-QEY9AMY9QMY9gPYAQGYAwDiAwUSATEgQIgGAZAGB7oGBggBEAEYE5IHCTEuMy01LjktMaAHiWGyBwczLTUuOS0xuAfiJw&sclient=gws-wiz-serp, accessed on 8th April, 2025.

Hill, C. (2003). *International Business*, 4e McGrawll-Hill.

Hoadley, C., and Uttamchandani, S. (2021). 'Current and Future Issues in Learning, Technology, and Education Research', Spencer Foundation, Available at: https://spencerfoundation.s3.us-east-2.amazonaws.com/store/0bde4ae6d0b87961a75c4cf01b769ca4.pdf, Accessed on 20th October, 2022.

Kavenna, J. (nd). 'Soshana Zuboff: 'Surveillance Capitalism is an assault on human autonomy', *The Gaurdian* (int) (online) available at: https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy, accessed on 9th April, 2025.

Keevy, J., Rajab, R., Arnesen, J., Ngeleza, B., Beukes, JC., Freeth, R., Akpan, A., Ntuli, S., Laughton, P., Marais, MA., Vannini, S., Shiohira, K., and Pereira, C. (2022). Reclaiming self-sovereignty for all South Africa citizens' data by 2030, *JET Education Services and merSETA*, Available at: https://jet.academia.edu/JamesKeevy, Accessed on 4th November, 2022.

Kimmons, R., and Rosenberg, M.J. (2022). 'Trends and Topics in Educational Technology: 2022 Edition', *TechTrends* (online, February) pp. 134-140. Accessed on 14th March, 2022. Available at: https://link.springer.com/article/10.1007/s11528-022-00713-0.

Kukutai, T., and Taylor, J. (ed: 2016). *Indegenous Data Sovereignty: Towards an Agenda*, Australian National University Press, Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjf372V-KL7AhVQhFwKHZGjCWIQFnoECBwQAQ&url=https%3A%2F%2Flibrary.oapen.org%2Fbitstream%2Fhandle%2F20.500.12657%2F31875%2F624262.pdf&usg=AOvVaw2pow_cdEwSiHYJW8G1dwo7, Accessed on 10th

November, 2022.

Kwet, M. (2019). 'Digital Colonialism: South Africa's Education Transformation in the Shadow of Silicon Valley', Rhodes University (PhD Thesis), Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3496049, Accessed on 16th October, 2022.

Lanier, J. (2010). *You are not a gadget: A manifesto*, New York; Alfred A. Knopf Publishers. Available at: https://www.pdfdrive.com/you-are-not-a-gadget-e193499055.html, Accessed on 3rd October, 2022.

Liywali, E. (2024). 'Artificial Intelligence (AI) Ethics and Governance in Zambia: A Philosophical Perspective on the Challenges and Opportunities', University of Zambia (seminar presentation). Available at: https://www.researchgate.net/publication/381489781_Artificial_Intelligence_AI_Ethics_and_Governance_in_Zambia_A_philosophical_perspective_on_the_Challenges_and_Opportunities, Accessed on 25th November, 2024.

Macra, G.M. (2021). 'Unlocking digital connectivity in Africa', European Investment Bank, Available at: https://www.eib.org/attachments/publications/unlocking_digital_connectivity_in_africa_en.pdf, Accessed on 29th January, 2025.

Manzar, O. (2017). 'What is data colonization and why it matters to us in India', *Business Standard*, August online edition. Accessed on 22nd March, 2023, Accessible at: https://www.business-standard.com/article/economy-policy/who-owns-your-data-india-needs-to-tackle-data-colonisation-soon-117081700234_1.html

Ministry of Technology and Science (MOTS, 2022). 'National Digital Transformation Strategy 2023-2028', GRZ, Accessed 29th May, 2024. Available at:

Mouton, M., and Burns, R. (2021). '(Digital) neo-colonialism in the smart city, Regional studies', Taylor & Francis (Routledge)', Volume 52 # 12, pp. 1890-1901, Available at: https://hal.archives-ouvertes.fr/hal-03236274/document, Accessed on 5th October, 2022.

Mulenga, A. (2024). 'Zambia reports rise in global cyber security Index', Available at: https://itweb.africa/content/KzQenqjyL9AMZd2r, accessed on 8th February, 2025.

Mulenga, A. (2023). 'Zambia gets ready to build a tier 3 data center', Data Management (online) available at: https://itweb.africa/content/kLgB17ezWlNM59N4, Accessed on 8th February, 2023.

Mukosa, F., and Mweemba, B. (2019). 'The Digital Divide Hindering E-learning in Zambia', *International Journal of Scientific Research and Engineering Development* Volume 2 # 3 (May-June) pp. 860-865. Available at: https://www.researchgate.net/publication/334318597_The_Digital_Divide_Hindering_E-learning_in_Zambia-, Accessed on 28th June, 2021.

Ndulo, M. (1977). Mining Rights in Zambia, Oxford University PhD Thesis. Available at: https://ora.ox.ac.uk/objects/uuid:af14b92c-9a22-49e1-b4cb-f410d6edf4d3, accessed on 8th April, 2025.

Oyedotum, T.D. (2020). 'Sudden Change of Pedagogy in Education driven by Covid-19: Perspectives and Evaluation from a Developing country', Research in Globalization (online) Volume 2 Available at: https://www.sciencedirect.com/science/article/pii/S2590051X20300186, Accessed on 20th July, 2022.

Ohara-Devereaux, M., and Johansen, R. (1994). *Global Work: Bridging Distance, Culture & Time*, Jossey-Bass Publishers.

Patton, M.Q. (2002). *Qualitative Research & Evaluation Methods*, London: Sage Publications.

Pinto, A.R. (2018). 'Digital Sovereignty or Digital Colonialism?', *SUR* Volume 15 # 27, pp. 15-27. Available at: https://sur.conectas.org/wp-content/uploads/2018/07/sur-27-ingles-renata-avila-pinto.pdf, Accessed on 5th October, 2022.

Roberts, S.J., and Montoya, L. (2022). 'Decolonization, Global Data Law, and Indigenous Data Sovereignty', *Accel AI Institute*, Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjf372V-KL7AhVQhFwKHZGjCWIQFnoECBUQAQ&url=http%3A%2F%2Farxiv.org%2Fabs%2F2208.04700&usg=AOvVaw0a34GAlrtUaA546YhIYQcy, Accessed on 12th October, 2022.

Rowntree, L., Lewis, M., Price, M., Wyckoff, W .(2015). *Diversity Amid Globalization: World Regions, Environment, Development*, 6e, Pearson.

Scasserra, S., and Elebi, C.M. (2021). 'Digital Colonialism: Analysis of Europe's trade agenda, Trade & Investment Policy Briefing', (October), Available at: https://www.tni.org/en/publication/digital-colonialism, Accessed on 5th October, 2022.

Sichone, B.C. (2023). 'Assessment of eReadiness status for enhanced adaptation to online education in 20 selected HEIs in Zambia', ARU unpublished PhD Thesis.

Steger, M.B. (2003). *Globalization: A Very Short Introduction*, Oxford University Press.

Trepels, I. (2012). 'Bridging the Digital Divide in Zambia', (Master's Thesis) Radbound University Nijmegen. Available at: https://www.ru.nl/publish/pages/769526/iristrepels_2012.pdf. Accessed on 22nd June, 2021.

Zuboff, S.(2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs

Bio

Dr. Billy C Sichone serves as Deputy Vice Chancellor for Research and Graduate studies at Central Africa Baptist University. He holds several doctorates including a PhD in Online Education and has been in Academia for over a decade after a near two decade experience in the Development Industry. He is also author of several books and paper on Research, Apologetics and Business.